Cyberprzestrzeń: nowa granica dla policji?

Opublikowana w 2011 r. brytyjska strategia bezpieczeństwa cybernetycznego stwierdza, że:

Naszą wizją jest, aby w 2015 r. Wielka Brytania czerpała ogromną wartość gospodarczą i społeczną z tętniącej życiem, odpornej i bezpiecznej cyberprzestrzeni, w której nasze działania, kierując się naszymi podstawowymi wartościami, takimi jak wolność, sprawiedliwość, przejrzystość i praworządność, zwiększają dobrobyt, bezpieczeństwo narodowe i silne społeczeństwo.

Wymowne jest to, że Wielka Brytania w ogóle posiada strategię bezpieczeństwa cybernetycznego. Rządy i ich agencje – nie tylko w Wielkiej Brytanii, ale na całym świecie – usiłują odróżnić przestępczość, która w szczególności opiera się na wykorzystaniu hiperłączności globalnej technologii informacyjnej, od „zwykłej" przestępczości, którą można po prostu umożliwić dzięki wykorzystaniu technologii informacyjno-komunikacyjnych. Pomimo interwencji legislacyjnych, takich jak Konwencja Rady Europy o cyberprzestępczości (jej analiza zob. Vatis, 2010, s. 207) z 2001 r., cyberprzestrzeń pozostaje w dużej mierze nieuregulowaną placówką jurysdykcyjną. Pierwszy akt prawa karnego regulujący użytkowanie – a raczej niewłaściwe użycie – komputerów w Wielkiej Brytanii został uchwalony w 1990 r. Motyw ustawy Computer Misuse Act z 1990 r. stwierdza, że była to ustawa „mająca na celu zabezpieczenie materiałów komputerowych przed nieautoryzowany dostęp lub modyfikacja; i dla powiązanych celów."

To wąskie, przedinternetowe skupienie w dużej mierze opierało się na koncepcji komputera jako funkcjonalnego pudełka (lub sieci pudełek) zawierającego „materiał" wymagający ochrony). Chociaż ustawa dotyczyła nieuprawnionego dostępu, koncepcja spowodowania, aby komputer spełniał funkcję wspierającą inne przestępstwa, była także centralną częścią nowego ustawodawstwa , które po raz pierwszy w Wielkiej Brytanii , starali się dogonić technologię komputerową, która stawała się częścią codziennego życia ludzi – był to wyścig, w którym proces legislacyjny nie miał szans. Chociaż przepisy zostały zmienione w 2006 r. wraz z wprowadzeniem nowego przestępstwa polegającego na nieuprawnionym działaniu zakłócającym działanie komputera lub programu itp., patrząc wstecz przez dzisiejszy cyfrowy pryzmat, ustawodawstwo ma zdecydowanie analogowy wygląd. Kiedy przepisy weszły w życie, nie mieliśmy pojęcia, jaki wpływ będzie miała „superautostrada informacyjna" na nasze codzienne życie, a tym bardziej angażujący wpływ mediów społecznościowych. Według brytyjskiej strategii bezpieczeństwa cybernetycznego z 2011 r. w momencie jej publikacji 2 miliardy ludzi korzystało z Internetu i istniało ponad 5 miliardów urządzeń podłączonych do Internetu. Jak wynika z dokumentu Ministerstwa Sprawiedliwości, w tym samym roku liczba osób, przeciwko którym toczono postępowanie w związku z przestępstwami na podstawie ustawy o nadużyciu komputera z 1991 r. w Anglii i Walii, wyniosła dziewięć , przy czym żadna osoba nie toczyła postępowania z tytułu dwa przestępstwa z art. 1 ust. 1 i art. 1 ust. 3. Co być może zaskakujące, dane z krajowej bazy danych prawnych policji (PNLD), wykorzystywanej przez wszystkie siły policyjne w Anglii i Walii do określania sformułowań dotyczących przestępstw, kodów opłat i badań prawnych pokazują, że w ciągu dwóch tygodni (wybranych losowo) w 2013 r. weszła w życie ustawa o nadużyciach komputerowych 1990 i jego części składowe były dostępne w następujący sposób:

Między 4 a 10 marca — 907 razy

Między 10 a 16 listopada — 750 razy

Pogodzenie tych dwóch zbiorów danych jest trudne. Chociaż z danych dostępowych PNLD jasno wynika, że funkcjonariusze organów ścigania w Anglii i Walii w dalszym ciągu często przesłuchują przepisy z 1990 r. (średnio około 825 razy w tygodniu lub 118 razy dziennie lub 42 900 razy w roku), liczba postępowań karnych w związku z przestępstwa powiązane są znikomo małe. Jednym z wielu

wyzwań związanych z cyberprzestępczością i przestępczością wykorzystującą cyberprzestępczość jest ustalenie jej rozmiaru i kształtu.

KSZTAŁT WYZWANIA

Tak jak od 1990 roku kształt naszej technologii zmienił się nie do poznania, tak samo zmienił się kształt wyzwania. Niemal nieograniczony rozwój łączności internetowej można postrzegać z jednej strony jako fenomenologiczną emancypację mas, rozszerzenie Ruchu Danych Obywatelskich i prawo obywateli do danych znajdujących się w posiadaniu publicznym . Z drugiej strony, upoważnienie, jakie dało innym (szczególnie suwerennym państwom) do nadużywania cyberprzestrzeni, zostało uznane za reprezentujące „koniec prywatności", co skłoniło Organizację Narodów Zjednoczonych do zwrócenia się do Organizacji Narodów Zjednoczonych o „kartę praw cyfrowych". W ramach rozwiązania pośredniego strategia brytyjska określa kluczową – i, jak twierdzi się, najbardziej nieuchwytną – koncepcję w dokumencie: koncepcję „żywej, odpornej i bezpiecznej cyberprzestrzeni". można osiągnąć w tętniącej życiem przestrzeni zarządzanej przez komputery? Zarówno jeśli chodzi o komputery, jak i naszą na nich zależność, odeszliśmy tak daleko od pierwotnego pojęcia skrzynek, funkcji, poleceń i programów, wraz z konsekwencjami, jakie mogą być spowodowane ich wykorzystania, że konieczne jest gruntowne przemyślenie. Czym więc – i gdzie – jest cyberprzestrzeń? Ostatnio wiele napisano na temat zagrożeń, ryzyka i szkód powodowanych przez „cyberprzestępczość", „przestępczość elektroniczną" i „przestępczość wykorzystującą cyberprzestępczość", ale ustawodawstwo pozostało daleko w tyle. UE prowadzi znaczną liczbę działań związanych ze swoją „strategią cyberbezpieczeństwa" i własną roboczą definicją „cyberprzestrzeni", chociaż jej własna proponowana dyrektywa nie zawiera definicji prawnej, lecz raczej definicję dotyczącą bezpieczeństwa sieci i informacji, która ma odpowiadać agencji utworzonej w 2004 r. nazwa. W Wielkiej Brytanii w 2012 r. w pytaniu parlamentarnym Sekretarz Stanu ds. Sprawiedliwości zadał pytanie, ile postępowań karnych miało miejsce w związku z „przestępczością elektroniczną" w ciągu ostatnich 5 lat. W odpowiedzi parlamentarny podsekretarz stanu podał statystyki dotyczące art. 1(4), 2 i 3(5) ustawy o nadużyciach komputerowych, podczas gdy odpowiadający mu wpis Hansarda zawiera w nagłówku wyrażenie „cyberprzestępczość". Gdziekolwiek to jest, prawnicy konstytucyjni na całym świecie zmagają się ze stosowaniem ustawodawstwa swoich krajów w obliczu bezgraniczności wirtualnego słowa Internetu; zastosowanie „analogowych" praw terytorialnych do nieokreślonych cyfrowych granic nieskończonej globalnej sieci komunikacyjnej okazuje się, jak się wydaje, przesadą dla naszych konwencjonalnych systemów prawnych. Oto dlaczego. Jeśli chodzi o interpretację i stosowanie prawa poza naszymi własnymi granicami jurysdykcji administracyjnej, z biegiem czasu rozwinął się ustalony zbiór zasad, zachowań i orzecznictwa uzgodnionych na szczeblu międzynarodowym. Podejmowano próby zastosowania tych norm prawnych do cyberprzestrzeni. Na przykład Międzynarodowy Pakt Praw Obywatelskich i Politycznych określa pewne kluczowe obowiązki państw-sygnatariuszy. Ponadto działania prowadzone w cyberprzestrzeni lub za jej pośrednictwem nie powinny pozostawać poza zasięgiem innych zabezpieczeń wspólnotowych, takich jak te zapisane w Europejskiej Konwencji Praw Człowieka lub Karcie praw podstawowych UE, szczególnie gdy w grę wchodzą takie kwestie, jak wykorzystywanie seksualne dzieci w internecie. Pierwszym podstawowym wyzwaniem, jakie się z tym wiąże, jest jednak kwestia jurysdykcji. Cottim zidentyfikował pięć teorii i podejść jurysdykcyjnych w tym kontekście, a mianowicie

1. Teoria terytorialności: teoria, że jurysdykcję określa miejsce, w którym przestępstwo zostało popełnione w całości lub w części. Ta „teoria terytorialności" ma swoje korzenie w modelu suwerenności państwa, panującym w pokoju westfalskim, obowiązującym od 1684 r. Podejście to opiera się na założeniu, że państwo sprawuje suwerenność nad omawianym terytorium, które to

założenie jest oczywiste i łatwe do obalenia w większości przypadków związanych z „cyberprzestrzenią".

2. Teoria narodowości (lub osobowości aktywnej): oparta przede wszystkim na narodowości osoby, która popełniła przestępstwo (zobacz Stany Zjednoczone Ameryki przeciwko Jayowi Cohenowi; Docket No. 00-1574, 260 F.3d 68 (2d Cir., 31 lipca 2001 r.), gdzie World Sports Exchange wraz ze swoim prezesem byli oskarżeni w postępowaniu FBI w sprawie spisku mającego na celu wykorzystanie środków łączności do przesyłania zakładów w handlu międzystanowym lub zagranicznym. Oskarżonym postawiono zarzuty obierania za cel klientów w Stanach Zjednoczonych i zapraszania ich do obstawiać zakłady w firmie za pośrednictwem bezpłatnej rozmowy telefonicznej lub Internetu). Chociaż spółka Antiguan znajdowała się poza jurysdykcją sądu, prezydent był obywatelem USA i dlatego mógł zostać postawiony przed amerykańskim sądem karnym.

3. Teoria osobowości biernej: Podczas gdy „teoria narodowości" zajmuje się narodowością przestępcy, „teoria osobowości biernej" dotyczy narodowości ofiary. W tym, co Cottim nazywa „dziedziną cyberkryminologii", dobrym przykładem założenia tej jurysdykcji jest sprawa, w której obywatel Rosji mieszkający w Czelabińsku w Rosji został skazany przez sąd w Hartford Connecticut za włamanie do komputerów w Stanach Zjednoczonych

4. Teoria ochrony: „Teoria ochrony" Cottim (zwana także „zasadą bezpieczeństwa" i „teorią poszkodowanego forum") zajmuje się poszkodowanym interesem narodowym lub międzynarodowym, przypisując jurysdykcję państwu, które widzi, że jego interesy – krajowe lub międzynarodowe – są zagrożone z powodu akcji ofensywnej. Cottim uważa tę rzadko używaną teorię za mającą zastosowanie głównie do przestępstw takich jak fałszowanie pieniędzy i papierów wartościowych.

5. Teoria uniwersalności: W swojej ostatecznej teorii Cottim identyfikuje podejście uniwersalności oparte na międzynarodowym charakterze przestępstwa, pozwalającym (w odróżnieniu od innych) każdemu państwu na roszczenie sobie jurysdykcji w sprawie przestępstw, nawet jeśli przestępstwa te nie mają bezpośredniego wpływu na stwierdzenie Państwo. Chociaż teoria ta wydaje się mieć największy potencjał zastosowania w cyberprzestrzeni, istnieją dwa główne ograniczenia w dotychczasowym sposobie jej rozwijania. Pierwsze ograniczenie polega na tym, że państwo przejmujące jurysdykcję musi przetrzymywać oskarżonego w areszcie; po drugie, przestępstwo jest „szczególnie obraźliwe dla społeczności międzynarodowej". Chociaż podejście to, jak radzi Cottim, było stosowane w przypadku piractwa i handlu niewolnikami, istnieją znaczne praktyczne trudności w zdefiniowaniu parametrów podejścia uniwersalności nawet w konwencjonalnym kontekście, a możliwość rozszerzenia go na przestępstwa i działalność w cyberprzestrzeni nie została jeszcze zbadana.

Jeśli chodzi o konwencjonalne wyzwania eksterytorialne, metoda skupienia się na kluczowych elementach, takich jak narodowość sprawcy i położenie geograficzne zachowania przyczynowego lub wynikającej z niego szkody, zaowocowała skutecznymi ściganiem niektórych konwencjonalnych cyberprzestępców (i być może w ten sposób odstraszyła) -możliwość obrażania. Na przykład Cottim przytacza sprawę, w której dyrektor zarządzający CompuServe Information Services GmbH, obywatel Szwajcarii, został oskarżony w Niemczech o odpowiedzialność za dostęp – w Niemczech – do przedstawień zawierających przemoc, pornografię dziecięcą i zwierzęcą przechowywanych na serwerze CompuServe w Stany Zjednoczone. Sąd niemiecki uznał, że ma jurysdykcję wobec pozwanego, choć był on Szwajcarem, to mieszkał wówczas w Niemczech. Podejście sądu w Amtsgericht zostało skrytykowane jako nie tylko nadmiernie surowe, ale także niezrównoważone i trudno polemizować z Benderem, który twierdzi, że „należy zauważyć, że „stref wolnych od prawa" w Internecie nie można wypełnić takim orzeczeniem, jak to, ale potrzebują nowego podejścia opartego

na samoregulacji" . W niektórych przypadkach strony sporu wykorzystują również różnice jurysdykcyjne do argumentowania wagi sankcji lub zakresu swojej odpowiedzialności, szczególnie gdy sprawca z jednej jurysdykcji powoduje konsekwencje w innej. Dobrym niedawnym przykładem jest sprawa Klemis przeciwko Rządowi Stanów Zjednoczonych Ameryki [2013] All ER (D) 287, w której oskarżony z Wielkiej Brytanii rzekomo sprzedał heroinę dwóm mężczyznom w Illinois w USA. Jeden z mężczyzn następnie zmarł, a w chwili wydawania wyroku postawił pytania dotyczące tego, w jaki sposób różne ciała ustawodawcze w obu jurysdykcjach inaczej określiły wymogi dotyczące odpowiedniego aktu prawnego (czynu przestępczego) i mens rea (winnego stanu umysłu). Innym niedawnym przykładem tarć między jurysdykcjami jest sprawa Bloy i Another przeciwko Motor Insurers' Bureau [2013] EWCA Civ 1543. W tej sprawie kolizję drogową w Wielkiej Brytanii spowodował obywatel Litwy, który nie był wówczas ubezpieczony. Biuro Ubezpieczycieli Komunikacyjnych jest brytyjskim organem odszkodowawczym w rozumieniu odpowiedniej dyrektywy UE i było zobowiązane do wypłaty odszkodowania, jeżeli mieszkaniec Wielkiej Brytanii odniósł obrażenia w kolizji w innym państwie członkowskim spowodowanej przez nieubezpieczonego kierowcę. W takich przypadkach dyrektywa umożliwiła Prezydium wystąpienie o zwrot kosztów do odpowiedniego organu kompensacyjnego w innym państwie członkowskim. Jednakże zgodnie z prawem krajowym Litwy odpowiedzialność organu kompensacyjnego została ograniczona do kwoty 500 tys. euro. Biuro argumentowało, że jego odpowiedzialność za zapłatę na rzecz ofiary powinna być ograniczona litewskim prawem krajowym, mimo że do kolizji doszło na angielskiej drodze. Wyraźnie pojawiają się wyzwania związane z nieuprawnionym dostępem i wykorzystaniem danych; podobnie jak wyzwania jurysdykcyjne dotyczące umiejscowienia inicjatorów i konsekwencji. Należy je jednak rozumieć w kontekście znacznie bardziej szkodliwych i prawdziwie wirusowych zagrożeń, takich jak ataki typu „odmowa usługi", złośliwe oprogramowanie, szpiegostwo danych i to, co Cottim nazywa „strasznym słowem" „cyberterroryzmu", które obecnie zostało formalnie przyjęte przez wiele osób. organy ścigania, politycy i komentatorzy. Rzeczywistość jest taka, że przy odpowiedniej wiedzy i motywacji nastolatek z laptopem może zmieniać daty przydatności do spożycia produktów spożywczych w pakowalni na drugim końcu świata lub sterować systemem centralnego ogrzewania sąsiada - podłączony do domu, aby się przegrzał lub wprawił sygnalizację świetlną w odległym mieście w szał. Dalsza rzeczywistość jest taka, że konwencjonalne konstrukcje stanowienia prawa w krajach prawa zwyczajowego wraz z powiązanymi z nimi praktykami egzekwowania prawa nie zapewnią odpowiedzi na te zagrożenia i ryzyko, a nawet na podstawowe elementy, takie jak „miejsca zbrodni" i „miejsca zbrodni" sprawcy" nie są już adekwatne w nowej granicy cyberprzestrzeni. Jednak nie tylko dominacja i manipulacja cyberprzestrzeni przez przestępców budzą zaniepokojenie opinii publicznej. Następstwa ujawnień Edwarda Snowdena na temat natrętnego szpiegostwa rządowego pokazały, że prywatni użytkownicy uważają cyberprzestrzeń za potencjalnie niebezpieczne miejsce nie tylko ze strachu, że staną się ofiarami przestępczości na odległość. Istnieje również realna obawa, że środowisko technologiczne pozwala agencjom państwowym działać w wysoce inwazyjny, a jednocześnie anonimowy i niezrozumiały sposób, co skłoniło dyrektorów generalnych niektórych wiodących na świecie firm informatycznych do napisania listu otwartego do Prezydenta Stanów Zjednoczonych, domagającego się reformy nadzór cyberprzestrzeni oparty na szeregu nadrzędnych zasad, które gwarantują swobodny przepływ informacji, a jednocześnie ograniczają władzę rządową i nakładają znaczny stopień nadzoru. Jaka jest zatem skala wyzwania, jakie stanowi ten amorficzny konstrukt cyberprzestrzeni?

WIELKOŚĆ WYZWANIA

Rząd Wielkiej Brytanii szacuje populację cyberprzestrzeni na ponad 2 miliardy. Chociaż nie znamy dokładnie częstotliwości ani czasu trwania, oznacza to, że jedna trzecia populacji Ziemi odwiedza cyberprzestrzeń, a oczekuje się, że w ciągu następnej dekady dołączą do niej kolejne miliardy,

wymieniając ponad 8 bilionów dolarów w handlu internetowym Według komisarza policji londyńskiego City „cyberne" oszustwa (ogólnie przestępstwa nieuczciwości popełniane przy użyciu sieci komputerowych) kosztują Wielką Brytanię 27 miliardów funtów rocznie, podczas gdy „cybernaruszenie" (prawdopodobnie polegające na nieuprawnionej infiltracji prywatnej lub publicznej sieci komputerowej) odnotowuje 93% małych i średnich przedsiębiorstw w Wielkiej Brytanii w 2013 r., co oznacza wzrost o 87% w porównaniu z rokiem poprzednim. Pomijając pewne szczególne cechy kryminologiczne charakterystyczne dla przestępstw popełnianych w cyberprzestrzeni (takie jak brak jakiegokolwiek prawdziwego motywu, który skłoniłby kogokolwiek – ofiary indywidualne, korporacyjne lub ich dostawców usług internetowych – do zgłaszania przestępstw obejmujących oszustwo), podstawowym wyzwaniem stojącym przed nami obecnie wydaje się być tym, jak uporać się z koncepcją cyberprzestrzeni – tętniącej życiem, odpornej, bezpiecznej lub innej. Po oddzieleniu cyberprzestępczości od przestępczości wykorzystującej cyberprzestępczość w taki sam sposób, w jaki moglibyśmy oddzielić przestępczość w sieci transportowej od przestępczości, w której sieć transportowa jest jedynie czynnikiem umożliwiającym, z pewnością musimy zacząć traktować cyberprzestrzeń taką, jaka jest: odrębny wymiar społeczno-przestrzenny w którym ludzie decydują się nie tylko na komunikację, ale także na zamieszkiwanie, handel, utrzymywanie kontaktów towarzyskich i kultywację; tworzyć własność intelektualną, generować bogactwo ekonomiczne, rozpoczynać i kończyć relacje; żerować, walczyć i prosperować; leczyć i szkodzić. Tak postrzegana cyberprzestrzeń to kolejny kontynent, rozległy, realny i wirtualny, posiadający odrębną jurysdykcję wymagającą własnej konstytucji i systemu prawnego, własnych agentów i praktyk egzekwowania prawa. Dyrektor ds. wsparcia operacyjnego policji w Sekretariacie Generalnym Interpolu, Michael O'Connell, porównał ruch w cyberprzestrzeni z „2 miliardami pasażerów na całym świecie". Rzeczywistość jest taka, że cyberprzestępcy poruszają się po wirtualnym świecie bez granic z niemal niezmierzoną szybkością, niemal zerowymi kosztami i niemal całkowitą anonimowością. Wyzwanie, jakim jest rozwiązanie problemu bezpieczeństwa cybernetycznego, wykracza daleko poza zwykłą standaryzację naszych ram prawnych. Rząd Wielkiej Brytanii uznał również, że „bez skutecznego bezpieczeństwa cybernetycznego narażamy naszą zdolność do prowadzenia działalności gospodarczej i ochrony cennych aktywów, takich jak nasza własność intelektualna, na niedopuszczalne ryzyko". W raporcie zleconym przez rząd Wielkiej Brytanii firma Price Waterhouse Coopers szacuje, że istnieje ponad 1000 różnych globalnych publikacji określających standardy cybernetyczne. Co więcej, ich ocena sytuacji w zakresie standardów w organizacjach wydawała się niejednolita i niekompletna. Chociaż ogólnie stwierdzono, że świadomość zagrożeń cyberbezpieczeństwa i przywiązywana do nich waga są wysokie, wysiłki mające na celu ograniczenie ryzyka cyberbezpieczeństwa różnią się znacznie w zależności od wielkości organizacji i jej sektora. Z raportu wynika, że tylko 48% organizacji wdrożyło nowe zasady mające na celu ograniczenie zagrożeń dla bezpieczeństwa cybernetycznego, a tylko 43% przeprowadziło oceny ryzyka dla bezpieczeństwa cybernetycznego i analizę skutków w celu ilościowego określenia tych zagrożeń. Z raportu wynika również, że 34% organizacji, które zakupiły certyfikowane produkty lub usługi, zrobiło to wyłącznie po to, aby w rezultacie osiągnąć zgodność. Chociaż autorzy wyraźnie wskazują, że ankieta internetowa dotarła do około 30 000 organizacji, dała około 500 odpowiedzi, nie wszystkie z nich były kompletne. Niemniej jednak obraz, jaki wyłania się z raportu, przedstawia fragmentaryczną i niestandardową reakcję na globalne zagrożenie

ODPOWIEDŹ

Oprócz rozciągania i przeróbki zasad prawnych, takich jak jurysdykcja i strategie wydawania, wprowadzono kilka kluczowych odpowiedzi na wyzwania związane z cyberprzestępczością i przestępczością wykorzystującą cyberprzestępczość. Na przykład niedawno zgłoszono, że Metropolitan Police Service znacznie powiększyła swoją jednostkę ds. przestępczości elektronicznej do 500 funkcjonariuszy w odpowiedzi na zagrożenie, że „cyberprzestępczość" stanie się zagrożeniem dla

bezpieczeństwa narodowego pierwszego stopnia. Jest to spójne z reakcjami mającymi wpływ na całą brytyjską społeczność organów ścigania. Ustawa o reformie policji i odpowiedzialności społecznej z 2011 r. — ustawodawstwo, które stworzyło wybieranych komisarzy policji i komisarzy ds. przestępczości — również wprowadziła koncepcję strategicznych wymagań policyjnych (SPR). SPR jest publikowany przez Ministra Spraw Wewnętrznych i określa zagrożenia krajowe wymagające skoordynowanej lub zbiorczej reakcji, w ramach której gromadzone są zasoby różnych sił policyjnych; dotyczy wszystkich sił policyjnych w Anglii i Walii i odnoszą się do niego inne organy ścigania w całej Wielkiej Brytanii. SPR określa, w jaki sposób siły policyjne i ich organy zarządzające często muszą współpracować inter se, a także z innymi partnerami, agencjami krajowymi lub porozumieniami krajowymi, aby zapewnić skuteczne i skuteczne zwalczanie takich zagrożeń. SPR zawiera pięć obszarów działalności i zagrożeń, które są objęte oceną ryzyka bezpieczeństwa narodowego, jeśli znajdują się na poziomie ryzyka pierwszego lub drugiego poziomu. To są:

• Terroryzm (Poziom pierwszy)

• Inne sytuacje kryzysowe wymagające zbiorowej reakcji ponad granicami sił policyjnych

• Przestępczość zorganizowana (poziom drugi)

• Zagrożenia porządku publicznego lub bezpieczeństwa publicznego, którym nie może zaradzić pojedyncza policja działająca samodzielnie

• Incydent cybernetyczny na dużą skalę (Poziom pierwszy), obejmujący ryzyko wrogiego ataku na cyberprzestrzeń ze strony innych państw

SPR uznaje, że obszary te mogą w znacznym stopniu się pokrywać. Na przykład w incydent cybernetyczny może być zaangażowany istotny element przestępczości zorganizowanej i odwrotnie. Wszyscy wybrani komisarze policji i komisarze ds. kryminalnych oraz ich przełożeni muszą uwzględniać SPR w swoich planach i ustaleniach operacyjnych. Jest to ważny obowiązek prawny z powodów omówionych poniżej. Po określeniu tych kluczowych zagrożeń dla bezpieczeństwa narodowego SPR nakłada na organy policji obowiązek posiadania odpowiednich rozwiązań zapewniających, że ich lokalne zasoby będą w stanie zapewnić wymagane:

Pojemność (Capacity)

Zdolność (Capability)

Konsystencja (Consistency)

Łączność (Connectivity)

Wkład (Contribution)

do wysiłku narodowego („pięć „C”).

Biorąc pod uwagę trudności prawne i praktyczne analizowane poniżej, wątpliwy jest stopień, w jakim lokalne organy policji są w stanie w znaczący sposób spełnić te kryteria w odniesieniu do „incydentów cybernetycznych” – niezależnie od tego, czy „w” czy w cyberprzestrzeni. Na przykład, choć stosunkowo prostym zadaniem jest ocena potencjału i możliwości grupy lokalnych sił policyjnych (nawet tak dużej, jak policja metropolitalna) w zakresie zwalczania zakłóceń porządku publicznego na dużą skalę oraz zmierzenie powiązania ich zasobów przygotowując się na takie wydarzenie, znacznie trudniej jest wykazać, że te same siły spełniają pięć wymagań C (zdolność, łączność itd.) wymaganych do zrozumienia i zareagowania nawet na wysoce zlokalizowany incydent cybernetyczny, a tym bardziej na sponsorowany cyberatak przez inne państwo. To również jest ważne, ponieważ sądy w Wielkiej

Brytanii zinterpretowały wyrażenie „uwzględniać" politykę rządu w ten sposób, że organy publiczne, na których spoczywa taki obowiązek, muszą przede wszystkim właściwie rozumieć tę politykę. Jeżeli polityka rządu, którą organ publiczny musi wziąć pod uwagę, nie zostanie właściwie zrozumiana przez ten organ, ma to taki sam skutek prawny, jak gdyby organ ten w ogóle jej nie uwzględniał. Co więcej, jeśli organ publiczny zamierza odstąpić od polityki rządu, na którą musi „wziąć pod uwagę", organ ten musi podać jasne powody takiego działania, tak aby ludzie wiedzieli, dlaczego i na jakiej podstawie odstępuje. Chociaż UE może posiadać szereg ustaleń zobowiązujących państwa członkowskie do powiadamiania ich o „incydentach", które „wydają się mieć związek z cyberszpiegostwem lub atakiem sponsorowanym przez państwo" i odwoływać się do odpowiednich części klauzuli solidarności UE, istnieje niewiele dowodów że większość okręgów policyjnych byłaby w stanie śmiało przedstawić takie stwierdzenie, niezwłocznie lub w ogóle. Quaere: W jakim stopniu wszystkie agencje policyjne w Anglii i Walii, których to dotyczy, są w stanie wykazać, że właściwie zrozumiały zagrożenie cyberatakiem w kontekście SPR? Jeśli odpowiedź na to pytanie będzie inna niż bez zastrzeżeń „tak", dobrym rozwiązaniem może być wystosowanie powiadomienia w tej sprawie do swoich społeczności i interesariuszy.

WNIOSEK

Walka z przestępczością komputerową zasadniczo skupiała się na fizycznej obecności osób kontrolujących zdalną działalność, czerpiących z niej korzyści lub cierpiących z jej powodu – skupiała się na danych wejściowych i wyjściowych. Unia Europejska zaproponowała dyrektywę nakładającą na państwa członkowskie obowiązek zapewnienia minimalnego poziomu zdolności, wraz z zespołami reagowania na incydenty komputerowe (CERT) oraz ustaleniami dotyczącymi skutecznej koordynacji „sieci i systemów informatycznych". Jednocześnie Konwencja Budapeszteńska obowiązuje od prawie dziesięciu lat, aby zapewnić wielu krajom sygnatariuszom (w tym Stanom Zjednoczonym) model do opracowywania krajowych przepisów dotyczących „cyberprzestępczości", a powiązana branża bezpieczeństwa cybernetycznego jest ogromna i rozwijająca się. Ale czy nie istnieje pilna potrzeba zajęcia się tym, co dzieje się w samej cyberprzestrzeni? Korzystanie z istniejących teorii jurysdykcji prawdopodobnie nie wystarczy; potrzebne jest nie częściowe zastosowanie niektórych przepisów dotyczących sytuacji pozacyberprzestrzennych, dostosowanych do pewnych konsekwencji poza cyberprzestrzenią. Kontynuując stosowanie tradycyjnego podejścia kryminologicznego do innowacji technologicznych w kontekście cyberprzestrzeni, proponuje się raczej oddzielenie przestępczości, która ma miejsce w sieci transportu podziemnego, od tej, w której sprawca korzysta z londyńskiego metra w celu ułatwienia popełnienia przestępstwa. W pierwszej sytuacji otoczenie jest kluczowym elementem przestępstwa, w drugiej stanowi wybraną część szerszego sposobu działania, a sprawca równie dobrze mógł wybrać autobus, taksówkę lub udać się na piechotę. od miejsca ich przestępstwa. Na tym polega podstawowa różnica między przestępstwem wykorzystującym cyberprzestrzeń a przestępstwem w cyberprzestrzeni. Kontrolowanie wyjść i wejść nigdy nie będzie pełną ani nawet zadowalającą odpowiedzią na to drugie. Oprócz względów praktycznych i orzeczniczych zaczynają wyłaniać się także ważne imperatywy polityczne. Na przykład indyjski minister telekomunikacji i IT Kapil Sibal zapewnił niedawno, że w cyberprzestrzeni powinna panować „odpowiedzialność i odpowiedzialność" w taki sam sposób, jak w stosunkach dyplomatycznych:

Jeżeli dochodzi do naruszenia cyberprzestrzeni, a jego przedmiotem są Indie, ponieważ ma ono wpływ na Indie, wówczas jurysdykcja powinna przypadać Indiom. Na przykład, jeśli mam ambasadę w Nowym Jorku, wszystko, co dzieje się w tej ambasadzie, jest terytorium Indii i obowiązuje tam prawo indyjskie.

Aby to podejście wykraczało poza konwencjonalne podejścia jurysdykcyjne omówione powyżej, wymagałoby zupełnie nowego zestawu procesów, procedur i umiejętności; wymagałoby to więcej niż tylko opublikowania zestawu uzgodnionych standardów lub uzgodnionego przepisu na ustawodawstwo krajowe. Uważa się, że potrzebna jest nowa obecność w cyberprzestrzeni, wyspecjalizowana cyber siła, która zajmie się tym, co dyrektor generalny Narodowej Agencji ds. Przestępczości, Keith Bristow, nazywa „przestępczością cyfrową". Być może potrzebny jest nie nowy sposób nałożenia naszych konwencjonalnych zasobów i technik egzekwowania prawa na cyberprzestrzeń lub nowy sposób rozszerzenia naszych dwuwymiarowych konstrukcji jurysdykcji, aby dopasować je do wielowymiarowego świata, ale nowa fala zasobów cybernetycznych… cyberkonstabli" – do patrolowania i nadzorowania społeczności cybernetycznych przyszłości. Jednakże biorąc pod uwagę nasze globalne doświadczenie w zakresie sposobów, w jakie niektóre agencje państwowe działały w cyberprzestrzeni, w erze post-Snowdenowskiej ta odwieczna kwestia demokratycznego egzekwowania prawa „quis cusodiet" jest tak samo niezmiennie ważniejsza od cyberpolicji, jak ma to miejsce w każdym środowisku analogowym spotykać się z kimś.

Definicje cyberterroryzmu

WSTĘP

Termin cyberterroryzm pojawił się po raz pierwszy w połowie lat osiemdziesiątych. Według kilku źródeł Barry C. Collin, starszy pracownik naukowy Instytutu Bezpieczeństwa i Wywiadu w Kalifornii, zdefiniował ówczesny cyberterroryzm jako „zbieżność cybernetyki i terroryzmu" – co jest elegancką i prostą definicją. Definicja ta nie była jednak na tyle szczegółowa, aby można było dokonać wyraźnego rozróżnienia między pojęciami takimi jak cyberprzestępczość, cyberaktywizm (haktywizm) i cyberekstremizm. Pierwsze przebłyski cyberrewolucji, kolejnej fali po rewolucji przemysłowej, były szeroko omawiane w latach osiemdziesiątych . Nic więc dziwnego, że w tej dekadzie podjęto pierwsze dyskusje na temat cyberterroryzmu i terroryzmu w przewidywanym nowym świecie. W latach dziewięćdziesiątych debata na temat cyberrewolucji rozszerzyła się na takie zjawiska, jak wojna informacyjna i wyższość informacyjna. To ponownie wzmocniło pogląd, że terroryści mogą wkroczyć do cyberprzestrzeni i wykorzystać ją jako domenę działań terrorystycznych. Pomysł ten znalazł odzwierciedlenie w Krajowej Radzie ds. Badań Naukowych (1991): „Terrorysta jutra może być w stanie wyrządzić więcej szkód za pomocą klawiatury niż bomby". W efekcie cyberterroryzm znalazł się na liście poważnych zagrożeń narodowych dla Stanów Zjednoczonych. Nieoczekiwany wynik bitwy o Mogadiszu w 1993 r. pokazał potencjał asymetrycznego zagrożenia o poważnym wpływie politycznym, a wraz z niepewnością milenijną jeszcze bardziej zwiększyła niepewność społeczną co do możliwego zagrożenia dla społeczeństwa ze strony cyberprzestrzeni inicjowanego przez terrorystów . Od tego czasu termin cyberterroryzm pomógł w tworzeniu dramatycznych i przyciągających uwagę nagłówków gazet. W rozdziale tym stwierdza się następnie, że w oparciu o definicję opracowaną na podstawie poprzednich definicji świat nie doświadczył jeszcze prawdziwego zdarzenia mającego wpływ na cyberterroryzm.

Zamieszanie wokół cyberterroryzmu

Na przestrzeni tysiącleci wielu ekspertów z różnych dziedzin wykazało zainteresowanie potencjałem cyberterroryzmu. Z tego powodu zaproponowano szeroką gamę umiarkowanych definicji cyberterroryzmu, szczególnie w okresie od 1997 do 2001 roku. Przyczyna niespójności definicji wynika z faktu, że ich pochodzenie leży w zupełnie różnych dziedzinach eksperckich, takich jak egzekwowanie prawa , badania międzynarodowe, zwalczanie terroryzmu, bezpieczeństwo informacji i operacje informacyjne. Prasa popularna powoduje jeszcze większe zamieszanie. Poniżej omówimy kilka z tych definicji, aby pokazać przykłady zamieszania. Z tych definicji możemy wyprowadzić elementy

obejmującej definicję cyberterroryzmu, jak podano w poniższych sekcjach. Z definicji wynika także, że nie miał jeszcze miejsca żaden akt cyberterroryzmu. W 1997 roku Mark Pollitt z FBI zdefiniował cyberterroryzm jako:

Z premedytacją, motywowany politycznie atak na informacje, systemy komputerowe, programy komputerowe i dane, którego skutkiem jest przemoc wobec celów niewalczących ze strony grup lokalnych lub tajnych agentów (FBI, 1997).

W tej definicji nacisk położony jest na to, co i kogo. Brakuje terrorystycznego aspektu strachu i stosowania groźby ataku. Kombatanci są wykluczeni, co odzwierciedla mandat FBI, ale nie pomogło w opracowaniu kompleksowej definicji. W 2004 roku FBI na nowo zdefiniowało cyberterroryzm jako:

Czyn przestępczy popełniony przy użyciu komputerów i możliwości telekomunikacyjnych, skutkujący przemocą, zniszczeniem i/lub zakłóceniem usług, którego zamierzonym celem jest wywołanie strachu poprzez wywołanie zamieszania i niepewności w danej populacji, w celu wywarcia wpływu na rząd lub populacji w celu dostosowania się do określonego programu politycznego, społecznego lub ideologicznego (FBI, 2004).

Definicja ta koncentruje się na przestępczości czynu, środkach tradycyjnych technologii informacyjno-komunikacyjnych (ICT), zamierzonym wpływie i motywacji. W definicji brakuje szerszego spojrzenia na nowsze ICT, takie jak te wbudowane na przykład w infrastrukturę krytyczną, samochody i sprzęt medyczny. Wpływ w definicji ogranicza się jedynie do wzbudzania strachu i niepewności, podczas gdy terroryzm może mieć na celu zakłócanie gospodarki, środowiska, stosunków międzynarodowych, a także procesów zarządzania rządowego. W 2000 roku ekspert ds. bezpieczeństwa informacji, profesor Dorothy E. Denning, zdefiniowała cyberterroryzm jako:

atak, którego skutkiem jest przemoc wobec osób lub mienia lub przynajmniej wyrządza wystarczającą szkodę, aby wywołać strach .

Definicja ta skupia się na możliwych skutkach cyberterroryzmu. Nie omawia się, dlaczego terroryści mieliby dokonać aktu cyberterroryzmu i w jaki sposób. Po 11 września na nowo zdefiniowała cyberterroryzm jako:

bezprawne ataki i groźby ataków na komputery, sieci i przechowywane w nich informacje, jeżeli mają na celu zastraszenie lub wywarcie nacisku na rząd lub jego obywateli w celu osiągnięcia celów politycznych lub społecznych .

Definicja ta wynika wyraźnie z punktu widzenia bezpieczeństwa informacji. Koncentruje się na integralności i dostępności informacji. Definicja ta nie obejmuje skutków fizycznych wynikających z dotkniętej warstwy cybernetycznej. W definicji nie ma również jasnego rozróżnienia od cyberaktywizmu (haktywizmu). W 2002 roku Amerykańskie Centrum Studiów Strategicznych i Międzynarodowych zdefiniowało cyberterroryzm jako:

Wykorzystanie narzędzi sieci komputerowych do zamknięcia krytycznej infrastruktury krajowej (takiej jak energia, transport, operacje rządowe) lub do wywarcia nacisku lub zastraszenia rządu lub ludności cywilnej.

Definicja ta jest nieprecyzyjna. Na przykład definicja ta sugeruje, że cyberterrorystą może być operator infrastruktury krytycznej, który zamyka (częścią) infrastruktury krytycznej ze względów technicznych lub bezpieczeństwa w swojej stacji operacyjnej. Jednocześnie haktywiści próbujący zaimponować decydentom rządowym również są cyberterrorystami i nie są nimi objęci. Kiedy zastanawiamy się nad nagłówkami prasowymi z ostatnich 25 lat, od razu staje się jasne, że każde nowe zaburzenie związane

z naszym cyberświatem jest określane przez prasę popularną jako „cyberterror". Z perspektywy czasu widać, że kilka lat później wydarzenie „cyberterrorystyczne" prawie nie jest pamiętane. Co najwyżej jest to uważane za prosty akt cyberprzestępczości lub aktywizmu. W przypadkach, gdy był to atak typu „odmowa usługi", ciągła przepustowość codziennych irytujących ataków na organizacje jest często uwzględniana powyżej zwykłego zdarzenia polegającego na wdrapaniu się na powierzchnię cybernetyczną, które w prasie zostało określone jako zdarzenie cyberterrorystyczne. Inne źródło nieporozumień wynika ze stosowania terminu „cyberterroryzm" w odniesieniu do wszelkiego wykorzystania działań w cyberprzestrzeni przez terrorystów i grupy terrorystyczne. Jest to połączenie cyberprzestrzeni jako możliwego celu i broni używanej przez terrorystów i grupy terrorystyczne z towarowymi usługami komunikacyjnymi, z których wszyscy korzystamy. Terroryści wykorzystują cyberprzestrzeń do dowodzenia i kontroli, globalnej wymiany i planowania informacji, zbierania funduszy i prób zwiększenia swojego wsparcia, społeczności, propagandy, rekrutacji i operacji informacyjnych , aby wpłynąć na opinię publiczną . Niektóre z tych zastosowań mogą zostać uznane przez rządy krajowe za przestępstwo, a nawet cyberprzestępczość, ale w świetle różnych krajowych systemów prawnych nie będą one uznawane za „terroryzm".

DEFINICJA CYBERTERRORYZMU

Jak omówiono w poprzedniej sekcji, pomiędzy poprzednią a wieloma innymi definicjami cyberterroryzmu widoczne są duże różnice. Niektóre z proponowanych definicji są ograniczone mandatem, a tym samym ograniczonym spojrzeniem na organizację; inne koncentrują się na konkretnych technologiach ICT, celach lub motywacjach aktorów. Potrzebna jest definicja, która jasno oddzieli cyberterroryzm od zwykłej cyberprzestępczości, haktywizmu, a nawet cyberekstremizmu. Z powyższego jasno wynika, że elementami, które muszą stanowić część definicji, są:

• Kontekst prawny (zamiar, spisek, sama groźba lub działanie?)

• Cyberprzestrzeń wykorzystywana jako broń lub będąca celem

• Cel(e) złośliwego czynu, który obejmuje rodzaj przemocy o dalekosiężnych skutkach psychologicznych wobec docelowej grupy odbiorców

• Zamiar w połączeniu z celem długoterminowym (np. zmiana społeczna lub polityczna; wpływ na proces podejmowania decyzji politycznych), który kieruje terrorystą lub grupą terrorystyczną.

Jeśli chodzi o cyberprzestrzeń – systemy, sieci i informacje – jako broń lub cel, możemy wyróżnić cyberataki cyberterrorystów na (lub ich kombinację):

• Integralność informacji (np. nieuprawnione usunięcie, nieautoryzowane zmiany) powodująca utratę zaufania do ICT i społeczeństwa. Celem mogą być bazy danych o krytycznym znaczeniu dla społeczeństwa: dane osobowe, rejestracje pojazdów, własność nieruchomości oraz dokumentacja i rachunki finansowe.

• Poufność informacji. Naruszenia prywatności osobistej i poufnych informacji organizacji na dużą skalę mogą powodować zaburzenia społeczne, np. publikacja pełnej dokumentacji zdrowotnej osób zakażonych wirusem HIV w danym kraju może zapoczątkować serię molestowań i samobójstw. Odpowiedź rządu może naruszyć prywatność obywateli i skutkować wzmocnieniem zamierzonych celów terrorystycznych.

• Dostępność usług opartych na ICT za pomocą środków ICT, na przykład poprzez długotrwały atak typu „odmowa usługi", nieuprawnione zakłócenie systemów i sieci lub atak fizyczny lub elektromagnetyczny na centra danych i krytyczne elementy systemu ICT.

• Procesy oparte na ICT, które kontrolują procesy fizyczne w świecie rzeczywistym, np.: elektrownia jądrowa, rafineria, pojazdy i inne formy transportu, monitorowanie i kontrola stanu zdrowia, inteligentne sieci i inteligentne miasta (patrz rozdział 3 dotyczący nowych i pojawiających się zagrożeń).

Aby podać bardziej precyzyjną definicję cyberterroryzmu w oparciu o wszystkie zidentyfikowane wcześniej elementy, należy najpierw przyjrzeć się definicji terroryzmu, która będzie obejmować definicję cyberterroryzmu. Niestety nie ma ogólnie przyjętej międzynarodowej definicji terroryzmu, zob. na przykład Saul (2005).

Brytyjska ustawa o terroryzmie (UK, 2000) definiuje terroryzm jako:

Użycie lub groźba działania mające na celu wywarcie wpływu na rząd lub międzynarodową organizację rządową lub zastraszenie społeczeństwa lub części społeczeństwa; dokonane w celu popierania sprawy politycznej, religijnej, rasowej lub ideologicznej.

Polega lub powoduje:

• poważna przemoc wobec osoby;

• poważne szkody w mieniu;

• zagrożenie życia człowieka;

• poważne zagrożenie dla zdrowia i bezpieczeństwa publicznego; Lub

• poważne zakłócenia lub zakłócenia w systemie elektronicznym (brytyjska ustawa o terroryzmie z 2000 r.).

Co ciekawe, definicja ta uwzględnia także aspekt cybernetyczny. Definicja zawiera pewne słabe punkty, na przykład partia polityczna próbująca wpłynąć na rząd, aby przywrócił palenie w biurach poprzez uchylenie przepisów antynikotynowych, wiąże się z poważnym zagrożeniem dla zdrowia i bezpieczeństwa publicznego. Definicja ta stwierdza, że partia taka jest organizacją terrorystyczną.

W 2010 r. rząd Holandii zmienił definicję terroryzmu, aby dostosować definicję stosowaną przez swój wymiar sprawiedliwości do operacyjnej definicji swoich służb wywiadowczych. Jednocześnie rząd holenderski próbował dostosować się do definicji terroryzmu podanej przez Radę Europejską (2002) i Organizację Narodów Zjednoczonych. Holenderska definicja terroryzmu brzmi:

grożenie, przygotowywanie lub dokonywanie, z powodów ideologicznych, aktów poważnej przemocy wobec ludzi lub innych czynów mających na celu wyrządzenie szkody majątkowej mogącej wywołać zakłócenia społeczne, w celu wywołania zmiany społecznej, wywołanie atmosfery strachu wśród ogółu opinii publicznej lub wpływania na decyzje polityczne.

Jednak porównując część Wielkiej Brytanii uznawaną za część dotyczącą skutków terrorystycznych z zdefiniowanymi gdzie indziej interesami narodowymi, „zniszczenie mienia” poniesione przez Wielką Brytanię wydaje się słabe. Holendrzy na przykład uważają „destrukcyjne szkody gospodarcze”, „poważne negatywne skutki dla bezpieczeństwa ekologicznego” oraz „poważną zmianę stabilności społecznej i politycznej” za elementy, które należy złagodzić ryzyko narodowe. Na podstawie powyższych rozważań terroryzm można prawdopodobnie lepiej zdefiniować jako:

Stosowanie, przygotowanie lub groźba działania, którego celem jest spowodowanie zmiany porządku społecznego, wytworzenie atmosfery strachu lub zastraszenia wśród (części) ogółu społeczeństwa lub wywarcie wpływu na podejmowanie decyzji politycznych przez rząd lub rząd międzynarodowy

organizacja; dokonane w celu popierania sprawy politycznej, religijnej, rasowej lub ideologicznej; i obejmuje lub powoduje:

• przemoc, cierpienie, poważne obrażenia lub śmierć osoby (osób),

• poważne szkody w mieniu,

• poważne zagrożenie dla zdrowia i bezpieczeństwa publicznego,

• poważna strata ekonomiczna,

• poważne naruszenie bezpieczeństwa ekologicznego,

• poważne naruszenie stabilności i spójności społecznej i politycznej narodu.

Z tego możemy wyprowadzić definicję cyberterroryzmu jako:

Stosowanie, przygotowanie lub groźba działania, którego celem jest spowodowanie zmiany porządku społecznego, wytworzenie atmosfery strachu lub zastraszenia wśród (części) ogółu społeczeństwa lub wywarcie wpływu na podejmowanie decyzji politycznych przez rząd lub rząd międzynarodowy organizacja; dokonane w celu popierania sprawy politycznej, religijnej, rasowej lub ideologicznej; poprzez wpływ na integralność, poufność i/lub dostępność informacji, systemów i sieci informatycznych lub przez nieuprawnione działania wpływające na kontrolę rzeczywistych procesów fizycznych w oparciu o technologie informacyjno-komunikacyjne; i obejmuje lub powoduje:

• przemoc, cierpienie, poważne obrażenia lub śmierć osoby (osób),

• poważne szkody w mieniu,

• poważne zagrożenie dla zdrowia i bezpieczeństwa publicznego,

• poważna strata ekonomiczna,

• poważne naruszenie bezpieczeństwa ekologicznego,

• poważne naruszenie stabilności i spójności społecznej i politycznej narodu.

CZY CYBERTERRORYZM KIEDYKOLWIEK WYSTĄPIŁ?

Stosując powyższą ostateczną definicję, istnieje jedynie ograniczony zestaw działań po połowie lat osiemdziesiątych, które mogły być bliskie prawdziwego aktu cyberterroryzmu. Pierwszy z nich miał miejsce podczas konfliktu w Górskim Karabachu około 1999 r. W następstwie niepotwierdzonych doniesień hakerzy zmodyfikowali grupy krwi w dokumentacji pacjentów w szpitalnej bazie danych, powodując ryzyko śmierci w wyniku otrzymania niewłaściwej transfuzji krwi. Drugim mogą być przygotowania w latach 2006–2007 grupy terrorystycznej powiązanej z Al-Kaidą, która planowała fizyczny atak na centrum telekomunikacyjne i centralę internetową Telehouse w obszarze London Docklands. W sierpniu 2006 r. potencjalne skutki społeczne takiego ataku zostały zademonstrowane poprzez niewielką przerwę w dostawie prądu w Telehouse. To zakłócenie techniczne spowodowało, że na kilka godzin przestały działać dziesiątki tysięcy stron internetowych i setki tysięcy klientów usług internetowych Plusnet . Można się jedynie domyślać, jakie skutki społeczne ewentualne długotrwałe zakłócenia mogą być wynikiem udanego ataku fizycznego, ale prawdopodobnie byłyby niewielkie, biorąc pod uwagę nadmiarowość systemów, sieci, informacji i usług objętych kopiami zapasowymi. Wszystkie inne zakłócenia w cyberprzestrzeni, które miały miejsce, zostały uznane przez firmę za akty cyberterroryzmu media informacyjne były (choć dla opinii publicznej i organizacji czasami niepokojące

i irytujące) zakłóceniami ICT spowodowanymi aktami cyberprzestępczości lub haktywizmu, lub okazały się mieć charakter techniczny.

WNIOSKI

Tu omówiono elementy wymagane do zakwalifikowania zdarzenia jako aktu cyberterrorystycznego oraz podano definicję cyberterroryzmu. Pomimo wielu nagłówków medialnych, na podstawie ukształtowanej powyżej definicji nie doszło jeszcze do jednoznacznego aktu cyberterroryzmu. Musimy jednak być przygotowani na akty cyberterroryzmu, ponieważ rosnące krytyczne zaufanie społeczne do ICT sprawi, że systemy i usługi ICT, a także wbudowane ICT staną się interesującym celem dla przyszłych terrorystów.

Nowe i pojawiające się zagrożenia cyberprzestępczością i terroryzmem

WSTĘP

Postęp w technologiach informacyjno-komunikacyjnych (ICT) nierozerwalnie niesie ze sobą nowe zagrożenia dla użytkowników końcowych i społeczeństwa. Jednakże ostatnie 40 lat pokazało, że wiele z tych samych błędów w projektowaniu i programowaniu bezpieczeństwa cybernetycznego powtarza się wielokrotnie, gdy ma miejsce nowy cykl innowacji i rozwoju ICT. Niestety, pozwala to przewidywać nowe awarie cyberbezpieczeństwa w kolejnym cyklu innowacji. Powodem jest to, że przy każdym nowym rozwoju ICT programiści i programiści nie biorą pod uwagę wcześniej zidentyfikowanych lekcji dotyczących bezpieczeństwa cybernetycznego. Dorastają w zupełnie nowych cyklach i środowiskach rozwoju ICT. Są nawet motywowani i zachęcani do ignorowania „starej szkoły" ICT. Po pierwsze, przedstawiono krótki przegląd historyczny niektórych zmian w zakresie zagrożeń cybernetycznych i powiązanej z nimi cyberprzestępczości. Stanowi to podstawę do następnej sekcji, w której omówiono poprzednie cykle innowacji ICT, wskazano powtarzające się awarie w zakresie bezpieczeństwa cybernetycznego wraz z późniejszym wprowadzaniem poprawek i naprawami, a także brak wyciągnięcia wcześniej zidentyfikowanych wniosków z zakresu bezpieczeństwa cybernetycznego. Przedstawiono część dotyczącą kwestii organizacyjnych, a w oparciu o wnioski wyciągnięte z przeszłości, ostatnia część omawia nowe innowacje ICT oraz przewiduje nowe i pojawiające się zagrożenia, a także ukryte stare zagrożenia w nowej strukturze, które mogą zostać wykorzystane przez cyberprzestępców, haktywistów , szpiedzy przemysłowi i państwa.

NIEKTÓRE HISTORYCZNE KAMIENIE MILOWE

Omawiając przestępczość związaną z cyberprzestępczością, Komisja Europejska (2007) wyróżniła trzy różne typy cyberprzestępczości, pomijając czwarty dodany poniżej:

1. tradycyjne formy przestępczości wykorzystującej cyberbezpieczeństwo dotyczą m.in. fałszerstw oraz oszustw sklepowych i e-rynkowych,

2. treści nielegalne, np. piracka muzyka i pornografia dziecięca,

3. przestępstwa charakterystyczne dla sieci elektronicznych, takie jak ataki hakerskie i ataki typu „odmowa usługi",

4. przestępstwa charakterystyczne dla cyberprzestrzeni, których celem jest wywarcie skutków dla systemów fizycznych i/lub świata fizycznego, np. cybermanipulacja systemami sterowania procesami w sieci przesyłu gazu powodująca pęknięcie rurociągu i późniejsze eksplozje.

Wiele osób uważa obecnie, że cyberprzestępczość jest nowym problemem. Jest odwrotnie, co pokazują poniższe przykłady:

• Według DHS (2014): „Począwszy od 1970 r. i przez trzy lata, główny kasjer oddziału nowojorskiego Union Dime Savings Bank w Park Avenue manipulował informacjami o koncie w systemie komputerowym banku, aby zdefraudować ponad 1,5 miliona dolarów z setek kont klientów." Od tego czasu pojawiło się wiele innych rodzajów cyberprzestępstw (np. fałszerstwa i oszustwa).

• Chociaż pierwsze replikujące się kody komputerowe opracowano w latach 60. XX wieku, dopiero w 1971 r. Bob Thomas opracował wirusa Creeper, który infekował inne systemy w Arpanecie. Choć niechętnie uruchamiał kod komputerowy na systemach należących do innej organizacji, jego „eksperyment" nie był wówczas jeszcze uważany za przestępstwo.

• Na początku 1977 r. osoba mająca dostęp do poufnych informacji w ciągu weekendu ukradła setki oryginalnych taśm komputerowych i ich kopie zapasowe z centrum komputerowego i magazynu kopii zapasowych firmy z branży chemicznej o nazwie ICI. Próbował wyłudzić ICI i zażądał 275 000 funtów szterlingów . Po zatrzymaniu sprawcy nagłówek gazety głosił: „Kradzież danych komputerowych ICI wyznacza nową erę przestępczości" .

• 2 listopada 1988 roku Robert T. Morris wypuścił w Internecie pierwszego robaka komputerowego, który zainfekował tysiące systemów. W 1990 roku Morris został skazany na podstawie ustawy o oszustwach i nadużyciach komputerowych z 1986 roku. Został skazany na trzy lata więzienia w zawieszeniu, 400 godzin prac społecznych i grzywnę w wysokości 10 000 dolarów ,

• W 1994 r. rosyjscy hakerzy dokonali 40 przelewów na łączną kwotę ponad 10 milionów dolarów z Citybank na konta bankowe w Finlandii, Rosji, Niemczech, Holandii, Stanach Zjednoczonych, Izraelu i Szwajcarii. Odzyskano całą kwotę z wyjątkiem 400 tys. dolarów. Sprawa ta pokazała, że cyberprzestępczość może skutkować nieautoryzowanymi transferami dużych kwot pieniędzy.

• W 1995 r. miały miejsce pierwsze próby phishingu.

• W 1997 roku powstał Electronic Disturbance Theatre (EDT). EDT stworzyło narzędzia do tworzenia elektronicznej wersji sesji sit-in w Internecie. 10 kwietnia 1998 r. ich narzędzie Floodnet zostało wykorzystane przez protestujących z wielu krajów do przeprowadzenia ataków typu „odmowa usługi" na stronę internetową Prezydenta Meksyku, a później na Biały Dom .

• W styczniu 1998 niezadowolony operator systemu zdalnie manipulował systemem SCADA elektrowni węglowej, wprowadzając go w tryb awaryjny i usunął oprogramowanie systemu SCADA.

• W 2005 r. celowo włamano się do systemu klimatyzacji w centrum komputerowym europejskiego banku. Temperatura w pomieszczeniu komputerowym powoli rosła, powodując wyłączenie wszystkich usług systemu komputerowego.

• W 2006 roku uruchomiono Rosyjską Sieć Biznesową (RBN). Wkrótce po powstaniu RBN stał się centralnym punktem oferującym narzędzia i usługi cyberprzestępcze w zakresie spamu, phishingu, trojanów i nie tylko.

• W lipcu 2010 r. powszechnie wiadome stało się istnienie wykrytego miesiąc wcześniej robaka systemu kontroli procesów Stuxnet. Celem projektu Stuxnet były w szczególności systemy kontroli procesów firmy Siemens w zakładzie wzbogacania uranu w Natanz w Iranie. Efektem tego była ukryta cybotyzacja kontroli prędkości ultrawirówek, co spowodowało ekstremalne zużycie.

• W 2011 roku brytyjskie agencje wywiadowcze zastąpiły stronę internetową zawierającą przepis na bomby przepisem na babeczki .

Jeśli pominiemy tradycyjne formy przestępczości i cyberprzestępczość o nielegalnej treści, powyższe przykłady ukazują cyberprzestępczość, haktywizm i (państwowe) operacje cybernetyczne, które wykorzystują słabości technologii, organizacji i ludzkich zachowań w zakresie ICT.

WNIOSKI W ZAKRESIE CYBERBEZPIECZEŃSTWA, NIE WYCIĄGNIĘTE Z POPRZEDNICH CYKLI INNOWACJI ICT

Od czasu ich powstania podczas II wojny światowej technologie informacyjno-komunikacyjne przeszły przez szereg cykli innowacyjnych. Nowe osiągnięcia ICT są przyjmowane przez przemysł i społeczeństwo w sposób odzwierciedlający model cyklu życia adaptacji technologii wymyślony przez Bohlena i Beala (1957). Pierwsi użytkownicy wdrażają innowacje. Po przełomie w zakresie innowacji ICT można zauważyć szybkie jej przyjęcie przez użytkowników i organizacje. Później następuje faza głównego nurtu, w której przezwyciężone zostały negatywne wady nowych innowacji. Wykazali to Venkatesh i inni oraz Venkatesh i Bala (2008), że przyjęcie innowacji ICT w dużej mierze wiąże się z łatwością obsługi i ich użytecznością dla użytkowników końcowych i ich organizacji; krótko mówiąc, przyjazna dla użytkownika funkcjonalność. Z ich ustaleń wynika, że aspekty cyberbezpieczeństwa innowacji ICT nie odgrywają żadnej roli. Po wielu cyklach innowacji ICT, przez które przeszliśmy, można było oczekiwać, że wymogi dotyczące bezpieczeństwa cybernetycznego wysuną się na pierwszy plan, ale oczywiście tak nie jest. Głównym powodem jest to, że z wcześniejszych cyklów innowacji ICT nie wyciągnięto żadnych wniosków w zakresie bezpieczeństwa cybernetycznego oraz że w kółko powtarzają się te same błędy, ponieważ siły napędowe innowacji ICT pochodzą ze społeczności zewnętrznych świadomych bezpieczeństwa. W latach sześćdziesiątych można było podejść do terminala i zacząć wpisywać nazwę użytkownika i hasło, aby się zalogować. Jeżeli nazwa użytkownika została wprowadzona błędnie, utworzono nowe środowisko użytkownika. Nazwy użytkowników i hasła były przechowywane w systemie w przejrzysty sposób, a plik haseł był często dostępny dla wszystkich użytkowników i programów systemowych. Z biegiem czasu poprawiono bezpieczeństwo dostępu do komputera i ograniczono liczbę prób hasła dla określonej nazwy użytkownika. Różnorodne problemy związane z bezpieczeństwem powodowane przez przepełnienia buforów i brak sprawdzania poprawności danych wejściowych, umożliwiających hakerom podniesienie poziomu dostępu do zasobów systemowych, zostały naprawione w systemach operacyjnych komputerów mainframe w połowie lat siedemdziesiątych. Jednak każda nowa wersja systemu operacyjnego zawierała ten sam typ błędów projektowych i kodowych w nowo opracowanej funkcjonalności i konieczne było załatanie tych dziur. W latach siedemdziesiątych istniejące i nowe firmy komputerowe spowodowały rewolucję ICT, wprowadzając minikomputery i komputery midi na poziomy działów organizacji. Ponieważ systemy te były przeznaczone do stosowania w małych środowiskach kooperacyjnych, ich zaletą była łatwość obsługi. Można podejść do systemu, zrestartować goi uruchamiać swoje programy bez żadnych zabezpieczeń komputera innych niż fizyczny dostęp do pomieszczenia. Korzystanie z wielu użytkowników zostało dodane w uproszczony sposób, biorąc pod uwagę aspekt bezpieczeństwa komputera. Na przykład oryginalny plik UNIX/etc/passwd był czytelny dla wszystkich. Pokazywał nazwy użytkowników i powiązane z nimi jednokierunkowo zaszyfrowane hasła oraz losową wartość soli. Proces szyfrowania jednokierunkowego miał zapewnić silne bezpieczeństwo dostępu do systemu, gdyż był to proces nieodwracalny. Twierdzenie było słuszne; jednakże, ponieważ proces szyfrowania był publiczny, hakerzy po prostu zastosowali brutalne przetwarzanie wszystkich permutacji znaków za pomocą algorytmu szybkiego hasła i porównali wynik z zaszyfrowanymi hasłami w pliku haseł. Nieszablonowe myślenie zaowocowało prostym sposobem ujawniania nazw użytkowników i haseł. Co więcej, prawo Moore'a powodowało coroczny wzrost szybkości przetwarzania, a tym samym

zmniejszało siłę hasła i czas potrzebny do złamania kombinacji nazwa użytkownika i hasło. Inne ówczesne systemy operacyjne umożliwiały użytkownikowi przerwanie programu mającego dostęp do pliku haseł i utworzenie zrzutu pamięci zawierającego wszystkie hasła w postaci zwykłego tekstu. Co więcej, podobnie jak we wcześniejszych komputerach mainframe, systemy operacyjne w komputerach mini i midi nie były zabezpieczone przed hakerami ze względu na złe praktyki kodowania, np. przepełnienie bufora i brak sprawdzania poprawności danych wejściowych. Zapewnienie nowej funkcjonalności w systemie operacyjnym miało pierwszeństwo przed bezpieczeństwem. Firma Apple wypuściła swój Apple II w 1977 r., a IBM wprowadził komputer osobisty (PC) w 1981 r. Początkowe systemy operacyjne dla dysków nie zapewniały żadnego zabezpieczenia poza bitem tylko do odczytu, chroniącym przed przypadkowym nadpisaniem pliku. W końcu były to komputery osobiste. Łączenie komputerów PC w sieć począwszy od 1983 r., np. za pomocą Novella i LAN Managera, z perspektywy czasu wymagało dodania do komputera większych zabezpieczeń. Wzrost liczby złośliwego oprogramowania, takiego jak wirusy i robaki, wymagał dodania dodatkowych środków bezpieczeństwa do platformy PC – która wcale nie miała być bezpieczna – i jej kolejnych systemów operacyjnych Windows. Główne błędy w bezpieczeństwie komputera stwierdzono w prostym dostępie do pamięci systemu i innych aplikacji, oczyszczaniu dysku, hasłach w sieci w postaci zwykłego tekstu i zbyt prostych implementacjach środków bezpieczeństwa, które dotyczyły starszych protokołów. Przykładem była dotychczasowa obsługa LAN Managera w Windows/NT, gdzie można było łatwo określić długość hasła użytkownika. W podobny sposób ochrona pliku haseł i systemu plików systemu Windows/NT opierała się na wewnętrznej ochronie systemu; nie powiodła się, gdy hakerzy od razu wykorzystali startową dyskietkę i aplikację opartą na systemie Unix, aby uzyskać dostęp do urządzenia systemowego. Dopiero po upływie tysiąclecia producenci tacy jak Microsoft zaczęli poważnie podchodzić do bezpieczeństwa swoich systemów operacyjnych dla serwerów. Jednocześnie wystąpiły błędy projektowe w procesach szyfrowania technologii sieci bezprzewodowych. Ważniejsze od odpowiedniego bezpieczeństwa cybernetycznego było wejście na rynek światowy i wprowadzenie nowej funkcjonalności. W szybkiej sekwencji bezprzewodowy protokół szyfrowania WEP okazał się niepewny, co spowodowało konieczność jego wymiany, która wkrótce potem została zerwana. Dlaczego projektanci systemów i programiści nie wyciągnęli wniosków z wniosków wyciągniętych z wcześniejszych błędów bezpieczeństwa? Dlaczego szukali tylko funkcjonalności? Równolegle ICT znalazły zastosowanie w automatyzacji procesów fizycznych i rzeczywistych, np. w przemyśle chemicznym, przełączaniu punktów kolejowych oraz sterowaniu sieciami energetycznymi, gazowymi i wodnymi. Protokoły kontroli nadzorczej i gromadzenia danych (SCADA) i podobne protokoły kontroli procesów zostały zaprojektowane bez wielu względów bezpieczeństwa. Oprogramowanie było zastrzeżone i nikt inny nie był zainteresowany jego szczegółowym działaniem. Sieci sterujące procesami były zamknięte, dlatego żaden haker nie miałby do nich dostępu. To samo hasło roota producenta, którego nie można było zmienić, było wbudowane w tysiące urządzeń na całym świecie. Przypadek Stuxneta był przykładem wykorzystania takiego błędu w projektowaniu i wdrażaniu . Projektowanie, implementacje protokołów SCADA i ochrona systemów w terenie nie nadążały za względami bezpieczeństwa przed ich polem. Łączność z sieciami publicznymi, łatwość telepracy i narzędzia takie jak Shodan, które identyfikują podatne na ataki systemy kontroli procesów podłączone do Internetu, tworzą ścieżki dostępu cyberprzestępców do infrastruktury krytycznej, takiej jak nasze sieci energetyczne (Averill i Luiijf, 2010). Zaledwie kilka lat temu testowanie sieci SCADA za pomocą narzędzia sieci ICT Nmap na dużej, niejednorodnej instalacji SCADA spowodowało awarię jednej trzeciej implementacji SCADA, a u kolejnej jednej trzeciej przerwanie komunikacji. Implementacje protokołu SCADA nie mogły poradzić sobie z nieoczekiwanym bajtem mniej więcej w odebranym pakiecie. Nie udało się zweryfikować odebranych pakietów protokołu, ponieważ implementacja oczekiwała łagodnego środowiska operacyjnego. To tylko niektóre przykłady innowacji i cykli adaptacyjnych ICT, w przypadku których projektanci systemów nie uwzględnili odpowiednio względów bezpieczeństwa, a programiści nie

wyciągnęli wniosków z wniosków z zakresu bezpieczeństwa cybernetycznego zidentyfikowanych we wcześniejszych cyklach adaptacyjnych ICT. Brak zabezpieczenia przed przepełnieniem bufora, brak sprawdzania poprawności danych wejściowych, brak czyszczenia wrażliwych informacji z buforów pamięci wielokrotnego użytku i osadzanie haseł systemowych to tylko niektóre przykłady błędów – a tym samym ukrywania starych zagrożeń – które powtarzają się w każdym cyklu innowacji ICT. Co więcej, sama nowa funkcjonalność ICT zapewnia nieznane backdoory. Na przykład nowe wersje płytek programowalnych sterowników logicznych (PLC) mogą obecnie zawierać wbudowane silniki internetowe. Często takie nowe płyty PLC zastępują stare, wadliwe płyty PLC. Nowa funkcjonalność umożliwia jednak dostęp do wszystkich funkcji PLC, chyba że ktoś poświęci czas na zablokowanie wpisu interfejsu internetowego.

ASPEKTY ORGANIZACYJNE, KTÓRE NIE NAUCZYŁY SIĘ Z POPRZEDNICH CYKLI INNOWACJI ICT

Kiedy przyjrzymy się stronie użytkownika końcowego, pierwsi użytkownicy innowacji ICT skupiają się głównie na wzroście efektywności, „fajnych" aplikacjach i łatwości użytkowania. Dlatego też pierwsi użytkownicy nagradzają producentów za to, że jako pierwsi na rynku pojawili się z nową, ciekawą funkcjonalnością, a nie za to, że kilka miesięcy później nie wprowadzili bezpiecznej, dobrze przetestowanej i mniej łatwej w użyciu innowacji opartej na wykorzystaniu ICT. Podczas głównej fazy cyklu innowacji ICT cały łańcuch (od producenta, sprzedawców i procesu nabycia u użytkownika końcowego, integratora systemów, instalatora, zewnętrznej organizacji zajmującej się konserwacją oraz codziennych operacji wykonywanych przez użytkownika końcowego) w dużej mierze zawodzi wziąć pod uwagę bezpieczeństwo cybernetyczne. Cały proces koncentruje się na zapewnieniu funkcjonalności, a nie na bezpiecznym środowisku operacyjnym. Zaczyna się od instrukcji instalacji producenta, która na pierwszych stronach omawia kompatybilność elektromagnetyczną, następnie gdzie podłączyć przewód zasilający i wtyczkę sieciową. Bezpieczeństwo, jeśli w ogóle, jest luźno udokumentowane na stronie 60. Zaskakujące może być nawet to, że czasami modyfikowano standardowe hasła producentów. Tam, gdzie technologie informacyjno-komunikacyjne są prawie ukryte jako część łatwiejszej funkcjonalności, ludzie czują się „nieświadomie niepewni".

POJAWIAJĄCE SIĘ ZAGROŻENIA

Z powyższego jasno wynika, że każdy kolejny cykl innowacji w zakresie ICT spowoduje nowe zagrożenia dla użytkowników końcowych i naszego społeczeństwa. Nowi, bystrzy wynalazcy ICT skupiają się na nowej funkcjonalności, zwiększonej wydajności i efektywności ludzi i organizacji oraz łatwości użytkowania. Brakuje im jakiejkolwiek historycznej wiedzy na temat poprzednich błędów w projektowaniu bezpiecznych rozwiązań i wcześniejszych wniosków wyciągniętych z dobrych praktyk kodowania. Oznacza to, że można przewidzieć pojawiające się zagrożenia, zwłaszcza w nowych obszarach ICT gdzie technologie informacyjno-komunikacyjne są głęboko osadzone w systemach funkcjonalnych. Często zagrożenia są starymi zagrożeniami ukrytymi w nowym wyglądzie. Umożliwią one cyberprzestępcom, haktywistom, cyberszpiegom i państwom przedostanie się do systemów opartych na ICT w nieautoryzowany sposób poprzez wykorzystanie:

• Niedociągnięcia w walidacji wartości wejściowych i elementów protokołu powodujące wykorzystanie nieoczekiwanych danych wejściowych jako otwieracza do puszek.

• Przepełnienia bufora umożliwiające podniesienie praw dostępu do poziomu administratora systemu (root).

• Man in the Middle atakuje kanały bliskiego pola i komunikacji bezprzewodowej.

• Dodanie samokonfigurujących się modułów sprzętowych do istniejącego systemu lub sieci, zapewniając backdoora.

• Znany publicznie producent i inne domyślne hasła.

• Nieskonfigurowana funkcjonalność zapewniająca backdoora.

• Nieświadomie niepewne zarządzane ICT, często osadzone w funkcjach, w których ludzie nie rozumieją, że zawierają ICT „pod maską".

Powyższe stanowi podstawę do zrozumienia dużej liczby kolejnych obszarów innowacji, w których wbudowane są technologie informacyjno-komunikacyjne i które mogą lub już zapewniają takie zagrożenia bezpieczeństwa i nowe drogi ataku. Wyróżniamy produkty masowe oraz istotne części sektorów krytycznych:

1. Nowoczesne życie: Coraz częściej telewizory cyfrowe są podłączane do sieci publicznych i Internetu. Wiele milionów telewizorów cyfrowych wyposażonych w zestawy szybkich silników przetwarzania wideo stanowi dla cyberprzestępców atrakcyjne źródło mocy obliczeniowej, umożliwiające na przykład włączenie ich do botnetów. Telewizja cyfrowa wkrótce stanie się platformą otwartą; zobacz na przykład rozwój Wyplay, który uczynił telewizor sercem multimediów, gier i innych nowych usług cyfrowych. Oczywiście nie ma jeszcze wyraźnych obaw co do zagrożeń bezpieczeństwa cybernetycznego telewizji cyfrowej, dopóki nie będzie za późno.

2. Nowoczesne życie: Domotyka (roboty domowe) wkrótce się rozwinie. Coraz większa liczba pierwszych użytkowników monitoruje i zmienia ustawienia temperatury w domu lub biurze zdalnie za pomocą smartfona. To dopiero pierwszy krok w zdalnym zarządzaniu domem. Nikt nie omawia zagrożeń cyberbezpieczeństwa związanych z tymi funkcjami.

3. Sektor zdrowia: Do monitorowania zdrowia ludzi wykorzystuje się coraz większą liczbę systemów opartych na ICT. Rozruszniki serca i pompy insulinowe zostały już zhakowane poprzez ich interfejs bezprzewodowy. Projektanci nie wzięli pod uwagę, że hakerzy mogą być zainteresowani manipulowaniem tak małymi systemami. Niewłaściwe ustawienia mogą jednak mieć skutki zagrażające życiu.

4. Już niedługo urządzenia monitorujące osobę z problemem zdrowotnym w trybie 24/7 zostaną podłączone do globalnej sieci za pomocą technologii mobilnych i bezprzewodowych. Jeśli na pierwszym miejscu postawiona zostanie funkcjonalność, zmanipulowane dane mogą spowodować automatyczne wezwanie wszystkich takich pacjentów w celu natychmiastowego zgłoszenia się do szpitala lub przepisanie pacjentom niewłaściwych dawek leków.

5. Monitorowanie stanu zdrowia i inny sprzęt medyczny w szpitalach jest coraz częściej podłączony do szpitalnej sieci szkieletowej. Ponieważ ochrona takich sieci może być słaba z powodów omówionych powyżej, pacjenci mogą być zagrożeni. Niemożliwe? W Holandii stwierdzono, że system monitorowania stanu zdrowia w szpitalnej izbie przyjęć jest członkiem sieci udostępniania muzyki Kazaa. Myślenie o cyberbezpieczeństwie wydaje się odradzane w pobliżu sprzętu medycznego. Czy dzieje się tak dlatego, że zagrożenie cybernetyczne podnosi tętno powyżej zdrowych granic? Właściwie jest to znowu zjawisko nieświadomie niebezpieczne.

6. Sektor finansowy: Chipy NFC (Near Field Communication) zapewniają nową formę identyfikacji i uwierzytelniania posiadacza smartfona. Stanowi to podstawę dla mikropłatności zbliżeniowych. Można się spodziewać, że cyberprzestępczość przejmie funkcję płatniczą poprzez zdalną manipulację smartfonem.

7. Sektor transportu: Nowoczesne samochody osobowe i ciężarowe zawierają ogromną ilość linii kodu w rosnącej liczbie elektronicznych jednostek sterujących (ECU). Według TRB (2012) są to dosłownie „komputery na kołach". Moduły kodu monitorują coraz większą liczbę czujników oraz sterują i aktywują wiele elementów wykonawczych, od hamulców po wycieraczki, od świateł po systemy zapobiegania kolizjom. Ponieważ wielu producentów opracowuje moduły, interfejsy między nimi muszą być otwarte. Zakładają, że jest to łagodne, zamknięte środowisko bez hakerów. Jeśli jednak nie masz tego jeszcze w swoim obecnym samochodzie, interfejsy sieciowe z sieciami publicznymi wkrótce zapewnią automatyczne usługi połączeń alarmowych, takie jak Assist i eCall. Wkrótce pojawią się inne usługi, co oznacza, że mobilne interfejsy do transmisji danych i mobilnego Internetu otworzą platformę samochodową na dwukierunkową komunikację. Cyberprzestępczość pojawi się we właściwym czasie. Należy pamiętać, że samochody mogą być wykorzystywane nie tylko do celów mobilności. Bateria może służyć jako tymczasowy magazyn energii produkowanej lokalnie, którą później można sprzedać do sieci elektroenergetycznej po znacznie wyższej cenie. Cyberprzestępcy mogą próbować zakłócać takie mechanizmy, aby wpłynąć na zachowanie sieci cyberfizycznej i ceny na rynku energii. Kolejną oczekiwaną innowacją stymulowaną przez władze może być włączenie klaksonów we wszystkich samochodach na wybranym obszarze. Mogą stanowić alternatywę dla trudnego w utrzymaniu, kosztownego i nieskutecznego na terenach wiejskich systemu syren alarmowych. Taka funkcjonalność może zainteresować hakerów, aby pokazać swoje możliwości (prawdopodobnie w środku nocy). Eksperymenty ze wspólnym i w pełni automatycznym prowadzeniem samochodów osobowych i ciężarowych prowadzone są w USA i UE. Bezpieczeństwo jest problemem, ale aspekty bezpieczeństwa ICT wydają się być mniej niepokojące pomimo wielu udanych ataków hakerskich na samochody w warunkach laboratoryjnych . Co więcej, nie zajęto się od razu zagrożeniem dla bezpieczeństwa systemu transportowego, np. ze strony złośliwego oprogramowania wpływającego na konkretny typ samochodu lub konkretny typ ECU. Po raz kolejny wcześniej zidentyfikowane wnioski nie są brane pod uwagę. Co więcej, mechanicy dokonujący aktualizacji oprogramowania samochodu podczas konserwacji nie zostali przeszkoleni w zakresie cyberbezpieczeństwa laptopów podłączanych do samochodów, co stanowi kolejne nieświadomie niebezpieczne ryzyko.

Kolejną innowacją jest cyfrowa kamera fotoradarowa nowej generacji. Będzie wymagało jedynie źródła zasilania. Szeroki zakres łączności przewodowej i bezprzewodowej umożliwia zdalny dostęp. Ponieważ kamerę można zdalnie zaprogramować do odczytu tablic rejestracyjnych i decydowania o tym, jakie informacje są zapisywane i przesyłane do zdjęcia w celu wystawienia mandatu, będzie to atrakcyjna funkcjonalna skrzynka dla hakerów, która będzie mogła siać spustoszenie, np. robić zdjęcie każdej taksówki niezależnie od jego prędkości w fazie zielonej.

8. Sektory energii i wody pitnej: Inteligentne liczniki są obecnie wdrażane w wielu krajach. Będą stanowić pierwszy inteligentny interfejs pomiędzy sieciami elektroenergetycznymi (takimi jak energia elektryczna, gaz, woda pitna) a lokalnym systemem użyteczności publicznej na terenie nieruchomości. Inteligentne liczniki umożliwiają odbiorcom mediów posiadanie bardzo elastycznych umów opartych na ekologiczności, porze dnia i dniu tygodnia. Jako prosumenci mogą w najlepszym momencie sprzedawać do sieci lokalnie wytwarzaną energię. Manipulowanie inteligentnymi licznikami zapewnia jednak model biznesowy dla (cyber)przestępców, jak wykazało już w USA KrebsOnSecurity (2012). Ponieważ inteligentne liczniki często wykorzystują technologie telekomunikacji mobilnej do komunikacji z sąsiednimi punktami koncentracji, a takich punktów koncentracji będzie wiele na danym obszarze lokalnym, inwestycje w technologię, a tym samym w bezpieczeństwo cybernetyczne, muszą być tanie. Z drugiej strony sprzęt musi działać latami i nie jest przygotowany na masową modernizację zabezpieczeń w przypadku, gdy złośliwe oprogramowanie lub inne awarie bezpieczeństwa cybernetycznego wpłyną na działanie inteligentnego licznika.

Niektóre inteligentne liczniki pozwalają na zdalne wyłączenie obsługi klienta. Cyberprzestępcy lub haktywiści mogą znaleźć sposób na wyłączenie usług użyteczności publicznej na dużą skalę, na przykład w celu wymuszenia przedsiębiorstwa użyteczności publicznej. Należy pamiętać, że w wielu krajach zdalne uruchamianie usług komunalnych w nieruchomości jest prawnie zabronione, ponieważ może to zagrozić bezpieczeństwu osób. Dlatego też rekonwalescencja po wydarzeniu na dużą skalę może zająć nawet kilka dni.

9. Inteligentne życie: Inteligentne urządzenia wkrótce będą częścią naszych domów. Inteligentna lodówka, zmywarka, pralka itp. zaczną komunikować się z inteligentną siecią i znajdą najbardziej ekologiczny lub najtańszy czas na wykorzystanie prądu i wody. Nawet inteligentne lodówki będą śledzić materiały eksploatacyjne i zamawiać produkty w lokalnym supermarkecie. Projekt takich urządzeń, których przewidywany czas życia wynosi co najmniej 15 lat, nie uwzględnia aktualizacji związanych z cyberbezpieczeństwem. Prawo Moore'a spowoduje jednak unieważnienie dowolnego mechanizmu ochrony kryptograficznej prawdopodobnie w połowie takiego życia. Przy słabym bezpieczeństwie inteligentne urządzenia mogą stać się nową rozproszoną platformą typu „odmowa usługi", atakującą albo poprzez systemy teleinformatyczne podłączone do warstwy ICT, albo inteligentną sieć (energetyczną). Na przykład w tym drugim przypadku atak mógłby dostarczyć do sieci na masową skalę fałszywą informację o tym, kiedy potrzebna jest moc na danym obszarze. Pozostaje zatem pytanie, w jaki sposób możemy zarządzać stanem bezpieczeństwa milionów lodówek, zmywarek i pralek, w tym ich statusem aktualizacji i licencją na działanie w systemie inteligentnych sieci? Staje się to wyzwaniem dla bezpieczeństwa cybernetycznego porównywalnym do tego, co Bijlsma i inni stwierdzili dla sektora motoryzacyjnego.

10. Wszystkie sektory: Inteligentne sieci (energetyczne) i inteligentne miasta wymagają współpracy dużej liczby interesariuszy, którzy łączą swoje usługi, głównie fizyczne, poprzez warstwę zarządzania z dużą bazą ICT. Zarządzanie ryzykiem w łańcuchu organizacji stanowi problem, zwłaszcza że często nie jest jasne, kto jest za nie odpowiedzialny. Jeszcze większym wyzwaniem jest zapewnienie odporności łańcucha (cyber). Jednak na wyższym poziomie wymiany informacji między organizacjami nie stosuje się wcześniej zidentyfikowanych lekcji dotyczących bezpieczeństwa cybernetycznego. Brak walidacji informacji uzyskanych od innej organizacji i zweryfikowanie, czy są one dopuszczalne i oczekiwane, może spowodować podjęcie decyzji z poważnymi konsekwencjami. Przestępcy mogą wykorzystać takie słabe interfejsy, np. poprzez staranne tworzenie skoków cen usług.

11. Sektor zdrowia i opieki: Po powolnym starcie roboty o stałej pozycji są stosowane w elastycznych gałęziach przemysłu, takich jak sektor motoryzacyjny. Obecnie na rynku dostępny jest robot mobilny pierwszej generacji. Oczekuje się szybkiego cyklu innowacji, ponieważ roboty te staną się częścią siły roboczej w szpitalach i domach dla osób starszych. Zapewnią elastyczne usługi po niższych kosztach i uzupełnią obecne luki w dostępności pielęgniarek i osób sprawujących opiekę osobistą. Presja na dostarczanie robotów na rynek może spowodować skupienie się na aspektach bezpieczeństwa, pomijając aspekty cyberbezpieczeństwa. Na podstawie wcześniej zidentyfikowanych lekcji dotyczących bezpieczeństwa cybernetycznego można przewidzieć, że awarie bezpieczeństwa cybernetycznego wystąpią w ochronie kanałów komunikacyjnych pomiędzy robotem a główną stacją sterującą podczas zatwierdzania poleceń kierowanych do robota. Kto ponosi odpowiedzialność, gdy w wyniku cyberataku robot podaje niewłaściwe lekarstwa lub potrząsa łóżkiem z osobą owiniętą w gips? Co więcej, robotami będzie zarządzał dział, który prawdopodobnie będzie nieświadomie niepewny. Uruchomi to roboty bez odpowiednio zabezpieczonej konfiguracji, ponieważ podręcznik konfiguracji będzie omawiał jedynie kwestie bezpieczeństwa robotów i nie będzie omawiał szczegółowo kwestii bezpieczeństwa cybernetycznego.

12. Wszystkie sektory: Kolejnym cyklem innowacji ICT jest Internet rzeczy (IOT). Prawie każde urządzenie będzie miało adres internetowy, będzie przekazywać to, co wykryje i może aktywować swoje elementy wykonawcze. Futuryści marzą o nowych, niesamowitych funkcjach ICT, a bystrzy techniczni ludzie je wdrażają. W niektórych przypadkach wstrzykują nawet pod skórę chip RFID, aby zidentyfikować się jako autoryzowani użytkownicy innowacyjnych usług opartych na ICT. Po raz kolejny projektanci nie przyszli do głowy bardziej wyszukanym myślom na temat bezpieczeństwa cybernetycznego.

WNIOSKI

Pokazano, że wyciągnięte wcześniej wnioski dotyczące bezpieczeństwa cybernetycznego dotyczące zagrożeń i ryzyka dla obecnych i poprzednich cykli innowacji ICT nie trafiają do następnego cyklu innowacji ICT. Stare lekcje dotyczące bezpieczeństwa cybernetycznego zostaną ponownie zidentyfikowane. Łatki posłużą do załatania dziur w projekcie „Ser szwajcarski". Osoby posiadające błyskotliwe, innowacyjne pomysły nie mają wykształcenia w zakresie cyberbezpieczeństwa, podobnie jak wielu programistów wdrażających ich pomysły. Zaniedbują stare zagrożenia, które zapewniają cyberprzestępcom ścieżki ataku. Można zatem przewidzieć nowe i pojawiające się zagrożenia, o ile ten cykl innowacji nie zostanie przerwany bez odpowiedniego cyberbezpieczeństwa. Jedyną zaletą jest to, że badacze zajmujący się cyberprzestępczością mogą przygotować się na kolejny cykl innowacji, wcześnie wdrażając rozwiązania i przygotowując odpowiedni zestaw narzędzi kryminalistycznych.

Policyjne procesy dochodzeniowe: praktyczne narzędzia i techniki zwalczania cyberprzestępczości

WSTĘP

Internet przyniósł i nadal będzie przynosił ogromne korzyści przemysłowi, indywidualnym obywatelom i ich społecznościom na całym świecie. Niestety, istnieje niewielka, ale rosnąca mniejszość osób, które starają się wykorzystać nowe możliwości dla wybranych przez siebie celów przestępczych. Cyberprzestępcy szybko dostrzegają potencjalne luki w nowych technologiach i wykorzystują je do popełniania przestępstw lub próbują udaremnić wykrywanie ich działań . Cyberprzestępczość i cyberterroryzm nie dotyczą już osób, które po prostu chcą uzyskać dostęp do systemów komputerowych, aby udowodnić, że jest to możliwe. Zagrożenia cybernetyczne są realne i szkodliwe. Przestępcy i terroryści stojący za współczesnymi cyberzagrożeniami dla społeczeństwa są dobrze zorganizowani i starają się wykorzystać osoby korzystające z usług internetowych. Niezależnie od tego, czy ma to na celu zysk finansowy, realizację ekstremistycznych ideologii, czy groźbę dla dzieci, wpływ na ofiary może być druzgocący. Najbardziej bezbronni członkowie naszego społeczeństwa zbyt często padają ofiarami cyberprzestępstw – od młodych ludzi zagrożonych znęcaniem się lub drapieżnikami seksualnymi po osoby starsze, które stanowią łatwy łup dla zorganizowanych oszustów. Aby stawić czoła zjawisku cyberprzestępczości i cyberterroryzmu, rządy na całym świecie zainwestowały znaczne zasoby w bezpieczeństwo wewnętrzne, co zaowocowało znaczącymi reakcjami organów ścigania i agencji wywiadowczych na zagrożenia w Internecie. Zaprojektowane z myślą o wykrywaniu, powstrzymywaniu i zakłócaniu wszelkiego rodzaju zagrożeń związanych z cyberprzestrzenią, szybko utworzono nowe jednostki policji cybernetycznej, których zadaniem jest prowadzenie dochodzeń w sprawie cyberprzestępstw. Taka inwestycja spełnia pierwszy obowiązek rządów, jakim jest ochrona bezpieczeństwa swojego kraju, obywateli i ich szerszych interesów. Z zadowoleniem przyjmuje się koncentrację i inwestycje mające na celu walkę z cyberprzestępczością i cyberterroryzmem, ale nikt sprawujący władzę nie może sobie pozwolić na samozadowolenie. Zagrożenie ze strony cyberprzestępczości i cyberterroryzmu stale ewoluuje – pojawiają się nowe możliwości popełniania „starych" przestępstw na nowe sposoby, a także przestępstwa związane z zaawansowaną technologią, które nie istniały kilka lat temu . Cyberprzestępcy stają się coraz bardziej wyrafinowani i w dalszym

ciągu tworzą złośliwe oprogramowanie oraz opracowują ulepszone metody infekowania komputerów i sieci. Cyberprzestępcy również stale dostosowują swoją taktykę w miarę wdrażania nowych zabezpieczeń. Aby przeciwdziałać nowym działaniom cyberprzestępczym, organy ścigania muszą kontynuować wysiłki, aby zapewnić, że cyberprzestrzeń będzie dla nich wrogim środowiskiem do działania. Złożony charakter i złożoność cyberprzestępczości i cyberterroryzmu wymaga dedykowanej reakcji, zwłaszcza ze strony śledczych, którzy mają kluczowe znaczenie dla powodzenia śledzenia cyberprzestępców i postawienia ich przed wymiarem sprawiedliwości. Dlatego też w niniejszym rozdziale skupimy się na roli cyberśledczego, omawiając stojące przed nim wyzwania oraz metody, modele i doktrynę dochodzeniową, z których powinien korzystać, aby stać się skutecznym cyberdetektywem. Chociaż rozdział ten nie skupia się na technicznej roli i odpowiedzialności wyspecjalizowanych, zaawansowanych technologicznie śledczych, zapewni im narzędzia i techniki umożliwiające rozwój ich podstawowych umiejętności dochodzeniowych. Ten rozdział powinien także służyć jako przypomnienie dla funkcjonariuszy policji i tradycyjnego detektywa kryminalnego, z których wielu jest obecnie zmuszonych do prowadzenia dochodzeń w sprawie przestępstw w Internecie, mając niewielkie lub żadne przeszkolenie i doświadczenie w tej dziedzinie. W związku z tym w niniejszym rozdziale rozważono pięć istotnych obszarów kluczowych kompetencji dochodzeniowych, które stanowią podstawę, na której należy prowadzić profesjonalne dochodzenia w sprawie cyberbezpieczeństwa, a w istocie wszystkie dochodzenia w sprawach karnych. Kluczowe umiejętności śledcze związane z podejmowaniem decyzji, rozwiązywaniem problemów, formułowaniem hipotez, wprowadzaniem innowacji i znaczeniem zarządzania kontaktami są badane w kontekście współczesnych dochodzeń cybernetycznych.

PODEJMOWANIE DECYZJI ŚLEDCZYCH

Dokonywanie rozsądnych ocen to podstawowa rola i ważna cecha każdego odnoszącego sukcesy cyberśledczego, zwłaszcza tych starszych oficerów dochodzeniowych (SIO), którym powierzono odpowiedzialność za zarządzanie i kierowanie dochodzeniami na dużą skalę. Zapewni to skuteczne podejmowanie decyzji, szczególnie na samym początku dochodzeń cybernetycznych możliwości nie są pomijane, a potencjalne kierunki badań są identyfikowane i rygorystycznie realizowane. W rzeczywistości funkcjonariusze organów ścigania zaangażowani na wczesnym etapie dochodzenia muszą na początku radzić sobie z brakiem wystarczających informacji, a niektóre ważne decyzje mogą wymagać szybkiego i intuicyjnego podjęcia. Według Cooka i Tattersalla (2010)

Kluczowa umiejętność polega na wytrwałości badacza, który potrafi rozpoznać, kiedy nie ma wystarczająco dużo czasu na zebranie dalszych informacji. Intuicja wywodzi się jednak z wiedzy i doświadczenia i może być podatna na stronniczość, dlatego decyzje dochodzeniowe muszą zawsze opierać się na rozumowaniu i analizie, aby uniknąć subiektywizmu.

Rozpoczęcie dochodzenia opartego na cyberprzestrzeni, zwłaszcza każdego złożonego dochodzenia, które może być głośne i prowadzone w świetle mediów, będzie gorączkowe. Nic nie powinno uniemożliwiać profesjonalnemu śledczemu cybernetycznemu wykonywania swoich zadań w tempie zapewniającym mu wykonywanie swoich ról zgodnie z najwyższymi standardami zawodowymi. Śledczy muszą mieć czas na dokończenie dochodzenia, co wymaga od nich, aby nie wpadali w tempo szerszego dochodzenia, lecz w razie potrzeby zwalniali jego tempo. Takie podejście będzie wspierać kluczowe procesy decyzyjne, które są niezbędne dla powodzenia każdego dochodzenia. Według Cooka i Tattersalla (2010):

Podejmowanie decyzji dochodzeniowych musi zawsze mieć na celu osiągnięcie wyznaczonych celów. Aby mieć pewność, że zostaną podjęte dobre decyzje zmierzające do osiągnięcia określonych celów,

należy już na najwcześniejszym etapie dochodzenia określić, jakie są główne cele dochodzenia. Ogólny przykład tego, jak takie cele mogą wyglądać, jest następujący:

• Ustalenie, czy przestępstwo zostało popełnione lub nie zostało popełnione.

• Zbierz wszystkie dostępne informacje, materiały, dane wywiadowcze i dowody.

• Działaj w interesie sprawiedliwości.

• Rygorystycznie badaj wszystkie uzasadnione kierunki dochodzenia.

• Przeprowadź dokładne dochodzenie.

• Identyfikuj, aresztuj i oskarżaj przestępców.

• Przedstaw wszystkie dowody organom ścigania

Skuteczną praktyką jest zapisywanie głównych celów dochodzeniowych dochodzenia cybernetycznego w dzienniku podejmowania decyzji dotyczących polityki dochodzeniowej na wczesnych etapach dochodzenia. Dzięki temu uzasadnienie kluczowych decyzji dochodzeniowych zostanie uchwycone w momencie ich podjęcia w świetle wszystkich łatwo dostępnych informacji. Podstawowe cele dochodzenia należy przekazać wszystkim pozostałym funkcjonariuszom i badaczom, którzy mają operacyjny wymóg znajomości strategicznego kierunku dochodzenia cybernetycznego. W trakcie dochodzenia śledczy i wyżsi funkcjonariusze będą wykorzystywać swoje umiejętności do analizowania, przeglądania i oceniania wszystkich dostępnych informacji i materiałów. Jest to niezwykle ważny proces, ponieważ dokładność, wiarygodność i przydatność uzyskiwanego materiału będą miały wpływ na podejmowanie decyzji. Wszelkie zmiany w głównych celach dochodzenia należy rejestrować i ponownie rozpowszechniać wśród wszystkich funkcjonariuszy prowadzących dochodzenie. Według Calessa:

Złota zasada mówi, że śledczy powinni stosować tak zwaną zasadę „ABC” przez cały czas trwania dochodzenia w następujący sposób:

A. Nie zakładaj niczego

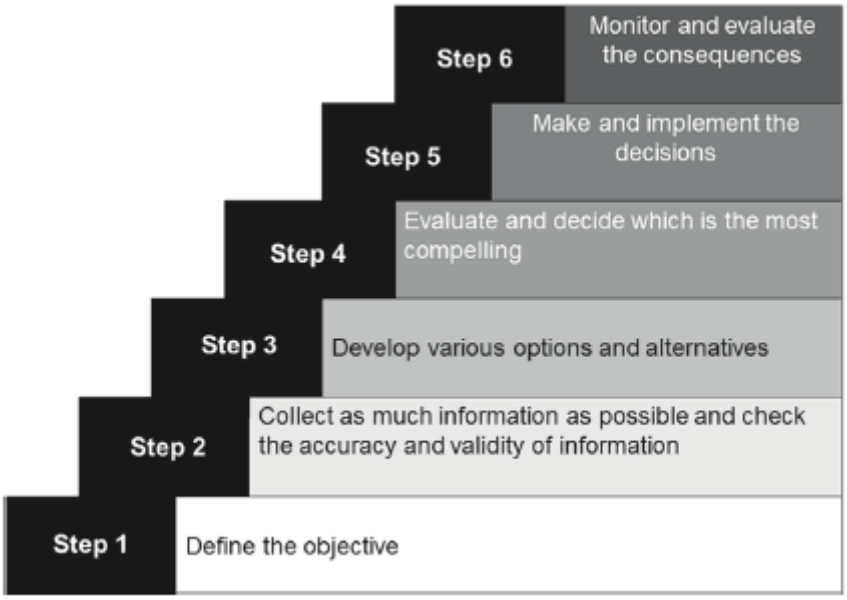
B. Nie wierz w nic

C. Rzuć wyzwanie i sprawdź wszystko

Wszyscy śledczy, zwłaszcza ci prowadzący złożone dochodzenia cybernetyczne, muszą upewnić się, że nic nie jest brane za pewnik i nie można zakładać, że rzeczy są takie, jakimi się wydają lub że procesy zostały przeprowadzone prawidłowo. Szukanie potwierdzenia, ponowne sprawdzanie, przeglądanie i potwierdzanie wszystkich aspektów dochodzenia to cechy charakterystyczne skutecznego cyberdetektywa, które zapewniają, że podczas dynamicznego i szybkiego dochodzenia cybernetycznego żadna potencjalna linia dochodzenia nie zostanie przeoczona.

ROZWIĄZANIE PROBLEMÓW BADAWCZYCH

Kluczowe dla podstawowych umiejętności śledczych związanych z podejmowaniem decyzji są elementy rozwiązywania problemów. Logiczne podejście do podejmowania decyzji w celu skutecznego rozwiązywania problemów w ramach dochodzeń cybernetycznych demonstruje model schodów Cyber Investigators Staircase Model (CISM). Przystosowany do egzekwowania prawa na podstawie modeli przywództwa i zarządzania, CISM zawiera ważne i sekwencyjne elementy zapewniające skuteczne rozwiązywanie problemów pokazanych na rysunku



Model działa w oparciu o założenie, że lepiej jest wybrać konkretny sposób działania spośród szeregu możliwych „opcji". Podstawową kwestią jest to, że badacz cyberbezpieczeństwa nie powinien zakładać, że dostępna jest tylko jedna opcja. Zawsze istnieją alternatywy, szczególnie w przypadku dochodzeń cybernetycznych, które mają tendencję do szybkiego gromadzenia dużych ilości danych. Informacje leżą u podstaw dochodzenia, a zgromadzenie wystarczających informacji pomaga określić liczbę opcji, które można następnie rozważyć w procesach podejmowania decyzji w celu wybrania, która opcja jest najbardziej przekonująca. W celu gromadzenia i gromadzenia informacji spełniających wymagania kroku 2 CISM, zestaw zaimków pytających, powszechnie znany w dziedzinie egzekwowania prawa jako metoda „5× WH + H" – Kto, Co, Kiedy, Gdzie, Dlaczego + Jak można to dobrze wykorzystać . Formuła ta pomaga uporządkować informacje dochodzeniowe i zidentyfikować luki w wiedzy. W przypadku dochodzenia w sprawie cyberprzestępczości może to wyglądać następująco:

• Kto jest ofiarą? – Dane ofiary i dlaczego ta ofiara?

• Co się stało? – Dokładne szczegóły dotyczące incydentu/zdarzenia

• Kiedy to się stało? – Kwestie tymczasowe, takie jak odpowiednie czasy

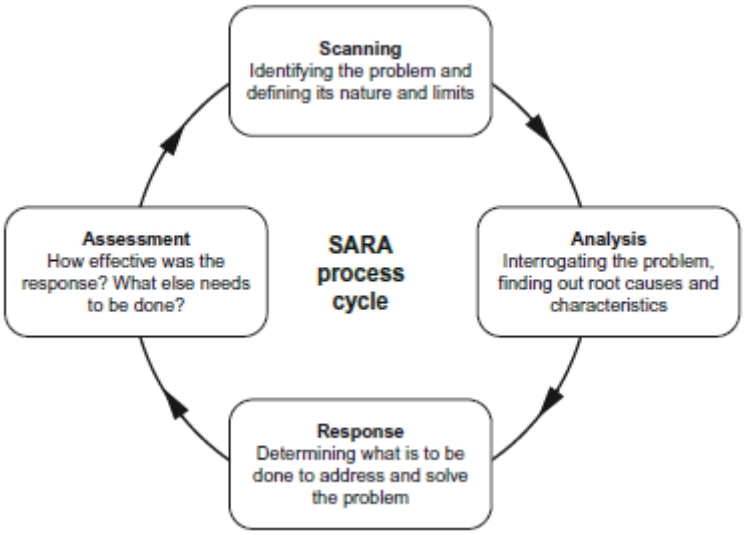
• Gdzie to się stało? – Lokalizacje geograficzne, krajowe/międzynarodowe?

• Dlaczego to się stało? – Motywacja przestępstwa lub terroryzmu

• Jak to się stało? – Dokładne szczegóły sposobu działania

Informacje te można następnie przekształcić w użyteczną matrycę dochodzeniową, która pomoże zidentyfikować luki w informacjach poprzez zestawienie wszystkich istotnych szczegółów w logicznej kolejności, która jest łatwo zrozumiała. Matrycę można następnie wypełnić w miarę rozwoju dochodzenia cybernetycznego i wykorzystać ją jako źródło odniesienia dla podstawy stosowania CISM i wszelkich związanych z tym procesów decyzyjnych, które są wymagane. Matryca musi być dokumentem żywym, regularnie aktualizowanym w miarę postępu dochodzenia. Matrycę można następnie powiązać z decyzjami w momencie ich podejmowania, co posłuży do zilustrowania tego, co było znane lub nie znane w momencie podejmowania konkretnej decyzji. Jest to bardzo ważny punkt uzasadniający, dlaczego badacz podjął lub nie podjął określonego sposobu działania. Struktura 5×WH + H może być również przydatna podczas uzyskiwania informacji lub aktualizacji na temat incydentu

lub zestawu okoliczności. Badacze mogą zadawać pytania, korzystając z nagłówków 5 × WH + H, aby ustalić wystarczające szczegóły na temat tego, co może już być znane. Metodę tę można zastosować, aby zapewnić dostarczanie jasnych i zwięzłych informacji w sposób systematyczny, a nie losowy. Aby wesprzeć śledczych zaangażowanych w prowadzenie złożonych spraw cybernetycznych, skuteczny proces stanowi model rozwiązywania problemów oparty na skanowaniu, analizie, reagowaniu i ocenie (SARA), pokazany na rysunku dla funkcjonariuszy policji.



Metodologia analityczna SARA oferuje etapowy proces identyfikacji, zrozumienia i rozwiązywania konkretnych problemów poprzez skanowanie, analizę, reakcję i ocenę. Wielu pracowników organów ścigania wykorzystuje czteroetapowy proces w celu zapewnienia ram pomagających im pokonać wyzwania związane ze znalezieniem rozwiązań złożonych problemów. Jest to podejście, które dobrze sprawdza się w przypadku problemów i wyzwań pojawiających się podczas dochodzeń w sprawie cyberprzestępczości i cyberterroryzmu. Oczywiście w rzeczywistości żaden model teoretyczny nie jest w stanie objąć wszystkich potencjalnych problemów przy próbach dynamicznego rozwiązywania problemów podczas złożonych dochodzeń cybernetycznych o wymiarze międzynarodowym, ale model zapewnia metodyczne podejście, które będzie wspierać i informować o kluczowych decyzjach dochodzeniowych. Tak też musi być ,że uznano, że etapy cyklu SARA mogą się nakładać, powtarzać, a niektóre mogą pozostać niezagospodarowane, podczas gdy inne dobiegają końca. Odzwierciedla to tempo dochodzeń cybernetycznych, ponieważ niektóre wątki złożonego dochodzenia mogą rozwijać się szybko, podczas gdy inne wymagają więcej czasu. Uznaje się również, że rozwiązując problemy funkcjonariusze policji nie postępują w sposób ciągły przez cztery etapy cyklu SARA, ale zamiast tego przechodzą przez niektóre etapy, gdy doświadczenie podpowiada im, że jest to celowe i leży to w interesie szerszego śledztwa. Biorąc to pod uwagę, cykl SARA zapewnia podejście metodyczne, na podstawie którego można określić działania związane z rozwiązywaniem problemów. Funkcjonariuszom odpowiedzialnym za prowadzenie dochodzeń w sprawie przestępstw związanych z cyberprzestępczością dobrze byłoby przyjąć taki model, który zapewnia pewność i jasność procesom decyzyjnym dotyczącym rozwiązywania problemów.

OPRACOWANIE HIPOTEZ BADAWCZYCH

Decyzje dotyczące skutecznego prowadzenia dochodzeń cybernetycznych mogą być oparte na hipotezie lub się nią kierować. W przypadku dochodzeń w sprawie cyberbezpieczeństwa Cook i Tattersall (2010) zalecają, co następuje:

hipoteza to propozycja wysunięta jako podstawa rozumowania bez założenia o jej prawdziwości i przypuszczenie przyjęte jako punkt wyjścia do dalszego badania znanych faktów. Opracowywanie i stosowanie hipotez to powszechnie uznawana technika wśród śledczych, którą można zastosować w celu ustalenia najbardziej logicznego lub prawdopodobnego wyjaśnienia, teorii lub wniosku na temat tego, dlaczego i w jaki sposób popełniono cyberprzestępstwo. W idealnym przypadku, zanim cyberprzestępcy opracują hipotezę, powinien być dostępny wystarczający, wiarygodny materiał, na którym można oprzeć hipotezę, taki jak szczegółowe dane ofiary, dokładne szczegóły incydentu lub zdarzenia, krajowy lub międzynarodowy wymiar przestępstwa, motywy przestępstwa i dokładny sposób operandi .

Oczywiście wiedza i doświadczenie z poprzednich przypadków również bardzo pomogą w skonstruowaniu odpowiedniej hipotezy. Generowanie i budowanie hipotez jest oczywistą i naturalną czynnością dla cyberprzestępców, szczególnie na wczesnych etapach dochodzenia. Oczywiście, jeśli dostępne są już wystarczające informacje lub dowody, nie będzie potrzeby stosowania metody hipotezy. Jednak cyberprzestępcy coraz częściej wzywani są do ustalenia na początku dochodzenia najbardziej podstawowych faktów, np. tego, czy popełniono przestępstwo. Hipotezy są ważne, aby zapewnić wstępny kierunek dochodzenia, jeśli taki istnieje mało informacji do pracy. Wszyscy badacze cyberbezpieczeństwa muszą „zachować otwarty umysł" i pamiętać, że lepiej zebrać jak najwięcej informacji, zanim zaczniemy zbytnio polegać na jakiejkolwiek teorii spekulatywnej. Błędem badaczy cybernetyki jest tworzenie teorii przed zgromadzeniem wystarczających danych, ponieważ łatwo wpaść w pułapkę manipulowania i masowania faktów w celu dopasowania ich do teorii, zamiast upewnić się, że teorie odpowiadają faktom. Cook i Tattersall (2010) przedstawiają wytyczne dotyczące profesjonalnej praktyki dochodzeniowej policji, powszechnie stosowane przez funkcjonariuszy organów ścigania na całym świecie. Ich porady, oparte na rozległym doświadczeniu śledczym w Wielkiej Brytanii, obejmują listy kontrolne, które należy uwzględnić przy formułowaniu hipotez. Cook i Tattersall (2010) zalecają, aby podczas opracowywania założeń teoretycznych badacze cyberbezpieczeństwa zwrócili należytą uwagę na następujące kwestie:

• Uważaj na zbytnie poleganie na jednej hipotezie lub na ograniczonej liczbie hipotez, gdy nie ma wystarczających informacji.

• Pamiętaj o maksymie „zachowuj otwarty umysł".

• Zapewnij dokładne zrozumienie znaczenia i wiarygodności dowolnego materiału.

• Upewnij się, że hipotezy są poddawane ciągłemu przeglądowi i pozostają dynamiczne, pamiętając, że każda hipoteza jest w najlepszym przypadku jedynie tymczasowa.

• Zdefiniuj jasny cel hipotezy.

• Rozwijaj jedynie hipotezy, które „najlepiej pasują" do znanych informacji i materiałów.

• Skonsultuj się ze współpracownikami i ekspertami, aby omówić i sformułować hipotezę.

• Zapewnij dostępność wystarczających zasobów do opracowania lub przetestowania hipotezy .

Postęp w dochodzeniach w sprawie cyberbezpieczeństwa wymaga współpracy, a funkcjonariusze policji muszą konsultować, słuchać i brać pod uwagę porady i wskazówki udzielane przez wyspecjalizowanych śledczych zajmujących się zaawansowanymi technologiami. Każdy badacz cyberbezpieczeństwa, który ignoruje porady specjalisty, robi to na własne ryzyko.

INNOWACJA ŚLEDCZ

Osoby prowadzące dochodzenia w sprawie cyberprzestępczości i cyberterroryzmu, zwłaszcza ci funkcjonariusze kierujący zespołami dochodzeniowymi i zarządzającymi nimi, muszą posiadać zdolność rozpoznawania dobrych pomysłów i wykorzystywania ich do realizacji celów. Jest to niezwykle przydatna umiejętność dla każdego śledczego policyjnego prowadzącego tradycyjne dochodzenia kryminalne, ale jest niezbędna dla śledczych zajmujących się cyberprzestrzenią, biorąc pod uwagę sam rozmiar, skalę, zakres i złożoność przestępczości internetowej. Aby wykrywać, powstrzymywać i zakłócać działalność cyberprzestępczą, wszyscy cyberprzestępcy muszą wykorzystać swoje doświadczenie, umiejętności i pomysłowość. Niezbędne jest innowacyjne podejście do zwalczania cyberprzestępczości i cyberterroryzmu, a w ramach procesu dochodzeniowego śledczy powinni wprowadzić lub wprowadzić nowe metody i pomysły do wdrożenia. Niezbędne jest, aby śledczy zajmujący się cyberatakami i starsi przywódcy stworzyli efektywne środowisko pracy zespołowej. Każda lekcja płynąca z każdego dochodzenia cybernetycznego pokazuje, że żaden pojedynczy śledczy nie jest w stanie samodzielnie skutecznie prowadzić dochodzenia cybernetycznego. Tylko współpracując i łącząc ze sobą indywidualne umiejętności i wiedzę, zespół cyberprzestępców będzie w stanie skutecznie uporać się z cyberprzestępczością i cyberterroryzmem. Dlatego funkcjonariusze zajmujący się inwestowaniem w cyberprzestępstwa muszą tworzyć spójną kulturę pozytywnego znajdowania rozwiązań i nowych pomysłów na problemy i wyzwania. Potrzeba dzielenia się i wspierania nowych pomysłów jest niezbędnym elementem każdego zespołu dochodzeniowo-śledczego, a innowacyjne pomysły, które ożywiają i wzbudzają ducha śledczych, są niezbędne. Należy zakwestionować założenia oparte na tradycyjnych wierzeniach i wiedzy prehistorycznej na rzecz znalezienia nowych sposobów działania, z wykorzystaniem nowych taktyk, technik i technologii. Nie oznacza to, że tradycyjne metody nie działają, jeśli są wyraźnie wypróbowane i przetestowane, ale przyjęcie bardziej radykalnego podejścia, charakteryzującego się mniejszą niechęcią do ryzyka i przyjęcie innowacyjnych pomysłów, aby postawić cyberprzestępców przed wymiarem sprawiedliwości, jest absolutnie konieczne dla dalszego rozwoju zawodowego cyberprzestępczości polityka, praktyka i procedura policji.

BADACZY KONTAKT Z KIEROWNICTWEM

W policji, a zwłaszcza w sprawach związanych z dochodzeniem w sprawie cyberprzestępczości, jednym z kluczowych punktów, z których wywodzi się całe postrzeganie policji, jest kontakt między społeczeństwem a policją. Ten pierwszy kontakt ze społeczeństwem, niezależnie od tego, czy jest to ofiara, czy świadek cyberprzestępczości, ma kluczowe znaczenie dla skutecznego zapewniania cyberpolicji na każdym szczeblu. Niezależnie od tego, czy kontakt ten polega na telefonicznym wezwaniu policji, czy na osobistym spotkaniu z funkcjonariuszem policji, dla członka społeczeństwa inicjującego interakcję i zgłaszającego się, jest to moment niezwykle ważny. Osoba kontaktująca się z policją, w sposób dorozumiany lub wyraźny w celu zgłoszenia cyberprzestępczości, zadaje sobie trzy następujące pytania:

• Czy moje obawy zostaną potraktowane poważnie?

• Czy otrzymam usługę, której oczekuję?

• Czy będę zadowolony z tego, co się wydarzyło?

Jeśli ten początkowy kontakt zostanie dobrze przeprowadzony, późniejsze działania opierają się na ustalonych podstawach. Aby stawić czoła wszelkim formom cyberprzestępczości, organy ścigania potrzebują pełnego wsparcia społeczeństwa, więc gdy członkowie społeczeństwa mają odwagę i przekonanie, aby zgłosić i omówić kwestie cyberprzestępczości, funkcjonariusze policji muszą należycie uwzględniać pozytywny kontakt kierownictwo. Zarządzanie kontaktami z cyberprzestępcami musi być priorytetem nie tylko dla funkcjonariuszy organów ścigania, którzy występują publicznie, ale dla

wszystkich funkcjonariuszy policji, w tym śledczych zajmujących się cyberprzestępczością. Samo zapewnienie, że doniesienia opinii publicznej zostaną odpowiednio potraktowane i potraktowane poważnie oraz że obywatel będzie na bieżąco informowany i usatysfakcjonowany reakcją policji, najlepiej wpłynie na skuteczność wstępnego dochodzenia. Wszyscy policjanci muszą zrozumieć, że pierwsze wrażenie naprawdę się liczy. Uprzejmy, profesjonalny i pozytywny kontakt z obywatelami jest ważny dla wszystkich działań policji, w tym dochodzeń w sprawie cyberprzestępczości. Przede wszystkim należy poważnie traktować sprawy zgłaszane policji w związku z cyberprzestępczością. W walce z cyberprzestępczością nie można popadać w samozadowolenie. Rozpatrując zgłoszenia dotyczące cyberprzestępczości, wszyscy funkcjonariusze mają obowiązek:

LISTEN członków społeczeństwa:

(Listen) Słuchaj obywateli i poważnie traktuj ich obawy

(Inspire) Wzbudzaj pewność siebie i zapewniaj pewność

(Support) Wsparcie w postaci informacji, porad i wskazówek

(Take) Przejmij odpowiedzialność i zarejestruj obawy obywateli

(Explain) Wyjaśnij, co masz zrobić i dlaczego

(Notify) Powiadom nadzór i zgłoś wątpliwości

Podczas wszystkich dochodzeń w sprawie cyberbezpieczeństwa na pierwszym miejscu należy stawiać społeczeństwo. Ofiarom cyberprzestępstw należy zapewnić profesjonalną opiekę i w razie potrzeby zapewnić specjalistyczną opiekę i wsparcie. Osoby składające skargi dotyczące cyberprzestępstw muszą być regularnie informowane o postępie dochodzenia. Wysłuchiwanie obywateli i zapewnianie służb policyjnych spełniających najwyższe standardy zawodowe zwiększy zaufanie społeczeństwa do zaangażowania i determinacji organów ścigania w walce z cyberprzestępczością.

BADANIE PRZESTĘPSTWA I TERRORYZMU

Kiedy funkcjonariusze Metropolitan Police w październiku 2005 roku wtargnęli do mieszkania w zachodnim Londynie, aresztowali młodego mężczyznę, Younesa Tsouli. Znaczenie tego aresztowania nie było od razu jasne, ale dochodzenie wkrótce ujawniło, że urodzona w Maroku Tsouli była najbardziej poszukiwanym „cyberterrorystą" na świecie . W swojej działalności Tsouli przyjął nazwę użytkownika „Irhabi 007" (Irhabi oznacza po arabsku „terrorysta"), a jego działalność rozrosła się od publikowania w Internecie porad dotyczących włamywania się do systemów komputerowych mainframe po pomaganie osobom w planowaniu ataków terrorystycznych (Staniforth, 2012). Tsouli przeszukała Internet w poszukiwaniu domowych filmów nakręconych przez żołnierzy amerykańskich w teatrach konfliktów w Iraku i Afganistanie, które ujawniałyby wewnętrzny układ amerykańskich baz wojskowych. Z biegiem czasu te małe fragmenty informacji zostały zebrane i przekazane osobom planującym ataki na bazy sił zbrojnych. Ten wirtualny wrogi rekonesans dostarczył poufnych danych ilustrujących, że terroryści nie muszą już przeprowadzać fizycznego rozpoznania, jeśli możliwe jest przechwycenie i skrupulatne zebranie odpowiednich informacji z Internetu. Dochodzenie policyjne ujawniło następnie, że na jego kontach Tsouliego znajdowały się fałszywe transakcje o wartości 2,5 miliona euro, które wykorzystywał do wspierania i finansowania działalności terrorystycznej. Przyznając się do zarzutów o podżeganie do popełnienia aktów terroryzmu, Tsouli został skazany na 16 lat pozbawienia wolności w więzieniu Belmarsh o zaostrzonym rygorze w Londynie, gdzie – co być może nie jest zaskoczeniem – odmówiono mu dostępu do Internetu. Ówczesny Krajowy Koordynator Dochodzeń Terrorystycznych, zastępca podkomisarza Peter Clarke, powiedział, że Tsouli:

podał łącze do rdzenia Al-Kaidy, do serca Al-Kaidy i szerszej sieci, z którą łączył się za pośrednictwem Internetu", dodał następnie: „pokazał nam, w jakim stopniu mogą prowadzić planowanie operacyjne w Internecie. Był to pierwszy wirtualny spisek mający na celu morderstwo, jaki widzieliśmy .

Sprawa przeciwko Tsoouli była pierwszą w Wielkiej Brytanii, która szybko doprowadziła do uświadomienia sobie, że cyberterroryzm stanowi realne i aktualne zagrożenie dla bezpieczeństwa narodowego Wielkiej Brytanii. Minęło dziesięć lat od aresztowania Tsouli, a funkcjonariusze organów ścigania zrozumieli, że Internet wyraźnie zapewnia pozytywne możliwości globalnej wymiany informacji, komunikacji, tworzenia sieci kontaktów i edukacji oraz jest głównym narzędziem w walce z przestępczością, ale nowe i wyłaniające się współczesne zagrożenia w dalszym ciągu wpływają na bezpieczeństwo społecznościstarają się chronić. Internet został przejęty i wykorzystany przez terrorystów nie tylko w celu usprawnienia planowania ataków, ale także w celu radykalizacji i rekrutacji nowych agentów dla swojej sprawy. Sprawa przeciwko Tsouli wzbudziła obawy wśród specjalistów ds. bezpieczeństwa w związku z całkowitym brakiem zrozumienia wśród śledczych policji kwestii związanych z przestępczością i terroryzmem, zarówno na poziomie strategicznym, jak i taktycznym. Aby zapewnić jasność, śledczy muszą przede wszystkim zrozumieć, że terroryzm jest przestępstwem, przestępstwem mającym poważne konsekwencje i takim, które wymaga odróżnienia od innych rodzajów przestępstw, ale mimo to jest przestępstwem. Osoby, które popełniają przestępstwa o charakterze terrorystycznym sprzeczne z prawem krajowym i międzynarodowym, podlegają procesom wymiaru sprawiedliwości w sprawach karnych, a osoby, co do których istnieje podejrzenie, że są zaangażowane w terroryzm, podlegają restrykcyjnym działaniom wykonawczym. Jednakże kluczowymi cechami terroryzmu, odróżniającymi go od innych form przestępczości, są jego podstawowe motywacje. Terroryzm może mieć podłoże polityczne, religię lub brutalną i ekstremistyczną ideologię . Te podstawowe cele różnią się od innych motywów przestępczych, takich jak chęć osiągnięcia korzyści osobistych lub chęć zemsty. Terroryści mogą kierować kimkolwiek lub dowolną kombinacją podstawowych motywacji, ale głównym motywatorem jest polityka. Terroryzm jest bardzo skuteczną metodą promowania przekonań i ma potencjalnie poważne konsekwencje dla społeczeństwa. Jeśli pozwoli się mu rosnąć i rozkwitać, terroryzm może podważyć bezpieczeństwo narodowe, spowodować niestabilność kraju, a w najbardziej ekstremalnych okolicznościach może doprowadzić do wojny. Terroryzm ma na celu podważenie legitymizacji państwa, wolności i demokracji. Są to zupełnie inne zestawy motywacji i wyników w porównaniu z innymi rodzajami przestępstw. To jest właśnie powód, dla którego walka z terroryzmem na szczeblu krajowym i międzynarodowym jest przedsięwzięciem kierowanym przez rządowe agencje wywiadowcze i postrzeganym jako działalność „wyższej policji" w tajnej i wrażliwej dziedzinie bezpieczeństwa narodowego. Prymat przyznany rządowemu aparatowi wywiadowczemu w celu zwalczania terroryzmu oznacza zatem, że zwalczanie terroryzmu różni się od prowadzenia dochodzeń w sprawie innych rodzajów przestępczości. Potencjalny wpływ na bezpieczeństwo narodu jest powodem, dla którego terroryzm we wszystkich swoich postaciach wymaga tajnego, zapobiegawczego i opartego na danych wywiadowczych podejścia, aby mu zapobiec. Chociaż dla osoby prowadzącej dochodzenie w sprawie cyberterroryzmu ważne jest rozróżnienie pomiędzy przestępczością a terroryzmem, należy również przyznać, że zarówno dochodzenia w sprawie cyberprzestępczości, jak i cyberterroryzmu bardzo różnią się od innych rodzajów tradycyjnych dochodzeń karnych. Należy wziąć pod uwagę trzy kluczowe różnice. Po pierwsze, dochodzenia cybernetyczne mają zasięg globalny. Każde większe dochodzenie w sprawie cyberprzestępczości lub cyberterroryzmu może prowadzić w wielu lokalizacjach. Na przykład jedno dochodzenie dotyczące jednego cyberterrorysty może zaprowadzić śledczych do kilku jurysdykcji policyjnych w oddzielnych regionach tego samego kraju, a następnie do wielu krajów w Europie, na Bliskim Wschodzie, w Afryce i na całym świecie, w miarę prowadzenia dochodzenia. Po drugie, skala dochodzenia może szybko wzrosnąć, ponieważ w dowolnym miejscu na świecie zostanie zidentyfikowanych wiele ofiar i

podejrzanych. Zapewnienie zasobów dochodzeniowych na tym szczeblu dochodzeń, gdzie istnieje krytyczna potrzeba gromadzenia danych wywiadowczych i gromadzenia dowodów, może szybko przekroczyć możliwości tradycyjnych zespołów dochodzeniowych powoływanych do rozpatrywania najpoważniejszych przestępstw. Po trzecie, złożoność takiego dochodzenia jest widoczna nie tylko w transgranicznych protokołach transnarodowych, ale także w tym, że informacje wywiadowcze i dowody są gromadzone jednocześnie. Dowody są niezbędne do skutecznego ścigania, a dane wywiadowcze mogą być pilnie potrzebne w celu wsparcia trwających tajnych operacji agencji wywiadowczych na całym świecie.

WNIOSEK

Wpływ cyberprzestępczości i cyberterroryzmu zmusił agencje wywiadowcze i organy ścigania na całym świecie do wkroczenia w nową erę współpracy w celu wspólnego skutecznego zwalczania zagrożeń cybernetycznych. Mimo że dochodzenia w sprawie cyberbezpieczeństwa mają zasięg, skalę i złożoność wykraczające poza inne dochodzenia na dużą skalę, ich skuteczność zależy od dokładnej pracy policji dochodzeniowej. Celem tego rozdziału jest zilustrowanie, że chociaż śledczy w wyspecjalizowanych jednostkach ds. cyberprzestępczości i zwalczania terroryzmu mają wyjątkowe umiejętności i zdolności do wykonywania swoich ról, to ich dbałość o szczegóły w połączeniu z profesjonalnym i praktycznym zastosowaniem się do ich roli jako śledczego ma kluczowe znaczenie. do ich sukcesu. Koncentrowanie się na podstawowych narzędziach i technikach dochodzeniowych opisanych w tym rozdziale jest niezbędne do skutecznego prowadzenia dochodzeń w sprawie cyberprzestępczości i cyberterroryzmu. Cyberprzestępczość będzie nadal ewoluować w szybkim tempie i wszyscy specjaliści ds. bezpieczeństwa muszą zdawać sobie sprawę, że działają obecnie w świecie przestępstw o niewielkim wpływie i wielu ofiarach, w którym napady na banki nie muszą już skrupulatnie planować jednej kradzieży miliona dolarów. nowe możliwości technologiczne sprawiają, że jedna osoba może obecnie dokonać milionów napadów na jednego dolara każdy Paradoksalnie skuteczne współczesne dochodzenia w sprawie cyberbezpieczeństwa opierają się na podejściu opartym na współpracy, multidyscyplinarnym i obejmującym wiele agencji, w ramach którego detektywi policyjni, śledczy zajmujący się zaawansowanymi technologiami, analitycy kryminalistyczni oraz eksperci ze środowiska akademickiego i sektora prywatnego współpracują, aby stawić czoła cyberzagrożeniom. Złożony charakter i zaawansowanie cyberprzestępczości i cyberterroryzmu w dalszym ciągu wymagają oddanej i zdecydowanej reakcji, zwłaszcza ze strony śledczych, którzy mają kluczowe znaczenie dla powodzenia śledzenia cyberprzestępców i postawienia ich przed wymiarem sprawiedliwości. Obecnie potrzebny jest profesjonalnie przeszkolony i wysoko wykwalifikowany personel dochodzeniowy w dziedzinie cyberbezpieczeństwa. Pracownicy ci muszą przygotować się i wyposażyć na stojące przed nimi wyzwania cybernetyczne, a lektura kolejnych rozdziałów stanowi doskonały punkt wyjścia. Co jednak najważniejsze, osoby prowadzące dochodzenia w sprawie cyberprzestępczości i cyberterroryzmu – niezależnie od tego, jak złożone i techniczne staną się dochodzenia w sprawie cyberbezpieczeństwa w przyszłości – muszą rozwijać swoją wiedzę specjalistyczną w oparciu o podstawowe kompetencje dochodzeniowe opisane w tym rozdziale.

Specyfikacje cyberbezpieczeństwa: rejestrowanie wymagań użytkowników na potrzeby dochodzeń w sprawie cyberbezpieczeństwa

WSTĘP

W wielu obszarach bezpieczeństwa „człowiek w systemie” często stanowi kluczową linię obrony w zakresie identyfikowania zagrożeń, zapobiegania im i reagowania na nie. Tradycyjnie domeny te koncentrowały się na świecie rzeczywistym, począwszy od głównego nurtu bezpieczeństwa publicznego w zatłoczonych przestrzeniach i kontrolach granicznych, aż po identyfikację podejrzanych

zachowań, wrogi rozpoznanie i wdrażanie inicjatyw antyterrorystycznych. W takich przypadkach za bezpieczeństwo zwykle odpowiada personel pierwszej linii, posiadający określone role i obowiązki, działający zgodnie z protokołami organizacyjnymi. Z punktu widzenia systemu proces zapewniania bezpieczeństwa zależy od wydajności tych ludzi (np. użytkowników i interesariuszy) w szerszym systemie bezpieczeństwa. Pracownicy często pracują w złożonych i trudnych środowiskach pracy, w których charakter ich pracy jest taki, że określone naruszenia bezpieczeństwa mogą występować bardzo rzadko, dlatego ich zadaniem jest rozpoznawanie niewielkich zmian stanu w ramach masowego przepływu pracy, ale gdzie zdarzenia związane z bezpieczeństwem mogą mieć szybkie i katastrofalne konsekwencje (np. osoby zajmujące się bagażem linii lotniczych nie zidentyfikowały w bagażu pasażera improwizowanego urządzenia wybuchowego). Co więcej, wraz z rosnącą obecnością technologii w zapewnianiu bezpieczeństwa, konieczne jest wykorzystanie złożonych systemów rozproszonych, które pomagają użytkownikowi, a w niektórych przypadkach odgrywają zasadniczą rolę w ułatwianiu decyzji podejmowanych przez użytkownika. Jednak jedną ze znaczących korzyści płynących z wdrożenia wyspecjalizowanego personelu ochrony jest to, że często zapewnia on elastyczność operacyjną i lokalną/ukrytą wiedzę na temat swojego środowiska pracy, której po prostu nie posiadają zautomatyzowane systemy . Dzięki wyjątkowemu zrozumieniu kontekstu pracy (oraz umiejętności dostrzegania subtelnych wzorców zachowań i leżących u ich podstaw norm społecznych w tych środowiskach) pracownicy ochrony stanowią kluczowy atut w identyfikowaniu nietypowych zachowań lub podejrzanych incydentów, które mogą stanowić ryzyko dla bezpieczeństwa publicznego . Jednakże ci sami ludzie wykazują również potencjalną słabość systemową, jeśli ich wymagania i ograniczenia nie zostaną odpowiednio rozważone lub w pełni zrozumiane w odniesieniu do innych aspektów całego systemu, w którym działają. Z podobnej perspektywy cyberbezpieczeństwo działa na poziomie systemowym, na którym użytkownicy (np. społeczeństwo), dostawcy usług (np. moderatorzy społeczności i biznesu w Internecie) oraz podmioty komercyjne lub społeczne (np. określone instytucje bankowe, detaliczne, sieci społecznościowe) i fora) łączą się w wirtualnych i współdzielonych interakcjach w cyberprzestrzeni w celu przetwarzania transakcji. Kluczowa różnica polega na tym, że w systemie nie ma formalnych funkcjonariuszy policji, policji ani ochroniarzy, do których użytkownicy mogliby zwrócić się o pomoc. Być może najbliższą analogią do jakiejkolwiek formy policji w Internecie byliby moderatorzy sieci społecznościowych i forów, ale często są to ochotnicy bez formalnego przeszkolenia i ostatecznie nie ponoszący prawnej odpowiedzialności za cyberbezpieczeństwo. Chociaż istnieją wymogi dotyczące bezpiecznych transakcji, zwłaszcza gdy ludzie udostępniają swoje dane osobowe i dane bankowe witrynom sprzedaży detalicznej, witryny mediów społecznościowych są szczególnie narażone na kradzież tożsamości w wyniku informacji, które ludzie mogą swobodnie i/lub niczego niepodejrzewający przekazywać stronom trzecim. Nie ma wspólnego prawa obowiązującego w cyberprzestrzeni, ponieważ w świecie rzeczywistym normy społeczne można łatwo zniekształcić i wykorzystać, tworząc podatność na zagrożenia bezpieczeństwa. Innym czynnikiem wpływającym na bezpieczeństwo cybernetyczne są potencjalne zniekształcenia czasowe, które mogą wystąpić w przypadku cybermediów. Historyczne wpisy lub blogi mogą propagować przyszłe zagrożenia bezpieczeństwa w sposób, w jaki artefakty ze świata rzeczywistego nie mogą. Na przykład fale cybernetyczne mogą wynikać z historycznych postów i blogów i mogą mieć większy oddźwięk po konkretnym wydarzeniu. Cyber stwarza paradoksalną perspektywę bezpieczeństwa. Zagrożenia mogą pojawiać się szybko i dynamicznie w odpowiedzi na bezpośrednie działania (np. zamieszki w Wielkiej Brytanii w 2011 r.), podczas gdy w innych przypadkach dane mają charakter historyczny i mogą pozostawać uśpione przez długie okresy czasu. Jednak dane te nadal mają w sobie coś, co może być tak samo uderzające, jak wydarzenie, które dopiero co miało miejsce. Zrozumienie sposobów, w jakie użytkownicy mogą czerpać znaczenie z cybermediów, jest ważną częścią zrozumienia cyberwpływu. Z punktu widzenia cyberbezpieczeństwa tradycyjne spojrzenie na bezpieczeństwo stwarza szereg wyzwań:

• Kim są użytkownicy (i gdzie się znajdują w momencie interakcji)?

• Kto jest odpowiedzialny za cyberbezpieczeństwo?

• Jak identyfikujemy potrzeby użytkowników w zakresie cyberbezpieczeństwa?

• Jakie metody i narzędzia mogą być dostępne/odpowiednie do uzyskiwania wymagań cybernetycznych?

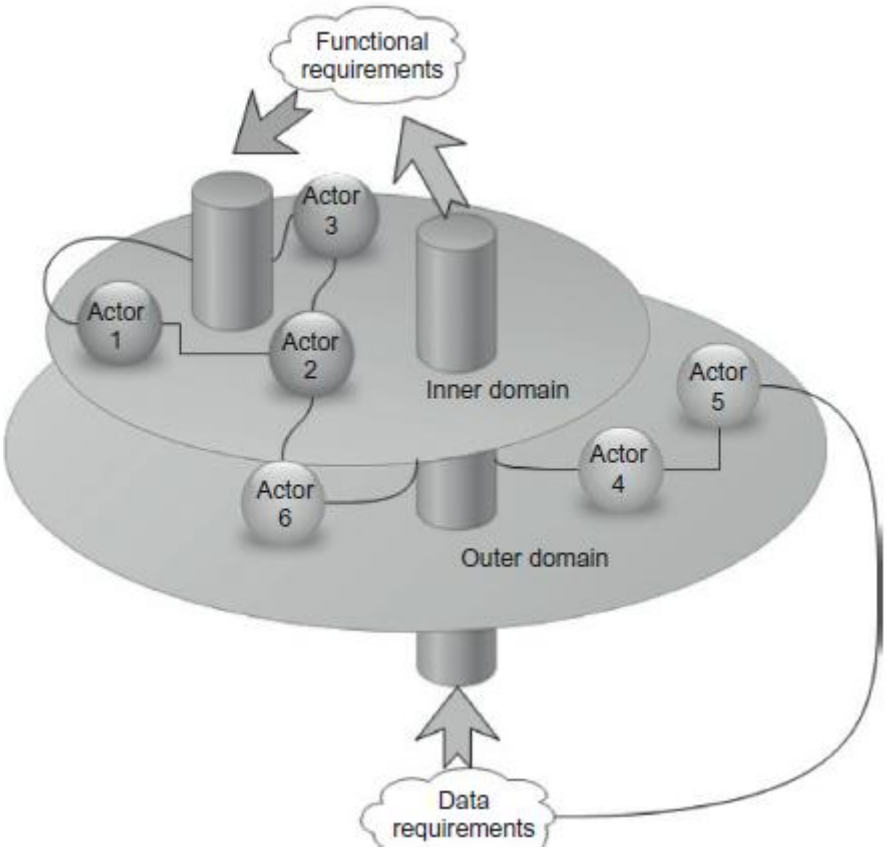
• Co może charakteryzować podejrzane zachowanie w ramach interakcji cybernetycznych?

• Jaka jest natura obserwowanego obiektu (np. czy jest to zachowanie, stan, działanie itd.)?

U podstaw tych wyzwań leżą fundamentalne kwestie bezpieczeństwa i wydajności użytkownika. Coraz ważniejsze jest zmniejszanie prawdopodobieństwa błędu ludzkiego w interakcjach cybernetycznych. Błędy ludzkie mogą nie tylko utrudniać prawidłowe wykorzystanie i działanie technologii cybernetycznych, ale mogą również zagrozić integralności takich systemów. Istnieje zapotrzebowanie na formalne metody, które umożliwią badaczom analizę i weryfikację poprawności systemów interaktywnych, szczególnie w odniesieniu do interakcji międzyludzkich. Tylko rozważenie tych kwestii i zrozumienie podstawowych wymagań, jakie mogą mieć różni użytkownicy i zainteresowane strony, można opracować bardziej zintegrowane podejście do cyberbezpieczeństwa z perspektywy skoncentrowanej na użytkowniku. Rzeczywiście, w przypadku dochodzeń w sprawie cyberbezpieczeństwa kwestie te stwarzają ważne pytania do rozważenia przy badaniu podstaw, na których mogą opierać się interakcje cybernetyczne i gdzie najlepiej skierować przyszłe wysiłki w celu opracowania rozwiązań.

WYMAGANIA UŻYTKOWNIKÓW I POTRZEBA PODEJŚCIA SKONCENTROWANEGO NA UŻYTKOWNIKU?

Podczas badania potrzeb użytkowników podstawową kwestią jest prawidłowa identyfikacja wymagań użytkownika, które następnie są ponownie sprawdzane w sposób iteracyjny w całym procesie projektowania. W wielu przypadkach wymagania użytkownika nie są uwzględniane na początku procesu projektowania i czasami są uwzględniane dopiero podczas opracowywania prób z użytkownikami w celu oceny ostatecznych koncepcji (często, gdy jest już za późno na zmiany). To samo w sobie jest głównym problemem przy opracowywaniu skutecznych produktów i procesów, które konkretnie spełniają potrzeby użytkowników. Kolejną kwestią związaną z wymaganiami użytkowników w zakresie cyberbezpieczeństwa są techniki badań kryminalistycznych, częściej stosowane w dochodzeniach w sprawie wypadków, aby zapewnić wgląd w możliwości i ograniczenia użytkowników w określonym momencie wystąpienia błędu. Częściej podczas pisania specyfikacji wymagań identyfikuje się i analizuje różne domeny.



Na przykład, jeśli projektowano inteligentny system telewizji przemysłowej (CCTV), konieczne byłoby rozważenie:

• Domena wewnętrzna – rozwijany produkt i użytkownicy (np. CCTV, operatorzy), w tym różne poziomy wymagań systemowych w stosunku do wymagań na poziomie produktu.

• Domena zewnętrzna – klient, któremu ma służyć (np. do którego raportuje operator CCTV).

• Aktorzy — ludzie lub inne elementy systemu, które wchodzą w interakcję z systemem (np. operator korzystający z inteligentnego oprogramowania lub czujniki kamery, które muszą wchodzić w interakcję z oprogramowaniem itp.).

• Wymagania dotyczące danych – modele danych i progi.

• Wymagania funkcjonalne – deskryptory procesów (przepływy zadań i interakcje), wejścia/wyjścia, komunikaty itp.

Oferuje to użyteczny sposób konceptualizacji wymagań i zrozumienia wymagań niefunkcjonalnych, takich jak ocena jakości, solidność, integralność systemu (bezpieczeństwo) i odporność. Jednak często potrzebne jest bardziej szczegółowe podejście do mapowania wymagań użytkowników. Wymagania użytkownika są często ograniczone konkretnym „kontekstem zastosowania" badań, ponieważ zapewnia to granice projektu, a także ramy odniesienia do przekazywania problemów użytkownikom końcowym i innym zainteresowanym stronom. Aby to osiągnąć, często konieczne jest ustalenie priorytetów potencjalnych rozwiązań, aby zapewnić odpowiednie zarządzanie oczekiwaniami. Dążenie do zrozumienia wymagań konkretnych użytkowników końcowych i zaangażowanie kluczowych interesariuszy w rozwój nowych systemów lub protokołów jest istotną częścią każdego procesu

projektowania. W odpowiedzi na to rozwinęło się formalne pozyskiwanie wymagań użytkownika i ergonomia partycypacyjna, aby wspierać te obszary badań, generowania rozwiązań i ostatecznie własności rozwiązań . Wymagania użytkownika obejmują krytyczne elementy, których użytkownicy końcowi i interesariusze potrzebują i oczekują od produktu lub procesu. Wymagania te obejmują wyłaniające się zachowania i aby to osiągnąć, wymagane są pewne ramy zrozumienia potencjału i wiarygodnych zachowań . Prawdopodobne zachowania obejmują wszystkie możliwe zachowania, które mogą wystąpić. Są one następnie mapowane na wymagania systemowe, które wyrażają, w jaki sposób system interaktywny powinien być zaprojektowany, wdrożony i używany. Jednakże te dwa czynniki nie zawsze są zrównoważone i mogą pojawić się rozwiązania, które nie zostaną w pełni wykorzystane lub wykorzystane zgodnie z przeznaczeniem. Podejścia do ergonomii partycypacyjnej mają na celu włączenie użytkowników końcowych i szerszych interesariuszy do analizy pracy, procesów projektowania i generowania rozwiązań, ponieważ ich reakcje, interakcje, zoptymalizowane wykorzystanie i akceptacja rozwiązań ostatecznie zadecydują o skuteczności i powodzeniu ogólnej wydajności systemu. Podejścia skoncentrowane na użytkowniku zastosowano w tak szerokich obszarach badawczych, jak opieka zdrowotna, projektowanie produktów, interakcja człowiek-komputer, a ostatnio bezpieczeństwo i zwalczanie terroryzmu. Wspólnym celem jest skuteczne przechwytywanie informacji z perspektywy użytkownika, tak aby można było następnie zaprojektować wymagania systemowe tak, aby wspierały potrzeby użytkownika w określonych kontekstach użytkowania. Pozyskiwanie wymagań charakteryzuje się szeroko zakrojonymi działaniami komunikacyjnymi pomiędzy szeroką gamą osób z różnych środowisk i obszarów wiedzy, w tym użytkownikami końcowymi, interesariuszami, właścicielami lub liderami projektów, mediatorami (często w roli ekspertów od czynników ludzkich) i programistami . Jest to proces interaktywny i partycypacyjny, który powinien umożliwić użytkownikom wyrażenie własnej wiedzy lokalnej, a projektantom wykazanie się zrozumieniem, aby zapewnić wspólną bazę projektową. Użytkownicy końcowi są często ekspertami w swoich konkretnych obszarach pracy i posiadają głęboką wiedzę zdobytą z biegiem czasu, którą często trudno jest przekazać innym . Użytkownicy często nie zdają sobie sprawy, jakie informacje są cenne dla badań i opracowywania rozwiązań, ani w jakim stopniu ich wiedza i doświadczenie mogą informować i wpływać na sposób ich pracy.

RÓWNOWAGA MOŻLIWOŚCI TECHNOLOGICZNYCH I LUDZKICH

W obszarze cyberbezpieczeństwa uwzględnienie wymagań użytkowników może być niezwykle trudne. Mając na uwadze wcześniejsze kwestie związane z cyberbezpieczeństwem, często wyzwaniem jest identyfikacja użytkowników, którzy są kluczowi dla każdego dochodzenia, i dotarcie do nich. Na przykład, gdy zaufanie użytkownika zostało naruszone (np. za pośrednictwem serwisu społecznościowego lub innej formy ataku typu phishing), użytkownicy mogą czuć się zawstydzeni, winni za wypłacenie środków fałszywemu dostawcy i mogą nie chcieć zwracać na siebie uwagi. Pod wieloma względami może to być podobne w przypadku większych korporacji, które mogą być celem oszustów stosujących taktykę kradzieży tożsamości, aby udawać legalnych klientów. Chociaż istnieją zabezpieczenia wspierające interakcję użytkownika i poprawiające jego doświadczenie, ważne jest, aby upewnić się, że spełniają one oczekiwania użytkowników, dla których są przeznaczone. W kontekście świata rzeczywistego wiele aspektów bezpieczeństwa i identyfikacji zagrożeń w przestrzeni publicznej w dalszym ciągu zależy od wydajności personelu bezpieczeństwa na pierwszej linii frontu. Jednakże odpowiedzialność ta często spoczywa na barkach pracowników, którzy są nisko opłacani, słabo zmotywowani i którym brakuje wyższego poziomu wykształcenia i szkolenia (Hancock i Hart, 2002). Rozwiązania bezpieczeństwa stosowane w świecie rzeczywistym próbują ucieleśniać złożone, skupione na użytkowniku systemy socjotechniczne, w których wielu różnych użytkowników współdziała na różnych poziomach organizacyjnych, aby zapewnić możliwości bezpieczeństwa skupione na technologii. Z perspektywy makroergonomii możliwe jest zbadanie, w jaki sposób czynniki systemowe

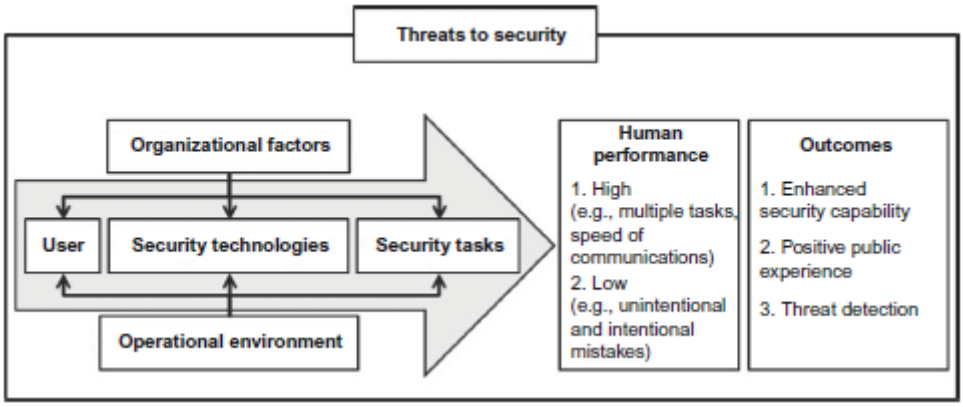
przyczyniają się do powodzenia inicjatyw w zakresie cyberbezpieczeństwa i gdzie mogą istnieć luki. Podejście to przyjmuje całościowe spojrzenie na bezpieczeństwo poprzez ustanowienie podmiotów społeczno-technicznych, które wpływają na funkcjonowanie systemu pod względem integralności, wiarygodności i wydajności . W tej perspektywie ważne jest również rozważenie szerszych kwestii etycznych badań nad bezpieczeństwem, a w odniesieniu do dochodzeń w sprawie cyberbezpieczeństwa – równowagi między bezpieczeństwem publicznym a potrzebą interwencji w zakresie bezpieczeństwa. Aspekty prywatności i poufności leżą u podstaw wielu wyzwań etycznych związanych z pozyskiwaniem wymagań użytkowników, w przypadku których badacze muszą upewnić się, że:

• Użytkownicy końcowi i zainteresowane strony czują się komfortowo co do rodzaju udostępnianych informacji i sposobu, w jaki informacje mogą zostać wykorzystane.

• Użytkownicy końcowi nie są zobowiązani do łamania jakichkolwiek umów i obowiązków zawartych ze swoimi pracodawcami lub stowarzyszonymi organizacjami.

Pod wieloma względami te kwestie etyczne są regulowane przez kodeksy postępowania regulowane przez organizacje zawodowe, takie jak Brytyjskie Towarzystwo Psychologiczne (BPS), ale ważne jest, aby śledczy jasno określili cel dochodzenia oraz ustalili jasne i uzasadnione granice zamierzonego wykorzystania i komunikacja

Zebrane dane. Podejście makro różni się od mikroergonomii, która tradycyjnie skupia się na interakcji pojedynczego użytkownika i jego natychmiastowym wykorzystaniu technologii. Często stanowiło to punkt wyjścia dla tradycyjnego podejścia do czynnika ludzkiego; jednakże poprzez zrozumienie zagadnień na poziomie makro złożoność czynników społeczno-technicznych można przełożyć na czynniki na poziomie mikro w celu bardziej szczegółowej analizy . Na przykład Kraemer i inni zbadali kwestie związane z kontrolą bezpieczeństwa oraz inspekcją ładunków i pasażerów, przyjmując podejście makroergonomiczne. Zaproponowano pięcioczynnikową strukturę, która przyczynia się do „obciążenia stresem" pracowników ochrony na pierwszej linii frontu w celu oceny i przewidywania indywidualnych wyników w ramach ogólnego systemu bezpieczeństwa .



Osiągnięto to poprzez identyfikację interakcji między: czynnikami organizacyjnymi (np. szkoleniem, wsparciem kierownictwa i strukturą zmiany), charakterystyką użytkownika (tj. zabójstwami poznawczymi operatora, szkoleniem), technologiami bezpieczeństwa (np. wydajnością i użytecznością stosowanych technologii) i zadania związane z bezpieczeństwem (np. ładowanie zadań i środowisko operacyjne). Centralnym czynnikiem struktury jest użytkownik (np. operator bezpieczeństwa na pierwszej linii, osoba przeprowadzająca kontrolę, inspektor), który posiada określone umiejętności w zakresie systemu bezpieczeństwa. Operator bezpieczeństwa może używać technologii i narzędzi do

wykonywania różnorodnych zadań kontroli bezpieczeństwa, które wspierają ogólne możliwości bezpieczeństwa. Jednakże wpływają na to czynniki związane z zadaniem i obciążeniem pracą (np. przeciążenie/niedociążenie/monotonia zadania/powtarzanie). Ponadto czynniki organizacyjne (np. szkolenia, wsparcie kierownictwa, kultura i struktury organizacyjne), a także środowisko operacyjne (np. hałas, klimat i temperatura) również przyczyniają się do ogólnej zdolności bezpieczeństwa. Podejście to pomaga zidentyfikować czynniki makroergonomiczne, w przypadku których złożoność zadania i wynikająca z niego wydajność człowieka w systemie bezpieczeństwa mogą obejmować błędy (np. przeoczone sygnały o zagrożeniu i fałszywe alarmy) lub naruszenia (np. naruszone lub zaadaptowane protokoły w odpowiedzi na dynamiczny wymagania środowiska operacyjnego) (Kraemer i in., 2009). Te ramy makroergonomiczne wykorzystano jako podstawę do zrozumienia wymagań użytkowników w obszarze przeciwdziałania terroryzmowi, koncentrując się na oddziałujących na siebie czynnikach i ich wpływie na ogólną wydajność systemów bezpieczeństwa, w tym na użytkowników i procesy organizacyjne . Ramy te zapewniają użyteczną perspektywę na cyberbezpieczeństwo i można je przerysować, aby ucieleśnić typowego użytkownika i zapewnić podstawę do badania wymagań użytkownika. W ten sposób cyberbezpieczeństwo można rozumieć w kategoriach użytkownika (np. osoby dorosłej lub dziecka), który posiada szereg umiejętności, ale ma także słabe punkty w całym systemie bezpieczeństwa cybernetycznego (np. dziecko może nie znać dokładnego tożsamość osoby, która zaprzyjaźnia się z nią na czacie; dorosły może nie zdawać sobie sprawy ze znaczenia przekazywanie znajomym szczegółów dotyczących krewnego w serwisie społecznościowym; osoba samotna może być podatna na podejście innych ludzi pod pretekstem przyjaźni). Użytkownik ma do dyspozycji szereg technologii i narzędzi umożliwiających wykonywanie różnorodnych zadań, z których część będzie skupiać się bezpośrednio lub pośrednio na jego własnym bezpieczeństwie lub na szerszym bezpieczeństwie sieci (np. protokoły logowania/hasła, sprawdzanie tożsamości użytkownika) i podobnie jak w przypadku ram bezpieczeństwa, wydajność jest kształtowana przez czynniki związane z zadaniem i obciążeniem pracą (np. przeciążenie/niedociążenie/monotonia/powtarzanie zadań). W obszarze cyberbezpieczeństwa kluczową różnicą w ustanowionych ramach bezpieczeństwa jest to, że czynniki organizacyjne są zastępowane czynnikami dostawcy usług. W ten sposób polityki cybernetyczne mogą narzucać określone środki bezpieczeństwa, ale jeśli chodzi o formalną zdolność bezpieczeństwa (nadzorowanie sieci w podobny sposób, w jaki pracownicy ochrony pilnują przestrzeni publicznej – przy wsparciu formalnego szkolenia, wsparcia kierownictwa, kultury i struktur organizacyjnych) nie ma takich zaopatrzenie. Rzeczywiście, indywidualne szkolenia użytkowników mają w najlepszym przypadku charakter doraźny i w większości przypadków nie istnieją. Środowisko operacyjne jest ograniczone wyłącznie przez użytkownika mającego dostęp do sieci. Użytkownik może wykonywać swoje zadania zarówno siedząc w zatłoczonym pociągu (gdzie inni mogą oglądać swoje interakcje lub nagrywać wideo, jak wprowadzają dane logowania/hasło), jak i w zaciszu własnego domu. Szczególnie interesującym obszarem cyberbezpieczeństwa jest zaufanie użytkowników. Z bardziej tradycyjnej perspektywy, jak w przypadku każdej formy technologii lub zautomatyzowanego procesu, musi istnieć zaufanie do systemu, specyficzna funkcjonalność komponentów systemu, komunikacja w ramach systemu i jasne rozróżnienie, gdzie w systemie znajduje się władza. Stosując to do zaufania cybernetycznego, pojawia się szereg problemów:

• Akceptacja transakcji on-line przez użytkowników jest wyważona z ryzykiem i szacunkowymi korzyściami.

• Zaufanie powstaje na podstawie technologii stosowanej w interakcjach (np. postrzeganie bezpiecznych protokołów pod kątem podatności sieci otwartych), a także na wiarygodność osób lub organizacji biorących udział w procesie interakcji .

• Aby zbudować zaufanie w Internecie, nacisk kładzie się na to, aby osoby i organizacje prezentowały się jako godne zaufania. Aby to osiągnąć, ważne jest, aby komunikować zaufanie w sposób, z którym użytkownicy będą się identyfikować (np. poprzez reputację, wydajność, a nawet wygląd strony internetowej).

• Interakcje internetowe oferują użytkownikom wiele doświadczeń „po raz pierwszy" (np. kupowanie produktów na różnych stronach internetowych lub dołączanie do różnych pokojów rozmów). Sugeruje to, że osoby, którym brakuje doświadczenia w transakcjach internetowych i organizacjach internetowych, mogą mieć inny poziom zaufania w porównaniu z osobami z większym doświadczeniem.

• Naruszenia bezpieczeństwa w interakcji człowiek-komputer mogą wynikać z przyczyn systematycznych, takich jak przeciążenie poznawcze, brak wiedzy na temat bezpieczeństwa oraz rozbieżności między zachowaniem systemu komputerowego a modelem mentalnym użytkownika.

• W pewnym stopniu użytkownicy opracują własne modele mentalne i takie interakcje, na podstawie których będą mogli ocenić kolejne procedury. Zrozumienie konstrukcji i ewolucji tych modeli mentalnych oraz sposobu ich ewolucji jest kluczowym czynnikiem w zrozumieniu oczekiwań użytkowników w zakresie nowych interakcji cybernetycznych.

Czynniki te można powiązać z ramami cyberbezpieczeństwa, aby uwypuklić kluczowe kwestie w badaniu wymagań użytkowników .

Czynniki: Charakterystyka systemu

Czynniki dostawcy usług:

• Funkcje prywatności, pewności i bezpieczeństwa

• Krzepkość

• Charakterystyka odporna na awarie (lub redundancja)

Charakterystyka użytkownika:

• Skłonność do zaufania

• Doświadczenie i biegłość w korzystaniu z Internetu

• Oczekiwanie na to, co zostanie zapewnione

• Poziomy świadomości na temat zagrożeń cyberbezpieczeństwa

Narzędzia bezpieczeństwa:

• Sygnały obecności społecznej

• Możliwości dostosowywania i personalizacji

• Ograniczone interfejsy umożliwiające swobodne korzystanie (np. możliwość przesyłania szczegółów przez bezpieczną sieć)

Zadania bezpieczeństwa:

• Interfejs użytkownika charakteryzuje się wysokim stopniem użyteczności

• Wyraźne cechy bezpieczeństwa

• Jakość/ilość/aktualność informacji

• Charakterystyka graficzna

Środowisko operacyjne:

• Doświadczenie i znajomość firmy internetowej

• Łatwość użycia w różnych kontekstach użycia

• Komunikowanie różnych poziomów zagrożenia

Korzystanie z ram bezpieczeństwa cybernetycznego w celu identyfikacji potencjalnych problemów związanych z wymaganiami użytkownika jest ważną częścią określania specyfikacji cybernetycznych. Aby jednak uchwycić znaczące dane, należy również wziąć pod uwagę zakres dostępnych metod. Stosowanie metod formalnych w weryfikacji poprawności systemów interaktywnych powinno uwzględniać także analizę zachowań człowieka w interakcji z interfejsem i uwzględniać wszelkie zależności pomiędzy działaniami użytkownika, jego celami i środowiskiem.

PRZEPROWADZANIE WYMAGAŃ UŻYTKOWNIKA

Jak wspomniano wcześniej, chociaż istnieją metody identyfikacji i gromadzenia potrzeb użytkowników w dziedzinie bezpieczeństwa, są one stosunkowo słabo rozwinięte. Dopiero w ostatniej dekadzie zaczęto systematycznie analizować aspekty bezpieczeństwa systemów interaktywnych; jednakże opublikowano niewiele badań na temat zrozumienia pracy personelu i systemów bezpieczeństwa, co prowadzi do braku studiów przypadków lub wytycznych dotyczących tego, w jaki sposób można przyjąć metody lub w jaki sposób zostały one wykorzystane w różnych warunkach bezpieczeństwa. W rezultacie konieczne jest ponowne rozważenie podstawowych zagadnień związanych z pozyskiwaniem wymagań użytkowników, które można następnie zastosować w badaniach nad bezpieczeństwem. Pozyskiwanie wymagań użytkowników stwarza przed badaczami kilka wyzwań, zwłaszcza jeśli chodzi o rekrutację reprezentatywnych użytkowników końcowych i innych interesariuszy, od których zależy cały proces. Co równie ważne, konieczne jest pozyskanie i kategoryzowanie/uszeregowanie odpowiedniej wiedzy fachowej i priorytetów oraz przekazywanie ich projektantom i decydentom, a także użytkownikom końcowym i innym zainteresowanym stronom. Jednym z pierwszych kroków w procesie pozyskiwania wymagań użytkownika jest zrozumienie, że mogą istnieć różne poziomy użytkowników końcowych lub zainteresowanych stron. Chociaż terminy „użytkownik końcowy" i „interesariusz" są często mylone, interesariusze nie zawsze są użytkownikami końcowymi produktu lub procesu, ale mają szczególną inwestycję lub interes w wyniku i jego wpływie na użytkowników lub szerszą społeczność (Mitchell i in., 1997). Termin „użytkownik końcowy" lub „użytkownik główny" jest powszechnie definiowany jako osoba, która będzie korzystać z określonego produktu lub procesu. W wielu przypadkach użytkownicy i interesariusze będą mieli różne potrzeby, a często ich cele lub oczekiwania wobec produktu lub procesu mogą być sprzeczne . Te rozróżnienia i podstawowe informacje na temat użytkowników, interesariuszy i konkretnych kontekstów użycia pozwalają projektantom i twórcom systemów na osiągnięcie świadomych wyników . W dziedzinie bezpieczeństwa, a dokładniej w cyberbezpieczeństwie, kluczowym wyzwaniem na początkowych etapach pozyskiwania wymagań

użytkowników jest uzyskanie dostępu i wybór odpowiednich użytkowników i interesariuszy. W „wrażliwych domenach" szczególnie skutecznymi metodami nawiązania kontaktu z docelowymi odbiorcami są próbkowanie w formie kuli śnieżnej lub łańcuchowej, często wspierane poprzez skumulowane polecenia dokonywane przez osoby, które dzielą się wiedzą lub wchodzą w interakcję z innymi na poziomie operacyjnym lub mają wspólne interesy w związku z dochodzeniem. Ta metoda próbkowania jest przydatna, gdy agencje i organizacje zajmujące się bezpieczeństwem mogą niechętnie udostępniać poufne i wrażliwe informacje osobom, które uważają za „obce". Metodę tę stosowano w obszarach badań nad używaniem narkotyków i uzależnieniami, gdzie informacje są ograniczone i gdzie podejście kuli śnieżnej można zainicjować poprzez kontakt osobisty lub za pośrednictwem informatora . Jednakże jednym z problemów związanych z taką metodą doboru próby jest to, że weryfikacja kwalifikowalności uczestników może być trudna, ponieważ badacze polegają na procesie skierowania, a próba obejmuje tylko jeden podzbiór odpowiedniej populacji użytkowników. Mówiąc dokładniej, w obszarze cyberbezpieczeństwa użytkownicy końcowi mogą nie znać się wystarczająco dobrze, aby takie podejście nabrało tempa. Chociaż pozyskiwanie wymagań użytkowników zwykle odbywa się wśród szerokiego grona użytkowników i interesariuszy, niektóre z tych domen są bardziej ograniczone i stanowią większe wyzwanie niż inne pod względem poufności, anonimowości i prywatności. Te wrażliwe domeny mogą obejmować te, które dotyczą dzieci, osób starszych lub niepełnosprawnych, systemów opieki zdrowotnej, środowiska personelu/pacjentów, handlu i innych dziedzin, w których informacje są często niedostępne publicznie (Gaver i in., 1999). Ponadto niektóre organizacje ograniczają zakres informacji, jakie pracownicy mogą udostępniać podmiotom zewnętrznym na temat ich zadań, ról, strategii, wykorzystania technologii i wizji przyszłości, aby chronić stanowisko handlowe lub konkurencyjne. W obszarze cyberbezpieczeństwa organizacje są bardzo wyczulone na ujawnianie wszelkich luk systemowych, które mogą zostać odebrane przez opinię publiczną jako brak świadomości bezpieczeństwa lub wykorzystane przez konkurencję szukającą dźwigni rynkowej. Takie domeny powodują dalsze komplikacje w ostatecznym raportowaniu ustaleń, aby pomóc w szerszym zrozumieniu potrzeb użytkowników w tych domenach.

Przechwytywanie i komunikowanie wymagań użytkowników

Istnieje wiele metod wykorzystujących czynnik ludzki, takich jak kwestionariusze, ankiety, wywiady, grupy fokusowe, obserwacje i przeglądy etnograficzne, a także formalne analizy zadań lub powiązań, które można wykorzystać jako podstawę do pozyskiwania wymagań użytkownika. Metody te zapewniają różne możliwości interakcji między badaczem a grupą docelową, a co za tym idzie, zapewniają różne rodzaje i poziomy danych. Aby uszczegółowić badane zagadnienia, często wybiera się szereg metod uzupełniających. Można na przykład zastosować wywiady i grupy fokusowe w celu uzyskania dalszych informacji lub uwypuklenia problemów, które zostały początkowo zidentyfikowane w kwestionariuszach lub ankietach. W porównaniu z bezpośrednią interakcją pomiędzy badaczem a uczestnikiem (np. wywiady) metody pośrednie (np. kwestionariusze) mogą dotrzeć do większej liczby respondentów i są tańsze w stosowaniu, ale nie są skuteczne w badaniu skomplikowanych zagadnień lub wiedzy ukrytej . Można również wykorzystać grupy fokusowe, w których osoba przeprowadzająca wywiad pełni rolę organizatora grupy, moderatora i podpowiedzi, aby zachęcić do dyskusji na kilka zagadnień wokół wcześniej zdefiniowanych tematów. Jednakże grupy fokusowe mogą być kosztowne i trudne do zorganizowania, w zależności od stopnia anonimowości wymaganej przez każdego z uczestników. Są one również notorycznie „na chybił trafił" w zależności od dostępności uczestników poszczególnych sesji. Ponadto potrzebują skutecznego zarządzania, aby wszyscy uczestnicy mieli możliwość wniesienia wkładu bez konkretnych osób dominujących w interakcji lub osób znajdujących się pod presją rówieśników, aby nie wypowiadali się na temat konkretnych kwestii (Friedrich i van der Poll, 2007). Podobnie jak w przypadku wielu analiz jakościowych, należy również zwrócić uwagę na sposób uwzględniania wyników przy określaniu wymagań. Podczas korzystania z metod

interaktywnych ważne jest, aby zapewnić uczestnikom możliwość spontanicznego wyrażania swojej wiedzy, a nie tylko odpowiadania na kierowane pytania badacza. Dzieje się tak dlatego, że istnieje niebezpieczeństwo, że pytania bezpośrednie będą obarczone uprzedzeniami, które mogą uniemożliwić badaczom zbadanie kwestii, których jeszcze nie zidentyfikowali. Na tej podstawie badacze powinni przyjąć rolę „uczniów", a nie „testerów hipotez". Można również zastosować metody obserwacyjne i etnograficzne, aby umożliwić badaczom zebranie wglądu w czynniki socjotechniczne, takie jak wpływ strażników, moderatorów lub bardziej formalnych mechanizmów w cyberbezpieczeństwie. Jednakże obserwacje i przeglądy etnograficzne mogą być natrętne, szczególnie w obszarach wrażliwych, gdzie prywatność i poufność mają kluczowe znaczenie. Ponadto obecność obserwatorów może wywołać zachowania, które nie są normalne dla obserwowanej jednostki lub grupy, ponieważ celowo postępują zgodnie z formalnymi procedurami lub zachowują się w sposób społecznie pożądany co więcej, metoda ta zapewnia dużą ilość bogatych danych, których analiza może być czasochłonna. Jednakże, jeśli jest stosowana prawidłowo i gdy badacz dobrze rozumie obserwowaną dziedzinę, metoda ta może dostarczyć bogatych jakościowych i ilościowych danych ze świata rzeczywistego . Badacze często skupiają się na zadaniach wykonywanych przez użytkowników w celu wydobycia ukrytych informacji lub zrozumienia kontekstu pracy . Zatem wykorzystanie metod analizy zadań do identyfikacji problemów i wpływu interakcji użytkownika na wydajność systemu jest głównym podejściem w kontekście czynników ludzkich . Analizę zadań definiuje się jako badanie tego, co musi wykonać użytkownik/system, włączając w to aktywność fizyczną i procesy poznawcze, aby osiągnąć określony cel . Scenariusze są często używane do zilustrowania lub opisania typowych zadań lub ról w określonym kontekście . Generalnie istnieją dwa typy scenariuszy: te, które przedstawiają i wychwytują aspekty rzeczywistych warunków pracy, dzięki czemu badacze i użytkownicy mogą przekazać swoje zrozumienie zadań, aby wspomóc proces programowania; oraz te używane do przedstawienia, jak użytkownicy mogą sobie wyobrazić korzystanie z przyszłego systemu, który jest w trakcie opracowywania . W tym drugim przypadku badacze często opracowują „osoby użytkowników", które reprezentują, w jaki sposób różne klasy użytkowników mogą wchodzić w interakcję z przyszłym systemem i/lub jak system będzie pasował do zamierzonego kontekstu użycia. Czasami jest to przekazywane za pomocą technik scenorysowych przedstawianych w postaci skryptów, diagramów połączeń lub diagramów koncepcyjnych w celu zilustrowania procesów i punktów decyzyjnych będących przedmiotem zainteresowania. Chociaż różne metody pomagają badaczom w określeniu wymagań użytkowników, ważne jest, aby przekazać ustalenia odpowiednim użytkownikom i zainteresowanym stronom. Istnieje kilka technik związanych z doświadczeniem użytkownika i projektowaniem skoncentrowanym na użytkowniku, służących do przekazywania wizji badaczom i użytkownikom. Obejmują one zazwyczaj modelowanie oparte na scenariuszach (np. narracje w tekście tabelarycznym, osobowości użytkowników, szkice i media nieformalne) oraz mapowanie koncepcji (np. skrypty, sekwencje zdarzeń, analizy powiązań i zadań), w tym działania i obiekty na etapie projektowania wymagań użytkownika. Modelowanie oparte na scenariuszach można wykorzystać do przedstawienia zadań, ról, systemów oraz tego, w jaki sposób wchodzą w interakcję i wpływają na cele zadań, a także identyfikuje powiązania i zależności pomiędzy użytkownikiem, systemem i środowiskiem . Mapowanie koncepcji to technika, która reprezentuje obiekty, działania, zdarzenia (a nawet emocje i uczucia), dzięki czemu zarówno badacze, jak i użytkownicy wypracowują wspólne zrozumienie w celu zidentyfikowania luk w wiedzy. Wizualne reprezentacje powiązań między zdarzeniami i obiektami na mapie pojęć lub analizie powiązań mogą pomóc w zidentyfikowaniu sprzecznych potrzeb, stworzeniu wzajemnego zrozumienia oraz wzmocnieniu przywoływania i zapamiętywania krytycznych wydarzeń . Przypadków użycia można również używać do reprezentowania typowych interakcji, w tym profili, zainteresowań, opisów stanowisk i umiejętności, w ramach reprezentacji wymagań użytkownika . Scenariusze z personami można wykorzystać do opisania, jak użytkownicy mogą zachować się w określonych sytuacjach, aby zapewnić bogatsze

zrozumienie kontekstu per se. Persony zazwyczaj przedstawiają profil konkretnego użytkownika, interesariusza lub rola oparta na informacjach z wielu źródeł (np. typowe dziecko korzystające z czatu, rodzic próbujący kontrolować bezpieczeństwo obecności swojego dziecka w Internecie, kupujący, osoba korzystająca z interfejsu bankowości domowej). Następnie przekazywane jest połączenie i synteza kluczowych cech w ramach jednego profilu, który można następnie wykorzystać jako pojedynczy punkt odniesienia (np. Mary to 8-letnia dziewczynka, która nie rozumie do końca technik uwodzenia w Internecie; Malcolm to 60-latek nieświadomy taktyk phishingu). W niektórych przypadkach osobom podaje się imiona i informacje ogólne, takie jak wiek, wykształcenie, odbyte ostatnio szkolenia, a nawet ogólne obrazy/zdjęcia, aby uczynić je bardziej realistycznymi lub reprezentatywnymi dla typowego użytkownika. W innych przypadkach osoby są wykorzystywane anonimowo w celu przekazania ogólnych cech, które mogą mieć zastosowanie w szerszej grupie demograficznej. Pozyskiwanie wymagań użytkowników w przypadku użytkowników pracujących w wrażliwych domenach wiąże się również z kwestiami anonimowości osobistej i poufności danych). Aby je chronić, można zastosować anonimowość i pseudonimowość w celu ukrycia osób, ról i relacji między rolami . W ten sposób nie należy wiązać cech identyfikujących uczestników z danymi lub należy zastosować podejście, które w szczególności wykorzystuje fikcyjne osoby w celu zilustrowania i zintegrowania obserwacji wielu uczestników. Jeśli zostanie to zrobione prawidłowo, osoby te można następnie wykorzystać jako skuteczne narzędzie komunikacji bez narażania zaufania zbudowanego w procesie pozyskiwania klientów. Stosowanie różnorodnych metod uwzględniających czynnik ludzki pozwala badaczom lepiej zrozumieć, w jaki sposób cyberbezpieczeństwo jako proces może działać w oparciu o perspektywę systemów społeczno-technicznych. Bez szeregu metod do zastosowania i bez wybrania tych, które są najbardziej odpowiednie dla konkretnego zapytania, istnieje niebezpieczeństwo, że najlepsze dane zostaną pominięte. Ponadto bez wykorzystania narzędzi do przekazywania wniosków z działań związanych z wymaganiami użytkowników cały proces byłby niekompletny, a użytkownicy końcowi i inne zainteresowane strony straciliby możliwości zdobycia wiedzy na temat bezpieczeństwa cybernetycznego i/lub wniesienia dodatkowego wglądu w swoje role. Takie podejście umożliwia badaczom znacznie lepsze zrozumienie szerszego obrazu, takiego jak kontekst i szersze systemy, a także bardziej szczegółowe zrozumienie konkretnych zadań i celów.

WNIOSEK

Podejście skoncentrowane na użytkowniku jest niezbędne do zrozumienia cyberbezpieczeństwa z perspektywy czynnika ludzkiego. Ważne jest również zrozumienie kontekstu pracy i powiązanych czynników wpływających na ogólną wydajność systemu bezpieczeństwa. Dostosowanie ram bezpieczeństwa w pewnym stopniu pomaga w skupieniu uwagi. Jednakże, chociaż istnieje wiele formalnych i ustalonych metodologii, istotne jest, aby praktyk przed wybraniem konkretnej metodologii rozważył kluczowe kwestie kontekstowe opisane w tym rozdziale. Chociaż różne metody i narzędzia mogą rzeczywiście być pomocne w uzyskaniu wglądu w poszczególne aspekty pozyskiwania wymagań w zakresie cyberbezpieczeństwa, należy zachować ostrożność, ponieważ obecnie nie istnieje odpowiedni model pozyskiwania takich danych specjalnie dla cyberbezpieczeństwa. Obecnie dochodzenia opierają się na doświadczeniu, zrozumieniu i umiejętnościach badacza w podejmowaniu decyzji, jakie podejście najlepiej przyjąć w celu zgromadzenia solidnych danych, które można następnie wprowadzić z powrotem do procesu systemowego.

Zaawansowane technologicznie dochodzenia w sprawie cyberprzestępczości

WSTĘP

Informacje cyfrowe stały się wszechobecne w dzisiejszym świecie; w celu utrzymania „normalnego” życia, komunikacji i ogólnej socjalizacji coraz większe znaczenie ma informacja cyfrowa. Powszechne

wykorzystanie urządzeń sieciowych umożliwia obecnie każdemu, z dowolnego kraju, zaatakowanie lub wykorzystanie urządzenia cyfrowego do ataku na sąsiada lub osobę na drugim końcu świata za pomocą zaledwie kilku kliknięć przycisku. Niewiedza ludzi, w tym przestępców, na temat tego, jakie informacje przechowuje urządzenie i ile danych generuje, sprawia, że odpowiednio przeszkolony i wyposażony ekspert jest w stanie odzyskać i wykorzystać informacje z niemal każdego urządzenia cyfrowego. Te same informacje cyfrowe mogą teraz stanowić dowód i informacje wywiadowcze, które mogą mieć kluczowe znaczenie w dochodzeniach karnych i cywilnych. Zrozumienie zagrożenia cyberprzestępczością i cyberterroryzmem pozwala nam umieścić w odpowiednim kontekście obecną sytuację techniczną, jednak identyfikacja potencjału ataku to dopiero początek. W tym rozdziale zajmiemy się definiowaniem zaawansowanych technologicznie dochodzeń i procesów dowodowych, które mają zastosowanie we wszystkich dochodzeniach. Opis i procesy będą pomocne w dochodzeniu w sprawie przestępstwa lub złośliwego działania po wystąpieniu zdarzenia.

Zaawansowane technologicznie dochodzenia i kryminalistyka

Termin „kryminalistyka" może przywodzić na myśl popularne amerykańskie seriale telewizyjne. Programy telewizyjne wychwalające analizy kryminalistyczne, takie jak te, zarówno pomogły, jak i w pewnym stopniu przeszkodziły kryminalistyce. Pomogło to w przybliżeniu koncepcji możliwości kryminalistycznych szerszemu gronu odbiorców, dzięki czemu wzrósł poziom świadomości. I odwrotnie, utrudnia to również, wyolbrzymiając możliwości techniczne kryminalistów: niezależnie od tego, co sugerują programy telewizyjne, jest całkowicie możliwe, że nawet najwybitniejsi eksperci nie będą w stanie odzyskać danych. Jednak, co zaskakujące, wielu użytkowników pozostaje nieświadomych rodzaju danych, które można pozyskać z różnych źródeł cyfrowych i które staną się podstawą dochodzenia. Urządzenia cyfrowe są zasadniczo częścią każdego dochodzenia w taki czy inny sposób:

• Wykorzystywane do prowadzenia działalności objętej dochodzeniem: urządzenie stanowi główny przedmiot działalności, np. główne urządzenie do przechowywania i dystrybucji w przypadku nieprzyzwoitych zdjęć dzieci.

• Cel badanego działania: urządzenie jest „ofiarą" np. w przypadku włamania.

• Wspiera badaną czynność: urządzenie służy do ułatwienia czynności, np. telefony komórkowe używane do komunikacji.

Zaawansowane technologicznie dochodzenia dotyczą analizy i interpretacji danych z urządzeń cyfrowych, często przywoływane w przypadku wystąpienia zdarzenia (karnego lub cywilnego). Nie chodzi im wyłącznie o wykorzystanie najbardziej zaawansowanej technologii do wykonania pracy. Duża część tego, co się robi, ma w rzeczywistości charakter „niski poziom technologii" w tym sensie, że pracę wykonuje umysł badacza i interpretuje dostępne dane. Podstawowym celem zaawansowanych dochodzeń jest ustalenie, co się stało i przez kogo.

PODSTAWOWE KONCEPCJE BADAŃ ZAAWANSOWANYCH TECHNOLOGII

Powszechnie uważa się, że dochodzenie dotyczące zaawansowanych technologii obejmuje cztery główne, odrębne elementy, z których wszystkie są ważne dla pomyślnego zakończenia dochodzenia:

1. Gromadzenie: wdrożenie procesu kryminalistycznego w celu zabezpieczenia danych zawartych w dowodzie cyfrowym, zgodnie z przyjętymi wytycznymi i procedurami. Jeżeli dane zostaną wykonane nieprawidłowo, dane uzyskane później mogą nie mieć mocy prawnej w sądzie.

2. Badanie: systematyczny przegląd danych z wykorzystaniem metodologii i narzędzi kryminalistycznych przy jednoczesnym zachowaniu ich integralności

3. Analiza: ocena danych w celu ustalenia przydatności informacji dla wymogów dochodzenia, w tym wszelkich okoliczności łagodzących.

4. Sprawozdawczość: stosowanie odpowiednich metod wizualizacji i dokumentacji w celu sprawozdania na temat tego, co znaleziono w dowodach cyfrowych istotnych dla dochodzenia.

Te cztery główne elementy stanowią podstawę całego procesu dochodzeniowego, pozwalając badaczom zajmującym się zaawansowanymi technologiami i recenzentom produktu końcowego mieć pewność co do jego autentyczności, ważności i dokładności (patrz także Rozdział 4). Ważnym czynnikiem podczas zaawansowanego technologicznie dochodzenia jest utrzymanie „łańcucha dowodowego" eksponatu, tak aby można go było uwzględnić na wszystkich etapach dochodzenia i zachować jego integralność. W przypadku eksponatu fizycznego osiąga się to częściowo poprzez zastosowanie torby na dowody i plomby zabezpieczającej przed manipulacją. Integralność informacji cyfrowych jest utrzymywana w formie jednokierunkowych funkcji skrótu, takich jak MD5, SHA-1 i SHA-256. Jednokierunkowe funkcje skrótu można wykorzystać do utworzenia unikalnego cyfrowego odcisku palca danych; oznacza to, że przy prawidłowym wdrożeniu nawet niewielka zmiana danych spowoduje powstanie zupełnie innego odcisku cyfrowego. Jeśli zachowana zostanie integralność fizyczna i cyfrowa eksponatu, umożliwia to osobie trzeciej weryfikację przeprowadzonego procesu. Jest to istotny czynnik zwiększający szanse na dopuszczenie dowodu w postępowaniu sądowym. Chociaż każdy kraj może mieć własne wytyczne lub najlepsze praktyki w tym zakresie w przypadku postępowania z dowodami cyfrowymi ogólna istota jest prawie zawsze taka sama. W Wielkiej Brytanii stowarzyszenie głównych funkcjonariuszy policji (ACPO) opracowało Przewodnik dobrych praktyk w zakresie dowodów cyfrowych , a w USA istnieje dokument Forensic Examination of Digital Evidence: A Guide for Law Enforcement (Krajowy Instytut Sprawiedliwości, 2004). Dokumenty te nie zawierają szczegółów technicznych dotyczących sposobu przeprowadzania analizy danych cyfrowych, skupiają się bardziej na najlepszych praktykach związanych z zajmowaniem i zabezpieczaniem dowodów. Umiejętność prawidłowego pozyskiwania i przetwarzania dowodów cyfrowych jest niezwykle ważna dla każdego, kto pracuje w dochodzeniach wymagających zaawansowanych technologii. Zdobycie eksponatów stanowi podstawę do solidnego śledztwa. Jeśli nabycie nie zostanie wykonane prawidłowo, integralność lub ciągłość eksponatu jest wątpliwa, wówczas cała sprawa może zakończyć się fiaskiem. Najistotniejsze punkty zostaną omówione w następnych sekcjach.

CYFROWE KRAJOBRAZY

Tradycyjnie cyfrowa kryminalistyka skupiała się na pojedynczym komputerze domowym lub sieci lokalnej (LAN) firmy. Jednak w świecie, w którym sieci są liczne, wraz z pojawieniem się Internetu i masowego rynku urządzeń przenośnych, dowody cyfrowe mogą pochodzić z niemal każdego urządzenia używanego na co dzień. Dlatego też przy przetwarzaniu dowodów cyfrowych ważne jest uwzględnienie różnych dróg technicznych i specyfiki. Pojawienie się zaawansowanych technologii w biznesie i w domu oznacza obecnie, że wymagane są bardziej zaawansowane techniki przechwytywania danych. Doprowadziło to do rozwoju technik gromadzenia danych w czasie rzeczywistym, online i offline. Zakres badania i technologia, która ma zostać zbadana, określą zastosowaną technikę gromadzenia danych. Jednak kluczem do fazy gromadzenia danych jest możliwość potwierdzenia i zweryfikowania integralności przechwyconych danych.

„MIEJSCE ZBRODNI"

Podobnie jak w przypadku każdego rodzaju dochodzenia, ważne jest zaplanowanie go przed jego rozpoczęciem, szczególnie gdy wymagana jest fizyczna obecność na „miejscu zbrodni", nie zawsze będzie to możliwe lub wymagane. Urządzenia cyfrowe mogą pojawić się w każdym dochodzeniu i łatwo przeoczyć znaczenie urządzenia cyfrowego dla określonego rodzaju dochodzenia. Przed przybyciem na „miejsce zbrodni" wywiad przeprowadzony przed przeszukaniem ma kluczowe znaczenie w określeniu układu miejsca zdarzenia, potencjalnej liczby osób lub urządzeń oraz rodzaju informacji cyfrowych istotnych dla dochodzenia. Informacje te umożliwiają organizację sprzętu i zasobów, które mogą być wymagane do przechwycenia lub przechwycenia danych. Należy wcześnie rozważyć, czy urządzenia cyfrowe można usunąć z „miejsca zbrodni", czy też należy przechwycić dane, a następnie dostarczyć je z powrotem do laboratorium w celu analizy. Jeżeli wymagana jest obecność na „miejscu zbrodni", nadrzędną zasadą jest zabezpieczenie dowodów. Nie może to jednak zagrażać bezpieczeństwu osób znajdujących się na miejscu. Po zapewnieniu bezpieczeństwa osobistego można rozpocząć zabezpieczanie materiału dowodowego. Przy pierwszej okazji wszystkie osoby nie biorące udziału w dochodzeniu powinny zostać usunięte z pobliża wszelkich klawiatur lub myszy (lub innego urządzenia wejściowego), aby nie można było nawiązać interakcji z żadnym urządzeniem cyfrowym. Jeśli zostaną pozostawione, ludzie mogą spowodować niewypowiedziane szkody w danych cyfrowych, co znacznie utrudni, jeśli nie uniemożliwi, dalszy etap dochodzenia. Fizyczne „miejsce zbrodni" należy utrwalić za pomocą zdjęć, nagrań wideo i szkiców. Umożliwia to późniejszą identyfikację lokalizacji urządzeń, a także pozwala osobie trzeciej zobaczyć układ i urządzenia na miejscu. Może się zdarzyć, że obrazy te zostaną poddane przeglądowi w późniejszym terminie i po analizie istotne punkty znalezione w danych cyfrowych pozwolą na wyciągnięcie wniosków z tego, co było fizycznie obecne; jak podłączenie nagrywarki DVD USB. Biorąc pod uwagę ogromną liczbę urządzeń cyfrowych, które mogą znajdować się na „miejscu zbrodni", należy wziąć pod uwagę prawdopodobieństwo, że urządzenie zawiera informacje związane z dochodzeniem. Nie jest już możliwe udanie się na miejsce i przejęcie każdego pojedynczego przedmiotu cyfrowego, budżet i ograniczenia czasowe na to nie pozwalają. Aby ustalić, czy urządzenie nadaje się do zajęcia, należy wziąć pod uwagę rodzaj dochodzenia, właściciela urządzenia oraz wszelkie dostępne informacje wywiadowcze i podstawowe. Decyzję taką należy podjąć w powiązaniu z głównym badaczem oraz ograniczeniami prawnymi i proceduralnymi. Jeśli urządzenie wymaga zatrzymania, należy najpierw ustalić, czy jest ono włączone, czy wyłączone. Jeśli opcja jest włączona, należy rozważyć przechwytywanie danych w czasie rzeczywistym i rejestrowanie wszystkich widocznych uruchomionych programów i procesów. Po podjęciu decyzji i przechwyceniu wszelkich bieżących danych należy odłączyć zasilanie od urządzenia. Jeśli urządzeniem jest serwer lub podobne urządzenie, na którym działają krytyczne systemy i bazy danych, należy zastosować się do prawidłowej procedury zamykania. Możliwe jest, że pozbawiona skrupułów osoba „przygotowała" system do uruchamiania określonych programów lub skryptów po jego zamknięciu, na przykład wymazując dane lub modyfikując pewne informacje; należy jednak w pełni rozważyć ryzyko utraty kluczowych informacji biznesowych w wyniku uszkodzenia bazy danych lub systemu. Ogólnie rzecz biorąc, w normalnym domowym laptopie lub komputerze można po prostu odłączyć zasilanie. Po wyłączeniu lub jeśli jest już wyłączone, urządzenie należy umieścić w torbie na dowody z plombą zabezpieczającą przed manipulacją i zachować łańcuch dostaw. Każdemu urządzeniu należy nadać niepowtarzalny numer referencyjny ułatwiający identyfikację, który powinien być unikalny dla każdego zaawansowanego technologicznie badania. Gdy miejsce zbrodni jest fizycznie zabezpieczone, należy zwrócić uwagę na urządzenia, które mają zostać przejęte, oraz na to, jak technicznie można to osiągnąć – szczegółowo opisano to w poniższych sekcjach.

PRZECHWYTYWANIE DANYCH NA ŻYWO I ONLINE

Przechwytywanie danych w czasie rzeczywistym jest wykorzystywane, gdy urządzenie nie jest przełączone w tryb offline, to znaczy nie zdecydowano się go wyłączać. Na przykład, jeśli krytyczny

serwer biznesowy zostanie wyłączony, może to spowodować zakłócenia lub utratę przychodów firmy. Jeśli program jest uruchomiony, może to oznaczać utratę krytycznych danych lub nie będzie możliwe ich odzyskanie po odłączeniu zasilania. Może się tak zdarzyć również w przypadku szyfrowania: po wyłączeniu zasilania dane nie są już w formacie, do którego można uzyskać dostęp bez prawidłowego hasła. Zaawansowane technologicznie dochodzenie powinno umożliwić komuś wykonanie wykonanych czynności i uzyskanie dokładnie takich samych wyników. Problem z danymi bieżącymi polega jednak na tym, że podlegają one ciągłym zmianom i dlatego nigdy nie można ich w pełni odtworzyć. Chociaż te problemy istnieją, obecnie przyjętą praktyką jest przeprowadzanie dobrze określonej i udokumentowanej analizy na żywo w ramach dochodzenia, a przechwycone dane można chronić przed dalszą zmiennością poprzez generowanie skrótów dowodów w momencie ich gromadzenia . Tradycyjnie, podczas poszukiwania dowodów związanych z dostępem do strony internetowej, dane byłyby przechwytywane z komputera lokalnego w postaci tymczasowych plików internetowych. Ponieważ jednak zaawansowane technologie kodowania internetowego pozostawiają mniej rozproszonych pozostałości na komputerze lokalnym, należy obecnie zastosować techniki umożliwiające zalogowanie się na rzeczywistą stronę internetową i pobranie zawartości widocznej dla użytkownika. Alternatywnie można zwrócić się do usługodawcy z prośbą o przedstawienie informacji. Proces ten wymaga szczegółowego zapisywania wykonanych czynności i hasha pliku na zakończenie. Przykładem przechwytywania danych w Internecie jest przechwytywanie dowodów z sieci społecznościowych, które obecnie staje się coraz bardziej widoczne w dochodzeniach z zakresu zaawansowanych technologii, w tym w dochodzeniach związanych z cyberprzemocą. W przypadku aktualnych danych, nawet po zabezpieczeniu fizycznego miejsca przestępstwa, nadal istnieje możliwość wywarcia wpływu zewnętrznego na dane cyfrowe, na przykład poprzez zdalny dostęp. Dlatego bardzo ważne jest, aby informacje te zostały jak najszybciej przechwycone cyfrowo. Jeśli to możliwe, należy sprawdzić dane na urządzeniu i po upewnieniu się, że dane nie zostaną utracone, urządzenie należy odizolować od komunikacji sieciowej, sygnałów komórkowych lub wszelkich innych form komunikacji, które mogłyby umożliwić usunięcie danych lub zdalny dostęp do nich. W dużych organizacjach należy zwrócić się o pomoc do administratorów systemów, aby pomóc w identyfikacji i izolacji urządzeń cyfrowych, aby zapobiec niepożądanemu uszkodzeniu ważnych danych. Następnie urządzenia można usunąć lub przechwycić dane przy użyciu odpowiednich narzędzi.

PRZECHWYTYWANIE DANYCH W TRYBIER OFFLINE (martwym).

Jest to tradycyjna metoda przechwytywania danych polegająca na usunięciu głównej jednostki pamięci, zazwyczaj dysku twardego: z danych znajdujących się na urządzeniu tworzona jest dokładna replika, która jest później analizowana. Podstawową zasadą kryminalistyki jest to, że oryginalne dane, które mogą zostać wykorzystane jako dowód, nie są modyfikowane. Dlatego podczas przetwarzania dowodów fizycznych konieczne jest użycie blokady zapisu; moduł blokujący zapis przechwytuje i zatrzymuje wszelkie żądania zapisu w dowodzie. Urządzenie to znajduje się w jednej linii z urządzeniem i maszyną analityczną. Dostępnych jest wiele programów blokujących zapis, które mogą chronić różnego rodzaju urządzenia fizyczne przed modyfikacjami przez badacza. Istnieją fizyczne blokery zapisu, które są fizycznie połączone z cyfrowym dowodem i maszyną analityczną. Istnieją również programowe blokery zapisu, które zakłócają działanie sterownika w systemie operacyjnym.

WERYFIKACJA DANYCH

Pierwszym krokiem badacza zaawansowanego technologicznie po przechwyceniu danych jest potwierdzenie, że dane nie zostały zmienione. Aby to ułatwić, wartość skrótu przechwytywanych danych jest ponownie obliczana; jest to następnie porównywane z oryginalnym skrótem. Jeżeli nie są one zgodne, nie podejmuje się dalszych kroków do czasu skontaktowania się ze starszym oficerem dochodzeniowym lub kierownikiem i omówienia sytuacji. Taki błąd może podważyć nawet najbardziej

konkretny dowód znaleziony na eksponacie. Niedopasowania skrótu mogą wystąpić, jeśli dane nie zostały poprawnie skopiowane lub mogła wystąpić usterka oryginalnego urządzenia. Być może trzeba będzie ponownie odwiedzić oryginalną wystawę i stworzyć nowy wizerunek. Może to nie być możliwe, jeśli dane zostały przechwycone w trybie online lub na żywo, ponieważ dane mogą nie być już dostępne. Po przechwyceniu do urządzenia mogą zostać dodane nowe dane, a wszelkie stare dane mogą zostać nadpisane, co oznacza, że urządzenie już nigdy nie będzie w tym samym stanie.

PRZEGLĄDANIE WYMAGAŃ

Wymogi dochodzenia lub zakresu dochodzenia dostarczają konkretnych pytań, na które należy odpowiedzieć. Można to wykorzystać do zidentyfikowania możliwych tras analizy. Ważne jest, aby na wczesnym etapie dochodzenia przeprowadzić dokładną analizę wymagań, aby mieć pewność, że czas i pieniądze nie zostaną zmarnowane. Z zakresu kompetencji, obok wszelkich dostarczonych informacji ogólnych, należy określić co najmniej następujące elementy:

1. Liczba i rodzaj eksponatów: wiadomo, jakie dane należy zbadać

2. Zaangażowane osoby/przedsiębiorstwa: wiadomo, kto ma być objęty dochodzeniem

3. Data i godzina: wiadomo, kiedy doszło do zdarzenia, co zapewni okno czasowe do zbadania

4. Słowa kluczowe: co może być interesujące w trakcie dochodzenia, jeśli zostanie odkryte, mogą to być na przykład nazwiska lub numery rachunków bankowych

5. Dostarczone dane: jeśli ma być poszukiwany konkretny plik lub dokument dotyczący danych – przydatne jest udostępnienie jego kopii

ROZPOCZĘCIE ANALIZY

Z przechwyconego materiału dowodowego można uzyskać wiele informacji, a niektóre z nich mogą nie być istotne. Żaden proces ani metoda nie odpowie na wszystkie postawione pytania. Podczas przeglądania informacji należy pamiętać o następujących kwestiach, aby upewnić się, że nic nie zostało pominięte lub źle zinterpretowane:

1. Fałszywie pozytywne: pliki, które nie mają związku z dochodzeniem, ale mogą zawierać ważne słowo kluczowe

2. Pozytywne: akta/dane istotne dla dochodzenia

3. Fałszywe negatywy: pliki, które nie zostały pobrane, ale są istotne – mogą być w nieczytelnym formacie (na przykład skompresowane lub zaszyfrowane)

Rzeczywista analiza danych będzie się różnić w zależności od rodzaju dochodzenia, które należy przeprowadzić. Dlatego też na początku dochodzenia należy dokonać rozważenia i dokładnej analizy faktycznych pytań, które są zadawane. Analizę danych można podzielić na dwa etapy:

1. Analiza wstępna: jeśli zostanie wykonana nieprawidłowo, może mieć poważny wpływ na resztę dochodzenia. Jest to proces przygotowywania danych tak, aby rzeczywista analiza była jak najbardziej płynna. Proces ten polega na przygotowaniu danych poprzez odzyskanie usuniętych plików i partycji oraz zamontowaniu skompresowanych plików i folderów oraz zaszyfrowanych plików (aby można było je następnie przeszukiwać i mieć kontekst).

2. Analiza: jest to przegląd danych w celu znalezienia informacji, które pomogą w dochodzeniu poprzez identyfikację dowodów potwierdzających lub obalających daną tezę.

Dochodzenie oparte na zaawansowanych technologiach nie powinno zależeć od użytego narzędzia; narzędzie jest po prostu środkiem do celu. Ważne jest jednak, aby badacz czuł się komfortowo oraz posiadał wystarczające kwalifikacje i doświadczenie w korzystaniu z wybranego narzędzia analizy cyfrowej. Możliwość kliknięcia przycisku w narzędziu kryminalistycznym lub wykonania wcześniej zdefiniowanego procesu nie jest kryminalistyką — jest to odzyskiwanie danych dowodowych. Zaawansowany technologicznie badacz musi być w stanie dokonać przeglądu tego, co go czeka i zinterpretować te informacje, aby sformułować wnioski i, jeśli to konieczne, opinię. Lokalizacja dowodu może być równie ważna jak sam dowód; dlatego należy dokładnie rozważyć kontekst tego, co widać. Jeśli plik znajduje się w folderze dokumentów osobistych użytkownika, nie oznacza to, że go tam umieścił. Rolą badacza jest określenie jego pochodzenia i przedstawienie kontekstu dotyczącego tego, jak się tam dostał, kiedy i czy został otwarty. Interpretacja i przedstawienie takich informacji może pomóc w udowodnieniu lub obaleniu kierunku dochodzenia. Nie ma prawidłowego sposobu rozpoczęcia właściwej analizy danych; nie ma żadnego zbioru zasad, który określałby dokładnie, co należy robić i na co zwracać uwagę. W zależności od ograniczeń prawnych badacz może ograniczyć się jedynie do przeglądania określonych plików i danych. Jeśli istnieje jakakolwiek niepewność w tej kwestii, badacz musi omówić to ze swoim przełożonym lub starszym badaczem. Jeśli dostęp do wszystkich danych jest możliwy, badacz może przeglądać foldery i pliki. Jeśli coś wyróżnia się jako „niezwykłe" lub interesujące, może wyznaczyć kierunek i skupić się na etapach analizy technicznej. W pewnym stopniu może to zależeć od sprawdzanego systemu operacyjnego. Na początku dochodzenia należy sprawdzić, czy uwzględniono wszystkie oczekiwane dane dotyczące przechwytywania. Bardzo łatwo jest zmodyfikować partycje na dysku tak, aby nie były od razu widoczne lub usunąć partycję i utworzyć nową. W przypadku dysku fizycznego może to obejmować sprawdzenie liczby sektorów dostępnych na dysku w porównaniu z aktualnie używanymi.

ANALIZA PODPISÓW

Łatwo jest zaciemnić prawdziwe znaczenie plików i przydatne jest określenie, czy wszystkie pliki są tym, za co się podają; może to być prosty sposób na wyróżnienie ważnych plików. Systemy operacyjne wykorzystują proces wiązania aplikacji w celu połączenia typu pliku z aplikacją. Na przykład system Windows używa rozszerzeń plików i prowadzi ich rejestr , aplikacja powinna otworzyć jaki plik: na przykład pliki .doc są otwierane w programie Microsoft Word. Fakt, że system Windows korzysta z rozszerzeń plików, powoduje powstanie techniki ukrywania danych, dzięki której użytkownik może zmienić rozszerzenie pliku, aby ukryć jego zawartość. Jeśli plik o nazwie MyContraband.jpg zostałby zmieniony na lansys.dll i przeniesiony do folderu systemowego, przypadkowy obserwator prawdopodobnie nigdy by go nie znalazł. Linux używa nagłówka (lub podpisu) pliku, aby określić, która aplikacja powinna otworzyć plik (aby to zobaczyć, plik można przeglądać w formacie szesnastkowym). Dlatego trudniej jest ukryć zawartość/prawdziwy typ pliku, ponieważ z uszkodzonym nagłówkiem plik często się nie otwiera. Linux (i Mac) mają wbudowane polecenie Terminal, które pozwala zidentyfikować podpis pliku za pomocą prostego polecenia plik –i [gdzie –i oznacza plik wejściowy]. Większość narzędzi kryminalistycznych ma możliwość sprawdzenia podpisu pliku i raportowania, czy różni się on od oczekiwanego po rozszerzeniu. Podpis pliku można sprawdzić w oparciu o prekompilowaną bazę danych. Jeśli podpis istnieje, sprawdzi powiązane z nim rozszerzenie. Następnie dla każdego pliku zostanie uzyskany jeden z następujących wyników (niektóre narzędzia kryminalistyczne mogą dawać bardziej szczegółowe wyniki, ale wszystkie są zgodne z tymi samymi dwoma koncepcjami):

• Dopasuj — podpis i rozszerzenie pasują do tego, co jest zapisane

• Niezgodność – podpis i rozszerzenie nie są zgodne, dlatego należy sprawdzić plik w celu znalezienia dowodów manipulacji

FILTROWANIE DOWODÓW

Powszechnie wiadomo, że wartość skrótu jest ważnym narzędziem w każdym dochodzeniu w dziedzinie zaawansowanych technologii. Wartości skrótu są nieodłącznym elementem dochodzenia kryminalistycznego; początkowo służą one weryfikacji i potwierdzeniu integralności otrzymanego materiału dowodowego. Można je następnie wykorzystać do potwierdzenia integralności wszelkich przedstawionych dowodów. Badacz może również użyć wartości skrótu, aby zmniejszyć ilość sprawdzanych danych, korzystając z tak zwanych zestawów skrótów, które stanowią po prostu grupę znanych wartości skrótu. Badacz może dysponować ogromnym zestawem skrótów, co może znacznie ograniczyć liczbę plików do przeglądu; usunięcie tego, co jest „znanym dobrem", może znacznie ograniczyć liczbę elementów wymagających zbadania, przyspieszając w ten sposób całe dochodzenie. Możliwe jest również tworzenie niestandardowych zestawów skrótów godnych uwagi plików, które można uruchomić przeciwko sprawie, aby szybko zidentyfikować, co jest obecne. Jeśli na początku dochodzenia zostanie dostarczony plik lub dane, na przykład interesujący obraz, można utworzyć skrót obrazu, a następnie wyszukiwać go na całej wystawie – wyłącznie na podstawie wartości skrótu. Jest to szybki sposób na identyfikację ważnych plików, który pozwoli śledczemu skoncentrować się na danych zawierających informacje zdecydowanie związane ze śledztwem.

WYSZUKIWANIE SŁÓW KLUCZOWYCH

Wyszukiwanie słów kluczowych umożliwia szybką identyfikację godnych uwagi terminów i informacji, zwykle uzyskiwanych z zakresu kompetencji lub informacji ogólnych. Umiejętność zidentyfikowania słów kluczowych istotnych dla dochodzenia jest niezwykle ważną umiejętnością. Nieprawidłowy wybór słowa kluczowego może zająć kilka dni i kilka miesięcy na sprawdzenie. Generalnie istnieją dwa sposoby wyszukiwania:

1. Wyszukiwanie indeksowe: stosowane narzędzie może indeksować wszystkie dane, zasadniczo rejestrując każde obecne słowo, aby można je było przeszukiwać. Ten typ wyszukiwania jest wszechstronny, ponieważ generalnie nie uwzględnia stosowanej kompresji, np. w plikach PDF lub ZIP, gdzie wyszukiwanie w czasie rzeczywistym nie byłoby w stanie zidentyfikować wszystkich odpowiednich słów kluczowych. Chociaż konfiguracja tego wyszukiwania jest zazwyczaj bardzo powolna, po zakończeniu wszystkie wyniki są niemal natychmiastowe (system Windows wykonuje podobną akcję na komputerze lokalnym).

2. Wyszukiwanie w czasie rzeczywistym: słowo kluczowe można utworzyć i uruchomić w dowolnym momencie dochodzenia — zakończenie wyszukiwania może zająć trochę czasu. Zazwyczaj wyszukiwanie w czasie rzeczywistym nie umożliwia wyszukiwania plików skompresowanych lub w nietypowych formatach, chyba że zostaną one najpierw zdekompresowane.

Do dokładniejszego wyszukiwania słów kluczowych można używać wyrażeń regularnych (regexp). Regexp to sposób definiowania wzorca wyszukiwania wykorzystujący symbole wieloznaczne i znaki specjalne, aby zapewnić większą elastyczność i możliwości niż proste wyszukiwanie słów kluczowych. Jeżeli jako numer seryjny urządzenia podano 1234-1234, ale nie było wiadomo, czy zawierał on łącznik; czy można go zastąpić innym znakiem specjalnym; lub jeśli w ogóle istniał, konieczne byłoby utworzenie wielu wyszukiwanych haseł. Zamiast próbować wpisywać wszystkie możliwe wyszukiwane hasła, można utworzyć proste wyszukiwanie wyrażeń regularnych, które obejmowałoby to: na przykład 1234[.]?1234. Wyrażenie stwierdza, że znaki w nawiasach można znaleźć zero lub jeden raz (jest to oznaczone ?). W nawiasie znajduje się . (kropka) jest to znak wyrażenia regularnego, który oznacza, że pomiędzy tymi dwiema liczbami może znajdować się wszystko. Dobrą praktyką jest przetestowanie

wyrażenia regularnego przed uruchomieniem go w danej sprawie, ponieważ jest to ciąg bardziej złożony niż proste wyszukiwanie słów kluczowych, a jego ukończenie może zająć więcej czasu.

GŁÓWNE DOWODY

Niemożliwe jest opisanie w jednym rozdziale podstawowych dowodów dostępnych na temat różnych systemów operacyjnych i systemów plików; jednakże istnieje kilka podstawowych obszarów dowodowych, które zwykle mają zastosowanie w dochodzeniach wymagających zaawansowanych technologii:

• Zapas plików: sposób przechowywania plików na urządzeniu oznacza, że znaczna ilość miejsca na dysku jest niewykorzystana, ale jest przydzielona do pliku. Nazywa się to luzem pliku i oznacza po prostu odstęp między końcem pliku a miejscem, które zostało mu przydzielone na urządzeniu. W tej wolnej przestrzeni mogą znajdować się informacje ze starych plików, które mogą stanowić fragmenty ważnych danych związanych ze śledztwem. Użytkownik może również ukryć informacje w tym miejscu, aby nie było ich łatwo odzyskać.

• Pliki tymczasowe: wiele aplikacji wykorzystuje pliki tymczasowe podczas wykonywania funkcji, na przykład gdy użytkownik pracuje nad dokumentem lub drukuje plik. Pliki te są zwykle usuwane po zakończeniu zadania. Jeśli jednak nastąpi nieprawidłowe wyłączenie urządzenia lub utrata zasilania, możliwe jest przywrócenie i zidentyfikowanie działań użytkownika.

• Usunięte pliki: sposób usuwania danych cyfrowych oznacza, że w wielu przypadkach możliwe jest ich odzyskanie. W większości przypadków usuwania jedyne, co zostaje zrobione, to usunięcie wskaźnika do pliku, rzeczywiste dane nadal znajdują się na wystawie i można je odzyskać w stosunkowo łatwy sposób.

Ponieważ Windows jest nadal najpopularniejszym systemem operacyjnym, w poniższych sekcjach opisano pokrótce niektóre podstawowe artefakty, które mogą być przydatne podczas dochodzenia, w tym znaczenie tych informacji (zobacz także Rozdział 7).

PLIKI LNK WINDOWS

System Windows używa skrótów, aby udostępniać łącza do plików w innych lokalizacjach. Może to dotyczyć aplikacji na komputerze stacjonarnym lub dokumentu w sklepie sieciowym. Pliki te nazywane są LNK (lub linkiem), ponieważ mają rozszerzenie .lnk. Szczególnie interesujące dla badacza zaawansowanych technologii są pliki LNK znalezione w folderze „Ostatnie” użytkownika. Pliki te powstają, gdy użytkownik otwiera dokument i stanowią odniesienie do oryginalnego dokumentu. Pliki LNK są trwałe, co oznacza, że istnieją nawet po usunięciu pliku docelowego lub przestają być dostępne. Folder „Ostatnie” i pliki LNK to jedne z pierwszych miejsc, które badacz sprawdza, szukając aktywności użytkownika w systemie Windows. Będą one dostarczać informacji związanych z aktywnością użytkownika; czy używane są jakieś dyski zewnętrzne/zdalne; i czy można znaleźć jakieś godne uwagi nazwy plików. Pliki LNK obejmują:

• Pełna ścieżka do oryginalnego pliku

• Numer seryjny woluminu: jest to unikalne odniesienie do partycji (lub woluminu)

• Rozmiar pliku, na który wskazuje LNK

• Znaczniki czasu MAC pliku, na który wskazuje LNK

WSTĘPNE POBIERANIE PLIKÓW W SYSTEMIE WINDOWS

Pliki Windows Prefetch mają na celu przyspieszenie procesu uruchamiania aplikacji i zawierają nazwę aplikacji; ile razy został uruchomiony; oraz znacznik czasu wskazujący czas ostatniego uruchomienia. Może to dać solidną wskazówkę co do aplikacji uruchomionych przez użytkownika, a nawet uruchomionego złośliwego oprogramowania. Można je znaleźć w folderze %SystemRoot%\Prefetch

Dzienniki zdarzeń systemu Windows

System Windows prowadzi rejestr wszystkich działań aplikacji i systemu w dziennikach zdarzeń. Są to wpisy tworzone automatycznie przez system operacyjny i mogące dostarczyć istotnych informacji o chronologicznych działaniach wykonywanych przez użytkowników i system. Obejmuje to logowanie i wylogowywanie użytkowników; dostęp do plików; tworzenie konta; usługi które działają; i instalacja sterowników. Są one zwykle używane do rozwiązywania problemów na komputerze: można je znaleźć w %SystemRoot%\Windows\system32\config.

REJESTR WINDOWS

Rejestr systemu Windows to baza danych przechowująca ustawienia komputera, określająca wszystkich użytkowników; Aplikacje; i sprzęt zainstalowany w systemie; oraz wszelkie powiązane ustawienia, umożliwiające prawidłową konfigurację systemu podczas uruchamiania. Rejestr jest przechowywany w formacie wymagającym odczytania; istnieje wiele narzędzi, które mogą to zrobić. Po otwarciu zapewnia bogactwo informacji, w tym między innymi dowody dotyczące aplikacji i plików otwartych przez użytkownika; jakie urządzenia zostały podłączone; oraz używane adresy IP.

PRZYWRÓĆ PUNKTY

Microsoft Windows udostępnia usługę zwaną punktami przywracania. Wersja systemu Windows określa, co one faktycznie zawierają. Prostym celem punktów przywracania jest utworzenie migawki komputera we wcześniej określonej dacie i godzinie lub w momencie wystąpienia zdarzenia (takiego jak instalacja oprogramowania), aby użytkownik mógł go przywrócić w przypadku wystąpienia błędu. Punkty przywracania zawierają migawki rejestru systemu Windows; pliki systemowe; LNK, a w nowszych wersjach systemu Windows mogą również zawierać przyrostowe kopie zapasowe plików użytkownika. Może to stanowić nieocenione źródło informacji na potrzeby dochodzenia, ponieważ dostarcza informacji historycznych, takich jak aplikacje, które nie są już zainstalowane. W systemie Windows XP domyślny okres przechowywania punktów przywracania wynosi 90 dni, podczas gdy nowsze wersje są ograniczone jedynie ilością dostępnego miejsca na dysku.

STUDIUM PRZYPADKU

W następstwie doniesień o nielegalnej sprzedaży klientom dokumentacji opartej na przepisach prawnych, kancelaria prawnicza zażądała przeprowadzenia dochodzenia w zakresie zaawansowanych technologii. Poczyniono ustalenia dotyczące wizyty na terenie organizacji objętej dochodzeniem, postępowanie sądowe oznaczało, że organizacja nie miała pojęcia, że tak się stanie – co zapobiegło złośliwemu niszczeniu danych. Wprowadzono zapis prawny, mający na celu ograniczenie utraty przychodów przedsiębiorstwa, co oznaczało, że urządzenia cyfrowe nie mogły być usuwane z lokalu. Dane wywiadowcze przeprowadzone przed przeszukaniem wykazały, że w obiekcie jednocześnie pracowało do 20 pracowników oraz jaki był dostęp do budynku; łącznie z drogami dojazdowymi pojazdów. Nie były dostępne żadne informacje ani czas, aby określić, jakie urządzenia cyfrowe mogą być obecne. Następnego dnia do lokalu przybył zarówno zespół prawniczy, jak i zespół śledczych zajmujący się zaawansowanymi technologiami. Miejsce zdarzenia zostało początkowo zabezpieczone poprzez usunięcie wszystkich osób z pobliża wszystkich urządzeń cyfrowych. Dokonano pełnego

nagrania miejsca zdarzenia przy użyciu kamer cyfrowych i szkiców, a następnie zidentyfikowano każde urządzenie cyfrowe. Dokonano przeglądu potencjalnych źródeł cyfrowych w celu określenia ich aktualnego stanu: przeważnie były to komputery lub laptopy, które nie były uruchomione i dlatego zostały odłączone od zasilania. Zidentyfikowano serwer, który jest obecnie uruchomiony, dokonano przechwycenia pamięci, aby upewnić się, że uruchomione procesy i połączenia zostały zarejestrowane, a następnie serwer został zamknięty. Przeprowadzono analizę kryminalistyczną wszystkich urządzeń na miejscu, co samo w sobie zajęło ponad 12 godzin. Złapy te następnie umieszczono w torebkach zabezpieczonych przed manipulacją, zwrócono do laboratorium i poddano analizie. Tło dochodzenia dostarczyło odpowiednich słów kluczowych i typów plików. Wykorzystano je do analizy danych, która następnie pozwoliła zidentyfikować szereg plików, e-maili i dokumentów istotnych dla dochodzenia, co umożliwiło zespołowi prawnemu dalsze postępy w postępowaniu sądowym.

STRESZCZENIE

Omówiono techniczną stronę dochodzeń w zakresie zaawansowanych technologii oraz sposób ich prowadzenia. Uwzględniono kluczowe koncepcje związane z badaniem danych cyfrowych oraz narzędzia; procesy; oraz techniki związane z procesem, od zebrania materiału dowodowego do jego analizy. Znajomość tych pojęć jest ważna dla każdego badacza, aby można było wdrożyć właściwe procedury i procesy, a także zrozumieć decyzje podejmowane przez innych. Należy pamiętać, że nie ma dwóch takich samych dochodzeń; istnieje po prostu zbyt duże zróżnicowanie rodzajów przechowywania danych i możliwości urządzeń, aby kiedykolwiek miało to miejsce. Dochodzenie prawie zawsze będzie sprowadzać się do badacza i jego zdolności do interpretacji i zrozumienia tego, co widzi. Ważne jest, aby nawet osoby, które nie są zaangażowane w dochodzenie w sprawie zaawansowanych technologii, były świadome zachodzących w nim procesów, ponieważ ma to tak znaczący wpływ na każde dochodzenie w sprawie cyberprzestępczości i cyberterroryzmu. Taka wiedza może pomóc w identyfikacji wcześniej nieprzewidzianych urządzeń cyfrowych lub obszarów badań.

Przechwytywanie, obrazowanie i analizowanie dowodów cyfrowych: wytyczne krok po kroku

WSTĘP

Istnieje wiele podejść, które można zastosować podczas tworzenia, a następnie wykonywania planu dochodzenia kryminalistycznego. Te, które są wybierane lub tworzone, są dokonywane w dużej mierze subiektywnie. Istnieją jednak pewne kryteria, których należy przestrzegać zarówno w zakresie stosowania najlepszych praktyk, przestrzegania przepisów ustawowych i wykonawczych, jak i zapewnienia, że wszelkie odkryte dowody pozostaną dopuszczalne w sądzie. Celem tego rozdziału jest przedstawienie wskazówek, jak osiągnąć te cele, a także omówienie niektórych z bardziej wnikliwych metod stosowanych podczas poszukiwania obciążających dowodów. Ponadto ma na celu zapewnienie egzaminatorowi ogólnego obrazu procesów. Od tego, co należy wziąć pod uwagę przy ubieganiu się o nakaz przeszukania, po właściwe zabezpieczenie i zdobycie dowodów. Na koniec omówiono sposób stosowania nowatorskich metod w celu odkrycia kluczowych dowodów za pomocą analizy kryminalistycznej, w tym dowodów, które mogły zostać zaciemnione za pomocą technik antykryminalistycznych.

USTALANIE PRZESTĘPSTWA

Dowody kryminalistyczne są zwykle gromadzone poprzez przeszukanie pomieszczeń podejrzanego i zajęcie odpowiedniego sprzętu. Aby zrobić to zgodnie z prawem, zazwyczaj konieczne jest uzyskanie nakazu przeszukania. Szczegóły tego procesu różnią się w zależności od prawa obowiązującego w kraju i jurysdykcji, w której miało miejsce zarzucane przestępstwo; jednak w większości przypadków nakazy są wydawane przez sędziego, który jest przekonany, że istnieją wystarczające dowody uzasadniające

jego wydanie. Na przykład w Wielkiej Brytanii sędzia musi upewnić się, że istnieją „uzasadnione podstawy", aby sądzić, że doszło do przestępstwa (Crown, 1984). Zwykle przestępstwo to byłoby wymienione w ustawie o niewłaściwym użytkowaniu komputera. W Stanach Zjednoczonych proces jest podobny – w czwartej poprawce dodano termin „prawdopodobna przyczyna" (FindLaw, 2014). Pełne zbadanie, co oznaczają zarówno „uzasadnione podstawy", jak i „prawdopodobną przyczynę", wykracza poza zakres tej pracy, ale w obu przypadkach jasne jest, że potrzebne są istotne dowody oraz że wniosek o przeszukanie lokalu nie opiera się na po prostu podejrzenie lub przeczucie. Ponadto dowody muszą potwierdzać założenie, że przestępstwo zostało, jest lub zostanie popełnione lub zaaranżowane w lokalu.

ZBIERANIE DOWODÓW DO NAKAZU PRZEGLĄDANIA

Dowody popełnienia cyberprzestępstwa można gromadzić na różne sposoby, w zależności od popełnienia przestępstwa, przy czym przestępstwa zazwyczaj należą do jednej z następujących czterech szerokich kategorii:

• Piractwo: powielanie i rozpowszechnianie materiałów chronionych prawem autorskim.

• Złośliwe hakowanie: Akt uzyskania nielegalnego, nieautoryzowanego dostępu do systemu komputerowego. Obejmuje to phishing i kradzież tożsamości.

• Pornografia dziecięca: dystrybucja, posiadanie lub oglądanie pornografii dziecięcej.

• Finansowe: Celowe zakłócanie zdolności firmy do prowadzenia handlu elektronicznego.

Niezależnie od rodzaju popełnionego cyberprzestępstwa konieczne jest powiązanie podejrzanego z przestępstwem. W poniższych sekcjach omówiono techniki, narzędzia i metody umożliwiające wykonanie tego.

ZGŁOSZONE PRZEZ OSOBY TRZECIE

Strony podejrzane przez obywatela o popełnienie cyberprzestępczości można zgłosić organom ścigania. Czyn przestępczy może zostać wykryty w wyniku audytu miejsca pracy lub programu monitorowania bezpieczeństwa. Alternatywnie może tego dokonać osoba, która dowiedziała się o działalności przestępczej w kontekście społecznym, w Internecie za pośrednictwem mediów społecznościowych lub osobiście.

IDENTYFIKACJA ADRESU PROTOKOŁU INTERNETOWEGO PODEJRZANEGO

Publiczny adres protokołu internetowego (IP) jednoznacznie identyfikuje każde urządzenie bezpośrednio podłączone do Internetu. Adresowanie IP wykorzystuje 32-bitowy (IPv4) lub 128-bitowy (IPv6) hierarchiczny schemat adresowania. Adres IP jest używany przez routery pośredniczące do podjęcia decyzji, jaką ścieżką pakiety danych powinny podążać od źródła do miejsca docelowego. Gdy adres IP jest używany do potencjalnej identyfikacji podejrzanego, zwykle jest on przydzielany podejrzanemu przez dostawcę usług internetowych (ISP) do jego routera obwodowego. W przypadku użytkownika domowego urządzenie to zazwyczaj znajduje się w jego siedzibie. Ich adres IP pozostaje zamknięty w pakietach danych tworzących sesję komunikacyjną i jednoznacznie identyfikuje publiczny interfejs tego routera. Identyfikacja adresu IP w złośliwej komunikacji stanowi wystarczający dowód do wydania nakazu przeszukania i aresztowania. Jednakże istnieją pewne problemy związane z tą metodą identyfikacji, z których najbardziej zauważalne jest wykorzystanie usług fałszowania adresów IP i anonimizacji usług przekazywania proxy. Omówiono je poniżej.

PODSZYWANIE POD IP

Podszywanie się pod adresy IP to proces, podczas którego złośliwy haker ręcznie tworzy pakiety danych z fałszywym źródłowym adresem IP. To nie tylko ukrywa ich prawdziwy adres IP, ale także pozwala im podszywać się pod inny system. Ograniczeniem jest to, że nie można go użyć w ataku polegającym na komunikacji zwrotnej od ofiary do atakującego, na przykład w celu przejęcia kontroli nad maszyną ofiary lub wyświetlenia danych z niej. W rezultacie jest to popularna metoda ataku polegająca na atakach typu „odmowa usługi", które powodują, że system nie działa, albo przytłaczając system dużą liczbą pakietów, albo specjalnie tworząc pakiet, który powoduje zakończenie usługi.

ANONIMOWE USŁUGI PRZEKAZANIA PROXY

Anonimowe usługi przekazywania proxy, takie jak Tor (2014), zapewniają prywatność i anonimowość pochodzenia. Osiąga się to poprzez zastosowanie odpowiednio algorytmu szyfrowania i przekazywania. Algorytm Tora wybiera losową ścieżkę od źródła do miejsca docelowego przez określone węzły sieci, które zostały wybrane przez społeczność wspierającą jako część usługi przekaźnikowej. Połączenia pomiędzy tymi węzłami są szyfrowane w taki sposób, że każdy węzeł posiada jedynie adres IP węzłów, z którymi jest bezpośrednio połączony. Chociaż komunikacja między węzłem wyjściowym a ostatecznym miejscem docelowym nie jest szyfrowana, pierwotny źródłowy adres IP jest nadal chroniony wieloma warstwami szyfrowania, po jednej dla każdego węzła. Ostateczny adresat będzie znał jedynie adres IP węzła wyjściowego lub końcowego używanego przez usługę, a nie hosta, z którego pochodzi wiadomość. Oznacza to, że sprawdzane są logi serwera, który został zaatakowany; nie ujawnią szczegółów atakującego używającego Tora, ale raczej węzeł wyjściowy przekaźnika Tora. Chociaż usługi przekazywania proxy, takie jak Tor, oferują złośliwym hakerom ochronę przed inwigilacją i anonimowość pochodzenia, mają one również pewne wady. Po pierwsze, są wolniejsze niż tradycyjne korzystanie z Internetu; wynika to z przebytych dodatkowych węzłów (trzy w przypadku Tora). Węzły te mogą znajdować się w różnych krajach i mogą być niskiej jakości, w związku z czym zarówno trasa, jak i przepustowość stają się nieoptymalne. Po drugie, mogą być trudne w konfiguracji, jest to szczególnie prawdziwe, jeśli nie jest wymagana łączność za pośrednictwem przeglądarki internetowej, jak ma to miejsce w przypadku Internet Relay Chat (IRC), który choć staje się mniej popularny wśród ogółu społeczeństwa, w dalszym ciągu pozostaje kanałem komunikacji dla złośliwych hakerów. Wreszcie polegają na tym, że szkodliwa strona pamięta o uruchomieniu usługi przed każdą złośliwą operacją, a wystarczy tylko raz zapomnieć, aby ich tożsamość została naruszona. Powszechnie uważa się, że była to główna metoda identyfikacji Hectora Xaviera Monsegura, znanego również jako Sabu, ze stowarzyszenia hakerskiego LulzSec w 2011 roku. Rzekomo tylko raz zalogował się na kanał IRC, nie korzystając z usługi anonimizującej. Z doniesień wynika, że FBI zażądało następnie danych od dostawcy usług internetowych odpowiedzialnego za ten adres IP, który ujawnił swój adres domowy.

SYSTEMY WYKRYWANIA WŁAMANIA, RUCH W SIECI I DZIENNIKI FIREWALLU

Systemy wykrywania włamań (IDS) służą do monitorowania ruchu sieciowego i wykrywania złośliwej aktywności. Zwykle osiąga się to poprzez dopasowanie zawartości ruchu sieciowego do znanej już szkodliwej aktywności (sygnatury). W przypadku wykrycia dopasowania generowany jest alert. Powszechnym zjawiskiem jest przechwytywanie ruchu sieciowego równolegle z wykrywaniem włamań do sieci; umożliwia to późniejsze zbadanie ruchu, który spowodował alert, w celu poznania większej liczby szczegółów ataku, w tym adresów IP. Zapora sieciowa i dzienniki systemowe również przechwytują adresy IP i mogą przechowywać informacje dotyczące złośliwej aktywności. W związku z tym informacje dostarczane przez te systemy mogą stanowić obciążające dowody dotyczące zarówno źródła naruszenia, jak i wagi przestępstwa, które mogą wystarczyć do wydania nakazu przeszukania lub aresztowania.

PRZESŁUCHANIE PODEJRZANYCH

Przesłuchania podejrzanych po aresztowaniu można również wykorzystać w celu uzyskania wystarczających podstaw do wydania nakazu przeszukania w przypadku zidentyfikowania innych zaangażowanych stron. Na przykład powszechnie udokumentowano, że po aresztowaniu Sabu został informatorem FBI, dostarczając informacji, które następnie doprowadziły do aresztowania i zajęcia sprzętu innych członków LulzSec .

ANALIZA PODEJRZANYCH MEDIÓW

Dowody obciążające podejrzanych sojuszników o cyberprzestępczość można czasami znaleźć w trakcie dochodzenia kryminalistycznego dotyczącego ich nośników danych lub poprzez dostęp do używanych wirtualnych serwerów prywatnych (VPS). Również w tym przypadku dowód ten może wystarczyć do wydania nakazu zajęcia sprzętu współpracujących stron.

DOXING

Aby umożliwić współpracę grupową, niektóre stowarzyszenia hakerów Black Hat organizują swoje ataki publicznie za pośrednictwem kanałów komunikacji online, takich jak IRC i Twitter. Informacje te często mają charakter głęboko obciążający; jednakże dopóki prawdziwa identyfikacja autora jest ukryta pod pseudonimem, pozostają oni anonimowi, a tym samym bezpieczni. Dlatego jednym z głównych celów identyfikacji złośliwej strony jest często powiązanie jej z jej osobą w Internecie, np. pseudonimem IRC, pseudonimem lub nazwą użytkownika na Twitterze. W społecznościach zajmujących się kryminalistyką cyfrową i hakerami istnieje termin „doxing", który opisuje, w jaki sposób można to osiągnąć. Doxing to termin wywodzący się od słów dokument i śledzenie i zasadniczo jest procesem zbierania informacji o użytkownikach Internetu, których woleliby nie znać i których prawdopodobnie nie są świadomi, że udostępnili publicznie. Przeprowadzenie udanego „doxu" obejmuje zebranie informacji takich jak imię i nazwisko, data urodzenia, nazwa użytkownika, konto e-mail, adres domowy, numer telefonu, osobiste zdjęcia i oczywiście pseudonimy i pseudonimy danej osoby w Internecie. Techniki i praktyki niezbędne do doskonalenia doxingu obejmują głębokie zrozumienie operatorów wyszukiwarek oraz sposobu gromadzenia informacji ze źródeł internetowych, takich jak media społecznościowe, reklamy online lub gdziekolwiek indziej, gdzie informacje mogły zostać opublikowane lub wyciekły. Obejmują inteligentne metody porównywania informacji między źródłami w celu stworzenia profilu podejrzanego. Ponownie, celem cyberśledczego jest powiązanie obciążających dowodów opublikowanych pod pseudonimem z prawdziwą tożsamością podejrzanego w celu uzyskania nakazu przeszukania i/lub aresztowania.

ZBIERANIE DOWODÓW

Po wydaniu nakazu przeszukania należy uzyskać dowód podejrzenia popełnienia przestępstwa; istnieją ścisłe wytyczne dotyczące sposobu zajmowania sprzętu, uzyskiwania obrazów cyfrowych i przechowywania dowodów. Wytyczne te mogą się różnić w zależności od jurysdykcji miejsca, w którym doszło do podejrzenia przestępstwa, jednak wszystkie mają wspólne procesy związane z wymogami fizycznymi, np. zabezpieczeniem dowodów. Zostaną one omówione w kolejnych sekcjach.

PRZECHWYTYWANIE SPRZĘTU

Istotne jest przestrzeganie ścisłych wytycznych dotyczących zajęcia sprzętu. Dane znajdujące się na sprzęcie komputerowym mają charakter dynamiczny i niestabilny, a nieprawidłowe przejęcie sprzętu może prowadzić do przypadkowego usunięcia, modyfikacji lub zanieczyszczenia materiału dowodowego. Poniższa sekcja zawierająca wskazówki dotyczące tego procesu została stworzona częściowo na podstawie odniesienia Stowarzyszenia Komendantów Policji (ACPO) „Przewodnik

dobrych praktyk w zakresie elektronicznego materiału dowodowego" (7Safe, 2007). Początkowo teren należy zabezpieczyć, co oznacza, że w pobliżu sprzętu powinny znajdować się wyłącznie organy ścigania. Wszystkie osoby niezaznajomione z procesem należy trzymać z daleka od sprzętu, aby zmniejszyć ryzyko przypadkowego naruszenia dowodów. Obszar ten należy dokładnie sfotografować i nagrać wideo, upewniając się, że uchwycono jak najwięcej szczegółów dotyczących sposobu podłączenia sprzętu. Ponadto wszystkie połączenia powinny być oznaczone, aby zapewnić możliwość późniejszego pomyślnego ponownego podłączenia sprzętu w niezmienionym stanie. Jeśli system komputerowy wygląda na wyłączony, należy to najpierw sprawdzić. Urządzenie może znajdować się w trybie uśpienia lub pusty wygaszacz ekranu może sprawiać wrażenie, że jest wyłączone. Należy sprawdzić wszystkie lampki, czy się nie świecą, na przykład lampki monitorujące dysk twardy. Jeśli po dokładnym zbadaniu zostanie to rozważone aby znajdował się w trybie uśpienia, należy go traktować jako włączony, patrz następny akapit. Jeżeli zostanie potwierdzone, że jest wyłączony, nie należy go włączać, ponieważ natychmiast podważy to ważność dowodów i umożliwi podejrzanemu odrzucenie dowodu na tej podstawie, że organy ścigania nawiązały interakcję z mediami. Po upewnieniu się, że wszystkie kable, połączenia i wyposażenie systemu zostały oznaczone i zapisane zgodnie z wcześniejszym opisem, można odłączyć i zabezpieczyć system oraz wszystkie urządzenia peryferyjne i otaczający je sprzęt. Jeśli systemem jest laptop, należy wyjąć baterię, aby mieć pewność, że jest całkowicie wyłączona i nie można jej przypadkowo włączyć. Jeżeli komputer jest włączony, uznaje się go za „pod napięciem". Obrazy na ekranie powinny zostać sfotografowane. Po wykonaniu tej czynności dostępne są dwie możliwe ścieżki. Aby zapobiec zanieczyszczeniu dowodów, komputer można wyłączyć. W przypadku wybrania tej opcji zaleca się odłączenie systemu lub odłączenie akumulatora, jeśli jest to laptop, zamiast podejmować zwykłe działania polegające na zamykaniu systemu z poziomu systemu operacyjnego. Ma to na celu nie tylko ograniczenie interakcji z działającym systemem, ale także zajęcie się możliwością, że złośliwa strona ustawiła maszynę tak, aby usuwała pliki przy zamykaniu. Jednak wyłączenie działającego systemu może spowodować utratę kluczowych, ulotnych dowodów przechowywanych w ulotnej pamięci RAM, na przykład kluczy deszyfrujących i pozostałości rozmów na czatach i w mediach społecznościowych. Alternatywne podejście polega na pobraniu zawartości pamięci RAM z działającego systemu poprzez wyodrębnienie zrzutu pamięci. Szczegóły dotyczące tego, kiedy i jak należy to zrobić, omówiono w poniższej sekcji Pozyskiwanie pamięci RAM. Po zakończeniu pobierania pamięci RAM system można wyłączyć w opisanym wcześniej dworku. Wreszcie cały skonfiskowany sprzęt musi być zarejestrowany przy użyciu unikalnych identyfikatorów i mieć dołączone identyfikatory. Wszystkie działania podjęte na danym terenie w momencie zajęcia powinny zostać udokumentowane. Należy podjąć wszelkie uzasadnione wysiłki, aby zapobiec niezamierzonemu uruchomieniu sprzętu, np. umieszczając taśmę zabezpieczającą przed manipulacją przez porty USB i, jak omówiono wcześniej, upewniając się, że baterie są wyjęte z laptopów. Na kontenerach należy również zastosować taśmę zabezpieczającą, aby mieć pewność, że dowód nie zostanie zmodyfikowany ani uszkodzony podczas transportu. Każde późniejsze przemieszczenie tych dowodów musi być udokumentowane przybycie i wymeldowanie, aby zachować łańcuch dostaw.

SZUKAJ PISEMNYCH HASŁ

Nieujawnienie haseł do szyfrowania i uwierzytelniania może być źródłem frustracji dla analityków kryminalistycznych. Pliki zaszyfrowane 256-bitowo i zawierające złożone hasła nie mogą zostać złamane w sensownym czasie. Zrozumiałe jest, że podejrzani często nie chcą zrezygnować z tych haseł. W Wielkiej Brytanii „Ustawa o uprawnieniach dochodzeniowych z 2000 r." uznaje za przestępstwo „niezastosowanie się do ujawniania na żądanie klucz do wszelkich zaszyfrowanych informacji." Jednak typową obroną przed tą sytuacją jest twierdzenie, że podejrzany zapomniał hasła. W tej sytuacji organy ścigania niewiele mogą zrobić. Jak na ironię, jeśli podejrzany później przyzna się do znajomości hasła i je ujawni, może zostać oskarżony o przestępstwo pierwotnego jego zatajenia. Ponieważ jednak

większość złośliwych hakerów rozumie potrzebę posiadania niezależnych, unikalnych i złożonych haseł w celu zapewnienia prywatności, możliwe jest, że hasło będzie dla nich zbyt trudne do zapamiętania; dlatego można to zapisać. Wszystkie dokumenty w okolicy powinny zostać skonfiskowane, ponieważ mogą zawierać hasła. Książki również należy konfiskować, ponieważ częstą praktyką jest umieszczanie na ich stronach zapisanych haseł. Warto pomyśleć także o innych typowych kryjówkach, np. pod materacem łóżka. Znalezienie papierowych kopii haseł jest czasami jedyną metodą odszyfrowania zaszyfrowanych danych z nośników.

PRZEJĘCIE SĄDOWE

Najbardziej podstawowym etapem zapewniającym, że dowody pozostaną pominięte, jest zapewnienie, że oryginalny obraz nie ulegnie zmianie w trakcie procesu. W tej części omówiono, jak zachować integralność materiału dowodowego podczas tworzenia wizerunku z mediów.

RAM

Pozyskanie zrzutu pamięci wiąże się z nieodłącznym ryzykiem, dlatego należy przeprowadzić ocenę ryzyka w celu ustalenia potencjalnej korzyści w stosunku do ryzyka w danej sytuacji. Jeśli jest to wymagane i względnie bezpieczne, można je wykonać, jednakże należy zachować szczególną ostrożność, aby ograniczyć i wyjaśnić ślad akwizycji, który pozostanie w systemie. Chociaż sądy zaczynają akceptować wprowadzenie śladu , istotne jest, aby stosować właściwe narzędzia i metody oraz dokumentować cały proces, najlepiej nagrać wideo, aby zmniejszyć prawdopodobieństwo, że ślad przejęcia stanie się umorzenie sprawy. Niektóre aplikacje, takie jak czaty, złośliwe oprogramowanie i programy kryptograficzne, mogą wykorzystywać technologie zapobiegające zrzucaniu pamięci, zaprojektowane w celu zapobiegania odczytywaniu danych z chronionych obszarów pamięci RAM. Te mechanizmy zabezpieczające usuwają śmieci, np. wartości losowe lub zera zamiast prawidłowej zawartości pamięci. Inne aplikacje wykorzystują ochronę przed debugowaniem, która może spowodować zablokowanie lub ponowne uruchomienie systemu przy próbie odczytania chronionej pamięci RAM. Ze względu na rozwój tych metod antykryminalistycznych pożądane jest użycie narzędzia do przechwytywania pamięci, które działa w trybie „jądra", a nie „użytkownika". Tryb jądra umożliwia nieograniczony dostęp do podstawowego sprzętu, np. pamięci RAM, i jest mniej prawdopodobne, że naruszy dowody w wyniku awarii systemu, ani nie zapewni fałszywych dowodów. Wybrane narzędzia powinny również pozostawiać jak najmniej miejsca i działać w trybie tylko do odczytu. Większość narzędzi do pozyskiwania pamięci RAM jest przenośna, zwykle ma postać urządzenia USB i ponownie nie wymaga instalacji, aby ograniczyć zajmowaną powierzchnię. Po wykonaniu zrzutu pamięci komputer należy wyłączyć, korzystając z metod omówionych wcześniej.

OBRAZ

Istotne jest, aby proces analizy kryminalistycznej mediów nie wprowadził żadnych zanieczyszczeń ze strony badacza. Interakcja z nośnikami danych bez odpowiednich środków ostrożności spowoduje zapisanie danych na nośniku i potencjalnie unieważni dowód. Aby zmniejszyć prawdopodobieństwo takiego zdarzenia, analizy kryminalistycznej nie należy przeprowadzać na faktycznie skonfiskowanym urządzeniu do przechowywania multimediów, lecz na obrazie, czyli repliki nośnika sektor po sektorze. Istnieje wiele narzędzi programowych umożliwiających pozyskiwanie obrazów z mediów i omawianie ich indywidualnie nie wchodzi w zakres tej pracy. Zaleca się jednak, aby wybrane narzędzie uruchamiało się z działającej płyty CD/DVD i aby dowody były montowane przez narzędzie w trybie „tylko do odczytu", aby zmniejszyć prawdopodobieństwo przypadkowego zapisania na nim. Dalszą pewność, że dowody nie zostały skażone, można zapewnić poprzez zastosowanie blokad zapisu. Blokady zapisu to urządzenia które są umieszczone w linii pomiędzy systemem używanym do analizy multimediów a samym urządzeniem do przechowywania multimediów. Umożliwiają przesyłanie

poleceń odczytu do urządzenia magazynującego multimedia, ale blokują polecenia zapisu. Blokery zapisu są łatwo dostępne i umożliwiają podłączanie do i z różnych interfejsów, np. kontrolerów USB, Firewire, SCSI i SATA. Na koniec, gdy obraz zostanie uzyskany, należy go zweryfikować jako dokładną kopię, porównując wartości skrótu dwóch obrazów. Wartości skrótu to ciąg bitów o stałym rozmiarze utworzony w wyniku przekazania danych przez kryptograficzną funkcję skrótu. Jakakolwiek modyfikacja dowodu, niezależnie od tego, jak mała jest, spowoduje zmianę jego wartości skrótu. Jeżeli pliki skrótu uzyskanego obrazu i badanego nośnika różnią się, wówczas albo obraz jest nieważny, albo sam dowód został naruszony.

ANALIZA SĄDOWA

Specjalista medycyny sądowej zwykle otrzymuje pewne uprawnienia w zakresie celu dochodzenia, na przykład ustalenia, za jakie przestępstwo może być odpowiedzialny podejrzany. Często jednak udostępniane informacje mogą nie być tak szczegółowe. Powodem przyznania badaczowi wąskich kompetencji jest zapobieganie potencjalnemu stronniczości wynikającej z wcześniejszej wiedzy. Na przykład badacz może zostać po prostu poproszony o dostarczenie dowodów potwierdzających profil maszyny jest skonfigurowana do złośliwego włamania, może też zostać poproszona o znalezienie dowodów na poparcie przypuszczenia, że konkretna osoba internetowa i podejrzany to jedna i ta sama osoba. W takich okolicznościach często pożądane jest zapewnienie, że znalezione dowody nie są stronnicze i że zostaną znalezione niezależnie od specyfiki sprawy (patrz rozdział 8). Chociaż przedmiot dochodzenia kryminalistycznego będzie zależał od przedstawionego zakresu, w większości przypadków zebrane dowody cyfrowe będą składać się z jednego lub większej liczby artefaktów .

ANTYKRYMINALISTYKA

Złośliwi hakerzy stają się coraz bardziej świadomi metod analizy kryminalistycznej. W rezultacie często wdrażają środki zaradcze, aby uniemożliwić śledczemu zebranie przydatnych dowodów. Praktykę tę określa się mianem antykryminalistyki lub czasami antykryminalistyki. Zasadniczo praktyka ta polega na eliminowaniu lub zaciemnianiu dowodów dotyczących działalności przestępczej lub złych zamiarów. Mając to na uwadze, głównym celem tej sekcji jest omówienie kryminalistyki przechowywania nośników twardych, ze szczególnym uwzględnieniem identyfikacji miejsc, w których można odkryć dowody przechowywane w słabo sformatowanych obszarach nośnika; obszarach, które albo są odporne na antykryminalistykę, albo które po prostu mogły nie zostać wzięte pod uwagę przez podejrzanego. W tej sekcji pokrótce omówiono także typowe techniki analizy kryminalistycznej, a ze względu na rosnącą tolerancję sądów w uznawaniu analizy RAM za dopuszczalną, również i tę omówiono.

ANALIZA RAMU

Jeśli z obrazu pobrano zrzut pamięci RAM, należy go przeanalizować na osobnym komputerze, aby uniknąć zanieczyszczenia dowodów. Istnieje wiele narzędzi, które można wykorzystać do analizy pamięci RAM; na uwagę zasługuje narzędzie Volatility, które zyskuje reputację podstawowego narzędzia wiersza poleceń typu open source do tego celu . Narzędzia takie jak Volatility pozwalają na analizę takich danych jak:

- Uruchomione i niedawno zakończone procesy
- Pliki mapowane w pamięci
- Otwarte i ostatnio zamknięte połączenia sieciowe
- Odszyfrowane wersje programów, danych i informacji

• Hasła klucza kryptograficznego

• Złośliwe oprogramowanie

Rzeźbienie danych i magiczne wartości

Jedną z głównych metod analizy pamięci RAM jest metoda zwana „rzeźbieniem danych". Rzeźbienie to proces poszukiwania wzorców w danych, czasami nazywanych „wartościami magicznymi". Wartości te wskazują, że w pamięci znajduje się określony typ danych. Na przykład wiadomości Skype v3 zaczynają się od danych „l33l", więc po każdym obszarze pamięci RAM zawierającym te znaki istnieje prawdopodobieństwo, że po nich nastąpi wiadomość Skype. Podobnie hasła TrueCrypt (2014) zawierają magiczną wartość „0x7d0". Typy plików istniejące w pamięci RAM (a także w pamięci multimedialnej lub przechodzące przez sieć) można również zidentyfikować na podstawie ich magicznych wartości. Po znalezieniu danych określonego typu, proces rzeźbienia danych może być kontynuowany, w zależności od rodzaju wykrytych danych, w celu wyodrębnienia i zaprezentowania danych w sposób, który stanie się bardziej zrozumiały dla analityka kryminalistycznego. Na przykład może być konieczne uporządkowanie danych w oparciu o granice pól, ich oddzielenie i zidentyfikowanie. W większości przypadków eksperta medycyny sądowej można oddzielić od szczegółów tych procesów za pomocą narzędzi kryminalistycznych. Jednakże jedną z głównych zalet otwartych narzędzi, takich jak Volatility, jest to, że umożliwiają one specjalistom medycyny sądowej kodowanie własnych modułów, co pozwala na swobodę wyodrębniania danych określonego typu, które nie są dostępne natywnie. Można to następnie udostępnić na korzyść ze społeczności open source .

PRZECHOWYWANIE MEDIÓW

W tej sekcji skupiono się zarówno na znanych, jak i niejasnych praktykach i procesach analizowania urządzeń do przechowywania multimediów pod kątem dowodów kryminalistycznych. Zawarto tutaj krótkie streszczenie struktury i formatu dysku twardego, aby dać kontekst dla kolejnych sekcji.

STRUKTURA I FORMAT DYSKU TWARDEGO

Dyski twarde składają się z jednego lub większej liczby wirujących dysków pokrytych folią magnetyczną, zwanych talerzami. Każdy talerz jest podzielony na koncentryczne pasma zwane ścieżkami; ścieżki znajdujące się w tym samym obszarze każdego talerza są wspólnie określane jako cylinder. Każda ścieżka jest podzielona na sektory, przy czym każda ścieżka ma identyczną liczbę sektorów niezależnie od jej położenia na talerzu, dlatego sektory są gęściej zapełnione na środku talerza. Sektor to najmniejszy możliwy obszar pamięci dostępny na dysku i ma zazwyczaj rozmiar 512 bajtów. Informacje są odczytywane i zapisywane w sektorach za pomocą głowic generujących pola magnetyczne zgodnie z instrukcjami kontrolera dysku, który z kolei otrzymuje instrukcje od plików i systemów operacyjnych. Chociaż obie strony talerza służą do przechowywania informacji, jedna strona jednego z talerzy służy do informacji o położeniu ścieżek; informacja ta jest kodowana fabrycznie i służy do ustawiania głowic podczas przemieszczania się pomiędzy ścieżkami i sektorami. Liczba sektorów i ścieżek oraz ich położenie są ustawiane fabrycznie przy użyciu procesu określanego jako formatowanie niskiego poziomu. Formatowanie niskiego poziomu jest wykonywane tylko raz i nie jest wykonywane przez użytkownika dysku twardego po zakupie, chociaż termin formatowanie niskiego poziomu (LLF) jest czasami błędnie używany do opisania procesu ponownej inicjalizacji dysku do stanu fabrycznego. Sposób, w jaki komputer komunikuje się z dyskiem twardym, jest ustawiany przez podstawowy system wejścia/wyjścia komputera (BIOS). Schemat adresowania, np. adresowanie bloków logicznych (LBA), jest ustawiany dla dysku w systemie BIOS. Adres bloku logicznego to 28-bitowy adres odwzorowujący określony sektor dysku. Należy zauważyć, że chociaż LBA jest najbardziej rozpowszechnionym

schematem adresowania, inne są powszechne, np. starszy schemat adresowania cylindra, głowicy, sektora (CHS) lub powstający schemat adresowania globalnie unikalny identyfikator (GUID).

PARTYCJE

Partycje to części dysku twardego; każdą partycję można sformatować do użytku przez określony system plików. W obecnej architekturze IBM PC możliwe jest posiadanie maksymalnie czterech partycji, z których jedna może być rozszerzoną partycją podstawową. Rozszerzoną partycję można dalej podzielić, co pozwala na utworzenie dodatkowych 24 partycji logicznych

partycje jak pokazano:

Partycja podstawowa nr 1

Partycja podstawowa nr 2

Partycja podstawowa nr 3

Partycja podstawowa nr 4

Partycja logiczna nr 1

Partycja logiczna nr 2

Partycja logiczna nr 3

…

…

Partycja logiczna nr 24

Jedna z partycji podstawowych zostanie oznaczona jako partycja aktywna i to właśnie ona będzie używana do uruchamiania komputera z systemem operacyjnym. Utworzenie pierwszej partycji na dysku spowoduje utworzenie głównego rekordu rozruchowego (MBR), który między innymi przechowuje informacje dotyczące partycji.

GŁÓWNY REKORD ROZRUCHU

MBR jest przechowywany w pierwszym sektorze dysku twardego i tworzony wraz z pierwszą partycją na dysku. Jest ładowany do pamięci jako jedna z pierwszych akcji podczas uruchamiania systemu. MBR składa się z małej części kodu niezależnego od systemu operacyjnego, podpisu dysku, tablicy partycji i podpisu MBR. Podpis dysku to unikalny czterobajtowy identyfikator dysku twardego, co oznacza, że powinien być unikalny dla każdego dysku podłączonego do systemu. Służy do takich celów, jak identyfikacja woluminu rozruchowego oraz kojarzenie partycji i woluminów z określonym dyskiem. Podpis MBR, czasami nazywany liczbą magiczną, ma ustawioną wartość 0xAA55, która po prostu identyfikuje go jako prawidłowy MBR. Tabela partycji informuje o pozycji początkowej i długości każdej partycji na dysku twardym. Podczas uruchamiania systemu w pierwszej kolejności wykonywany jest kod MBR, który odpowiada za analizę tablicy partycji i identyfikację, która partycja jest oznaczona jako aktywna. Po zidentyfikowaniu aktywnej partycji kontrola jest przekazywana do sektora startowego tej partycji, czasami określanego jako rekord rozruchowy woluminu (VBR). Plik VBR jest tworzony, gdy dysk jest sformatowany na wysokim poziomie do użytku z określonym systemem operacyjnym.

BLOK PARAMETRÓW VBR I BIOS

VBR zawiera kod specyficzny dla systemu operacyjnego niezbędny do załadowania systemu operacyjnego, wraz z blokiem parametrów BIOS (BPB), który opisuje format systemu plików partycji, np. liczbę ścieżek na sektor i liczbę sektorów na klaster. Klastry, często określane jako jednostki alokacji lub jednostki AU, to najmniejszy obszar pamięci dostępny dla systemu operacyjnego. System plików przydziela wiele sektorów, np. osiem, pojedynczemu klasterowi, aby zmniejszyć obciążenie związane z zarządzaniem dyskami, co skutkuje większą szybkością odczytu i zapisu, ale także powoduje marnowanie części miejsca na dysku podczas przechowywania plików lub części plików, co są mniejsze niż rozmiar klastra. Ta zmarnowana przestrzeń w klastrach nazywana jest swobodną przestrzenią.

SYSTEM PLIKÓW

Istnieje wiele systemów plików obsługujących wiele różnych systemów operacyjnych, każdy działa inaczej, ale wszystkie mają ten sam główny cel; mianowicie do zarządzania sposobem przechowywania, indeksowania, zapisywania i odczytywania plików i katalogów. Wraz z VBR są one tworzone w momencie formatowania dysku i ładowane podczas procesu uruchamiania z VBR. Przykładami systemów plików są NTFS, FAT32, ext4, XFS i btrfs. .

TABELA PLIKÓW

Tabele plików przechowują informacje o każdym pliku, w tym o jego lokalizacji, rozmiarze, uprawnieniach, znacznikach czasu i tym, czy został on usunięty, tj. czy oznaczono miejsce do ponownego wykorzystania. Informacje te same w sobie są zapisywane w specjalnych plikach używanych przez system plików, dlatego też sama tabela plików będzie zawierała wpis samoodwołujący się. W systemie NTFS dwa pliki używane do przechowywania tych informacji to $MFT i $Bitmap, pierwszy zawiera informacje dotyczące plików, a później dotyczące tego, które klastry są używane, a które nie.

WYSZUKIWANIE DOWODÓW

Dostępnych jest wiele narzędzi kryminalistycznych umożliwiających analizę kryminalistyczną, niektóre są zastrzeżone, a inne są dostępne na licencjach bezpłatnych lub typu open source. Zastrzeżone narzędzia, takie jak Encase i FTK są szeroko stosowane przez organy ścigania, a bezpłatne narzędzia typu open source, takie jak Autopsy , zyskują popularność wśród niezależnych śledczych i konsultantów. Poszczególne narzędzia mają swój własny zestaw mocnych i słabych stron i nie jest intencją ich tutaj porównywanie. Jednakże wykazują pewne podobieństwa pod względem funkcjonalności i działania, a cele badania są takie same niezależnie od wybranego narzędzia lub narzędzi. Dlatego też dyskusja w tej sekcji obejmie sposób wykrywania i odkrywania artefaktów na dyskach twardych, a nie będzie skupiać się na praktycznych aspektach wykorzystania narzędzi do osiągnięcia tego celu .

WYSZUKIWANIE SŁÓW KLUCZOWYCH I WYRAZÓW

Podstawowym narzędziem większości oprogramowania kryminalistycznego do celów śledczych jest funkcja wyszukiwania. Można wyszukiwać słowo lub frazę związaną z dochodzeniem. Słowo lub fraza może pasować na dysku twardym jako tekst ASCII lub może stanowić część pliku złożonego. Pliki złożone to pliki, których informacje opierają się na aplikacji, na przykład pliki zip, pliki e-mail, dokumenty Microsoft Office i Adobe; większość narzędzi śledczych może renderować formaty najpopularniejszych plików złożonych. Wyszukiwania można również używać do wyszukiwania samych plików, dopasowując słowa kluczowe do ich nazw plików. Można także identyfikować i katalogować określone typy plików złożonych, na przykład pliki obrazów, takie jak pliki jpeg, bmp i png. Wyszukiwania te należy wykonywać przy użyciu magicznych liczb plików, o których była mowa

wcześniej. Zapobiega to ukrywaniu prawdziwego celu plików przez złośliwe strony poprzez zmianę jego rozszerzenia. Większość narzędzi kryminalistycznych umożliwia oznaczenie wszelkich dowodów, które uznasz za istotne, i powiązanie ich ze sprawą. Niektóre umożliwiają także przeglądanie plików za pomocą wbudowanych aplikacji natywnych, które nie zapisują do materiału dowodowego, zachowując w ten sposób jego integralność.

ODZYSKIWANIE USUNIĘTYCH INFORMACJI

Usunięcie plików, folderów i partycji niekoniecznie jest trwałe i często można je odzyskać. Odzyskiwanie plików, folderów i partycji zostało pokrótce omówione tutaj.

ODZYSKIWANIE USUNIĘTYCH PLIKÓW I FOLDERÓW

Proces usuwania plików i folderów polega po prostu na oznaczeniu klastrów używanych przez usunięty plik lub folder jako nieprzydzielonych w tabeli plików. Do czasu fizycznego nadpisania klastrów dane w pliku lub folderze pozostają dostępne w nieprzydzielonych klastrach. Większość narzędzi kryminalistycznych pozwoli na identyfikację i odzyskanie usuniętych plików, których klastry nie zostały jeszcze nadpisane.

ODZYSKIWANIE USUNIĘTYCH PARTYCJI

Usunięcie partycji powoduje, że znajdujące się na nich dane stają się niedostępne dla systemu operacyjnego; jednakże same dane nie ulegają zniszczeniu w momencie usunięcia i często można je odzyskać. Informacje o tym, jakie sektory zajmowała usunięta partycja, są rejestrowane w tablicy partycji przechowywanej w MBR. Większość narzędzi analizuje informacje w tabeli partycji, umożliwiając badaczowi sprawdzenie nazw partycji, usuniętych lub innych, oraz sektora, w którym się one zaczynają i kończą. Korzystając z tych informacji, można zlokalizować VBR, czyli zapasowy VBR, dla dowolnej pojedynczej partycji. Lokalizacja różni się w zależności od używanego systemu plików, ale jest dobrze udokumentowana dla wszystkich popularnych systemów plików. Po zlokalizowaniu większość narzędzi przeanalizuje informacje w VBR, umożliwiając badaczowi odbudowanie usuniętej partycji.

GDZIE SCHOWAJĄ SIĘ DOWODY

W poniższych sekcjach omówione zostaną niektóre z bardziej skomplikowanych kryjówek istniejących w systemach operacyjnych Microsoft Windows. Niektóre z tych miejsc mogą zostać przeoczone podczas badań kryminalistycznych, a mimo to często zawierają dużo materiału dowodowego.

REJESTR

Rejestr jest odpowiedzialny za przechowywanie ustawień systemowych i informacji konfiguracyjnych dotyczących wszystkich aspektów systemu operacyjnego Windows i zainstalowanego oprogramowania. We współczesnych systemach operacyjnych Windows rejestr składa się z pięciu plików przechowywanych w folderze Winnt\system32\config\, a mianowicie Default, System, Security, Software i Sam, przy czym inny plik Ntuser.dat jest obecny dla każdego użytkownika systemu .W działającym systemie rejestr można sprawdzić i zmodyfikować za pomocą edytora rejestru regedit. Regedit łączy informacje przechowywane w plikach w gałęzie, format zaprojektowany tak, aby informacje były bardziej dostępne dla użytkownika. Informacje te są zorganizowane w ramach kluczy uchwytów, zwanych kluczami HKEY, które z kolei zawierają podklucze i powiązane wartości (nazwa, typ i dane). Te klucze to KEY_LOCAL_MACHINE(HKLM), HKEY_USERS (HKU), HKEY_CURRENT_USER (HKCU), HKEY_CLASSES_ROOT (HKCR) i HKEY_CURRENT_CONFIG (HKCC). Większość śledczych użyje narzędzia, które pozwoli im wyodrębnić dane z plików rejestru i przedstawić je w widoku

dostosowanym do dochodzenia. Chociaż rejestr większości systemów Windows jest duży i złożony, a pełne omówienie go wykraczałoby poza zakres tej pracy.

OSTATNIE UŻYWANE LISTY

Ostatnio używane (MRU) zostały zaprojektowane jako wygoda dla użytkownika. Po ponownym przejrzeniu niektórych pól wejściowych użytkownika użytkownicy mogą albo zobaczyć poprzednio wprowadzone informacje na liście, albo mogą zostać one automatycznie uzupełnione podczas pisania. Listy te są w większości wyodrębniane z pliku NTUSER.DAT. Przykłady list MRU obejmują: zmapowane dyski sieciowe, odtwarzacz multimediów, zapisane lub skopiowane otwarte okna, aplikacje otwarte w oknie uruchamiania, historię Google, ostatnio otwierane dokumenty i wyszukiwane hasła używane w polu wyszukiwania.

OSTATNI CZAS ZAPISU

Za każdym razem, gdy klucz jest otwierany, tworzony, usuwany lub modyfikowany, rejestrowany jest czas. Nazywa się to czasem „LastWrite". Umożliwia to badaczowi utworzenie harmonogramu działań, na przykład kiedy ostatni raz podłączono dysk twardy USB, kiedy zainstalowano oprogramowanie itd.

HIBERFIL.SYS

Hibernacja to funkcja stosowana w nowoczesnych systemach operacyjnych Windows, umożliwiająca całkowite zamknięcie systemu przy jednoczesnym zachowaniu ostatniego stanu roboczego po ponownym włączeniu zasilania. Odbywa się to poprzez skopiowanie systemowej pamięci RAM do pliku w momencie wprowadzenia systemu w stan hibernacji i przywrócenie jej z pliku po ponownym uruchomieniu komputera. Plik ten nazywa się hiberfil.sys i znajduje się w katalogu głównym dysku, zwykle oznaczonym jako C:\, a jego rozmiar odzwierciedla ilość dostępnej systemowej pamięci RAM. Jak można się spodziewać, z tego pliku można wyodrębnić potencjalnie istotne dowody, w podobny sposób, jak w przypadku analizy pamięci RAM. W chwili pisania tego tekstu struktura pliku nie była dobrze udokumentowana; przy ograniczonej liczbie narzędzi, które mogą wyrzeźbić plik. Warto jednak ponownie zwrócić uwagę na narzędzie do sprawdzania zmienności, które zawiera wtyczkę imagecopy, umożliwiającą konwersję pliku hiberfil.sys na surowy obraz. Obraz ten można następnie przeanalizować za pomocą narzędzia Volatility lub innych narzędzi w celu znalezienia dowodów, np. haseł, certyfikatów cyfrowych i złośliwego oprogramowania.

PAGEFIL.SYS

Aby umożliwić systemowi operacyjnemu dostęp do większej ilości pamięci RAM, niż jest ona fizycznie dostępna, wykorzystywany jest plik stronicowania. Gdy system operacyjny Windows potrzebuje więcej pamięci RAM niż jest dostępna, część z niej można zapisać w pliku stronicowania przed zwolnieniem i zwolnieniem pamięci fizycznej. Gdy informacje zawarte w pliku stronicowania są wymagane przez działający proces, są one pobierane z pliku z powrotem do pamięci. Ponieważ plik zawiera dane przechowywane w pamięci RAM, może stanowić nieocenione źródło dowodów dla osoby przeprowadzającej badanie, np. przemycane obrazy, hasła, podpisy cyfrowe i tak dalej. Wszystkie wspomniane wcześniej narzędzia kryminalistyczne, np. Encase, FTK i Autopsy, są w stanie wyciąć plik pagefil.sys, aby umożliwić przeglądanie i wydobywanie z niego dowodów.

FOLDERY INFORMACYJNE O WOLUMENIE SYSTEMU

W systemach operacyjnych począwszy od XP i nowszych dostępna jest funkcja przywracania systemu wywołania funkcji. Przywracanie systemu przechowuje „migawkę" stanu ważnego systemu operacyjnego, np. Windows, plików na dysku twardym w dowolnym momencie. Jeśli coś pójdzie nie

tak z komputerem, na przykład nieudana instalacja jakiegoś oprogramowania, co spowoduje, że komputer przestanie działać lub będzie niestabilny, można go „przywrócić", to znaczy przywrócić do tego migawki. Poprzednie wersje plików zostaną odzyskane, a komputer powinien znów zacząć działać. Domyślne zachowanie polega na tym, że te migawki są tworzone w systemie Windows 7 raz w tygodniu i na początku procesu instalacji oprogramowania. Alternatywnie można je ustawić ręcznie. Przywracanie systemu ma stałą ilość miejsca, która jest używana do przechowywania punktów przywracania i zapisuje w tym miejscu tyle, ile się da, w sposób okrężny, przy czym najstarsze punkty przywracania są zastępowane najnowszymi. Ilość miejsca można konfigurować, ale w systemach Windows Vista i 7 domyślnie wynosi ona 15%. Z punktu widzenia medycyny sądowej te migawki mogą zawierać kopie plików, które następnie zostały usunięte lub zmodyfikowane. Przy rozważaniu tego istotne znaczenie ma fakt, że kopie plików, które zostały zaszyfrowane, mogą nadal znajdować się w folderach z informacjami o wolumenie systemowym w stanie niezaszyfrowanym. Dlatego też, chociaż odszyfrowanie niektórych plików jest często niemożliwe, może się zdarzyć, że uda się znaleźć ich niezaszyfrowaną kopię w folderach z informacjami o wolumenie systemowym. Migawki obejmują kopie zapasowe rejestru, plików systemu Windows (w folderze \Windows) i profilu użytkowników lokalnych. Profil użytkownika zawiera artefakty, w tym wszelkie pliki przechowywane w obszarze „Moje dokumenty", ustawienia aplikacji, ulubione w Internecie, pulpit użytkownika (w tym wszelkie zapisane na nim pliki), internetowe pliki cookie, łącza do folderów udostępnionych i kosz. To drugie rozwiązanie może być szczególnie dochodowe, ponieważ podejrzany mógł opróżnić kosz aktywnego systemu, nie wiedząc, że pliki nadal znajdują się w koszu w folderach z informacjami o wolumenie systemowym. Foldery z informacjami o woluminie systemowym znajdują się w katalogu głównym dysku twardego w folderze o nazwie „Informacje o woluminie systemowym". W tym folderze istnieje oddzielny zestaw kopii woluminu dla każdego utworzonego punktu przywracania. Wiele narzędzi kryminalistycznych jest w stanie natywnie analizować informacje zawarte w folderach z informacjami o wolumenie systemowym. Alternatywnie foldery można zamontować ręcznie jako dyski. Proces ten jest dobrze znany, a procedura krok po kroku została udokumentowana w artykule bazy wiedzy firmy Microsoft kb309531 (Microsoft, 2013). Po zamontowaniu wolumin można go przechwycić i przeanalizować w taki sam sposób, jak dysk fizyczny, jak omówiono wcześniej.

PODSUMOWANIE

Przedstawiono wytyczne i wskazówki dla lekarzy sądowych. Omówiono kwestie niezbędne przy formułowaniu podstaw do wydania nakazu przeszukania, tj. konieczność wykazania, że istnieją „uzasadnione podstawy" lub „prawdopodobna przyczyna", że przestępstwo ma, ma lub będzie miało miejsce. Omówiono metody, jak to zrobić, takie jak powiązanie domniemanego przestępstwa z adresem IP podejrzanego, kontami w mediach społecznościowych lub pseudonimem IRC; podobnie jak trudności, jakie można napotkać, próbując to zrobić. Zaproponowano kontynuację tej najlepszej praktyki w zakresie zatrzymywania dowodów; obejmuje to, jak uniknąć zanieczyszczenia dowodów cyfrowych i zminimalizować wpływ przejęcia. Omówiono zastosowanie blokad zapisu w przypadku urządzeń do przechowywania multimediów i podkreślono potrzebę analizy ryzyka i zysku przed wykonaniem analizy kryminalistycznej pamięci RAM. Aby zapewnić kontekst, udokumentowano strukturę i format dysków twardych; włączając struktury fizyczne, np. talerze i głowice, wraz ze strukturami logicznymi, takimi jak sektory i klastry. Opisano również, w jaki sposób systemy plików i systemy operacyjne korzystają z nośników, np. tabele plików oraz główne i wolumenowe rekordy rozruchowe. W ostatniej części podkreślono niektóre z bardziej przydatnych obszarów poszukiwań dowodów kryminalistycznych, wraz ze sposobem formatowania danych w tych obszarach i sposobem ich renderowania. W tym celu omówiono rejestr systemu Windows, hiberfil.sys, pagefile.sys i foldery z informacjami o wolumenie systemowym.

Edukacja, szkolenia i świadomość w zakresie kryminalistyki cyfrowej

WSTĘP

We w pełni połączonym, prawdziwie zglobalizowanym świecie sieci, w szczególności Internetu, technologii mobilnych, rozproszonych baz danych, handlu elektronicznego i e-administracji, przestępczość elektroniczna objawia się jako pranie pieniędzy; Kradzież własności intelektualnej; oszustwo/kradzież tożsamości; Nieautoryzowany dostęp do informacji poufnych; Niszczenie informacji; narażenie na obsceniczne materiały; Spoofing i phishing; Wirusy i robaki, cyberprześladowanie, szpiegostwo gospodarcze, żeby wymienić tylko kilka. Według Komisji Spraw Wewnętrznych Izby Gmin, piąty raport z sesji 2013–2014 na temat przestępczości elektronicznej, „Norton obliczył swój globalny koszt na 388 miliardów dolarów rocznie pod względem strat finansowych i straconego czasu. To znacznie więcej niż łączna roczna wartość światowego handlu heroiną, kokainą i marihuaną wynoszącą 288 miliardów dolarów".

Od czasu uruchomienia pierwszej brytyjskiej strategii bezpieczeństwa cybernetycznego w czerwcu 2009 r. i krajowego programu bezpieczeństwa cybernetycznego (NCSP) w listopadzie 2011 r. rządy Wielkiej Brytanii stosują scentralizowane podejście do cyberprzestępczości i szerzej rozumianych zagrożeń cybernetycznych. Do niedawna przestępstwa elektroniczne musiały być rozpatrywane na podstawie przepisów prawnych odnoszących się do starych przestępstw, takich jak spisek mający na celu popełnienie oszustwa, kradzieży, nękania i kradzieży tożsamości. Sytuacja nieco się zmieniła w 1990 r., kiedy uchwalono ustawę o nadużyciach komputerowych, ale nawet wtedy była ona niewystarczająca i obejmowała głównie przestępstwa związane z hakowaniem. Od czasu ustawy Computer Misuse Act z 1990 r. do ustawy o oszustwach z 2006 r. nie wprowadzono żadnych nowych przepisów dotyczących przestępstw komputerowych. Prawa, na których się opieramy, są następujące:

• Ustawa o kradzieży z 1968 i 1978 r. (nowelizacja) z 1996 r

• Ustawa o próbach karnych z 1981 r

• Ustawa telekomunikacyjna z 1984 r

• Ustawa o porządku publicznym z 1986 r

• Ustawa o ochronie dzieci z 1978 r

• Ustawa o publikacjach obscenicznych z 1959 i 1964 r

• Ustawa o ochronie danych z 1998 r

• Ustawa o prawach człowieka z 1998 r

• Ustawa o zniesławieniu z 1952 i 1996 r

• Ustawa o próbie karnej z 1981 r

• Ustawa o wolności informacji z 2000 r

• Ustawa o ochronie przed molestowaniem z 1997 r

Mimo to pozew w dalszym ciągu nie jest odpowiedni do zwalczania przestępczości elektronicznej ze względu na szybkie tempo rozprzestrzeniania się technologii informatycznych i systemów informatycznych. W 2006 r. przyjęto dwie nowe ustawy mające na celu walkę z przestępczością elektroniczną, a mianowicie ustawę o oszustwach z 2006 r., która weszła w życie w 2007 r., a której „nowa ustawa ma na celu zamknięcie szeregu luk w postępowaniu legislacyjnym dotyczącym

zwalczania nadużyć finansowych, ponieważ – zdaniem rządu – nie nowoczesne oszustwa" oraz ustawę o policji i wymiarze sprawiedliwości z 2006 r. (część 5), która zabrania „nieuprawnionego dostępu do materiałów komputerowych; nieuprawnione działania mające na celu zakłócenie działania komputera i udostępnienie narzędzi mogących zostać wykorzystanych do celów hakerskich" (Ustawa o Policji i Sprawiedliwości z 2006 r.). Udokumentowane wytyczne, praktyki i procedury były przestarzałe i całkowicie niewystarczające, aby pomóc w zwalczaniu dowodów elektronicznych w kryminalistyce, aż do pierwszej publikacji ACPO w sprawie przestępstw elektronicznych w lipcu 2007 r., a następnie zmienionej w listopadzie 2009 i 2012 r. Wytyczne te uznawane są za najlepsze wytyczne, jakie kiedykolwiek opracowano aby pomóc organom ścigania w postępowaniu z dowodami cyfrowymi (Wytyczne ACPO, 2009). Dowody cyfrowe to dowody pobierane ze stacji roboczych podejrzanego lub nośnika elektronicznego, które można wykorzystać w celu wsparcia dochodzeń z zakresu medycyny sądowej. Zasadniczo istnieją dwa rodzaje dowodów, które mogą wesprzeć cyfrowe dochodzenie kryminalistyczne, a mianowicie dowody fizyczne i dowody cyfrowe. Dowody rzeczowe dzieli się na przedmioty dotykalne i istotne, które można wnieść do sądu i pokazać fizycznie. Przykładami dowodów fizycznych, które mogą pomóc w dochodzeniu, są komputery, zewnętrzne dyski twarde i urządzenia do przechowywania danych (pendrive'y i karty pamięci), urządzenia podręczne, w tym telefony komórkowe/smartfony, urządzenia PDA, urządzenia sieciowe, nośniki optyczne, klucze sprzętowe i odtwarzacze muzyczne. Dowodem cyfrowym są dane wyodrębnione z dowodu fizycznego lub systemu komputerowego. Aby fragment informacji lub danych można było uznać za dowód, musi on spełniać pięć zasad, którymi są:

1. Dowód powinien być dopuszczalny i wyłączony przed sąd

2. dowody muszą być autentyczne i niezanieczyszczone

3. Dowody muszą dotyczyć całego utworu, a nie tylko jego orientacyjnych części

4. dowód musi być wiarygodny i niezawodny

5. dowody muszą być wiarygodne

Dowody cyfrowe w porównaniu z twardymi dowodami są trudne do znalezienia pod względem określenia charakteru danych i zaklasyfikowania ich jako dowodu cyfrowego godnego przedstawienia w sądzie. Udowodnienie, że dowody są wiarygodne, okazało się trudnym zadaniem i to nie tylko ze względu na charakter dowodów, ale także szeroki zakres i środowisko, w jakim dowody są pozyskiwane. W środowisku korporacyjnym zespół dochodzeniowo-śledczy będzie musiał zidentyfikować, zabezpieczyć i utrzymać integralność dowodów oraz rozróżnić, czy dowód ma związek z bieżącym przestępstwem będącym przedmiotem dochodzenia oraz czy miałby szansę na znalezienie winnego i postawienie mu zarzutów na drodze postępowania sądowego. Do czynników, które śledczy musi ocenić podczas gromadzenia dowodów cyfrowych, należą wydatki, koszty i poniesione straty, a także dostępność usługi w trakcie zdarzenia i po nim. Brak wiedzy specjalistycznej organów ścigania, umożliwiającej zrozumienie zawiłości przestępczości elektronicznej, szerokiego spektrum demograficznego, jakiego dotyczy, a przede wszystkim kwestii związanych z jurysdykcją, był doskonałą okazją dla osób z sektora prywatnego, ponieważ ukazał niszę i zapotrzebowanie na rynku prywatnych osób oferujących usługi z zakresu informatyki śledczej. Pojawiło się wiele prywatnych firm oferujących początkowo usługi odzyskiwania danych, a ostatecznie usługi informatyki śledczej. W tym samym czasie na rynku pojawiło się wiele narzędzi komputerowych, takich jak Encase, FTK, Helix, Paraben Cell Seizure, MOBILedit, BitPim itp. Narzędzia te, zarówno programowe, jak i sprzętowe, automatyzowały przetwarzanie dowodów komputerowych i nie wymagały -głęboki proces myślowy lub znajomość informatyki w celu ich obsługi. Ułatwiało to życie tym, którzy musieli przetwarzać dowody komputerowe, ale jednocześnie dawało fałszywe poczucie bezpieczeństwa i przekonanie, że jeśli

można odpowiednio wykorzystać te narzędzia, utwierdza to ich w przekonaniu, że są ekspertami. Organy ścigania w dużym stopniu polegają na tych narzędziach i usługach, a wobec braku odpowiednich procesów oceny narzędzi i usług, osoby i firmy nieposiadające odpowiednich kwalifikacji, zrozumienia lub wystarczającego doświadczenia są niestety traktowane jako eksperci w dziedzinie informatyka śledcza.

PRZYGOTOWANIE I SZKOLENIE LABORATORIUM CYFROWEJ KRYMINALISTYKI

Aby założyć laboratorium kryminalistyczne, należy przestrzegać szeregu procesów i procedur. Jeśli laboratorium wymaga akredytacji, jednostki akredytujące, takie jak Międzynarodowe Organizacje Normalizacyjne lub Dyrektorzy Laboratoriów Amerykańskiego Towarzystwa Kryminalnego, ustalają dalsze wymagania (Jones i Valli, 2004; Watson i Jones, 2013). Istnieje wiele standardów istotnych przy tworzeniu cyfrowego laboratorium kryminalistycznego, m.in.: Systemy zarządzania środowiskowego (ISO 14000), Bezpieczeństwo i higiena pracy (OHSAS 18000), Zarządzanie ryzykiem (ISO 31000), Bezpieczeństwo informacji zarządzanie (ISO 27000) itp. Każde laboratorium kryminalistyczne musi być zabezpieczone przed zagrożeniami zewnętrznymi i środowiskowymi takimi jak: pożar, powódź, systemy tworzenia kopii zapasowych itp. oraz bezpieczne przechowywanie materiału dowodowego na miejscu w celu jedynie przechowywania materiału dowodowego. Łańcuch dowodowy wymaga przestrzegania solidnych procedur zarządzania dowodami. Wszystko to i wiele innych wymaga, aby wszyscy pracownicy byli regularnie szkoleni w zakresie świadomości bezpieczeństwa informacji w laboratoriach kryminalistycznych, specjalistycznego sprzętu i oprogramowania, zarządzania ryzykiem i wielu innych. Nie jest tajemnicą, że utworzenie laboratoriów kryminalistycznych pochłania duże zasoby i wymaga różnorodnych, drogich narzędzi potrzebnych do zwalczania różnych zagrożeń i różnych platform/systemów.

CYFROWE NARZĘDZIA I PODEJŚCIA DO ZABEZPIECZEŃ SĄDOWYCH

Koncepcja przeciwdziałania kryminalistyce jest tak stara jak tradycyjna kryminalistyka komputerowa. Osoba dokonująca czynu karalnego wykorzystuje wszelkie możliwe sposoby, aby pozbyć się dowodów związanych z czynem zabronionym. Tradycyjna kryminalistyka może obejmować szereg środków antykryminalistycznych, które zaczynają się od poziomu trywialnego (np. wycieranie odcisków palców z broni) i kończą się na poziomie, na którym nasza fantazja może spotkać się z realizacją idei antykryminalistycznej (np. zmiana DNA pozostawionego w przestępstwo). W cyfrowej antykryminalistyce obowiązują te same zasady, z tą różnicą, że są one dość nowe i wymagają niewielkiej liczby badań i rozwoju . Istnieje wiele technik stosowanych w medycynie sądowej. Techniki te niekoniecznie są zaprojektowane z myślą o wymiarze antykryminalistycznym. Na przykład osłony folderów zostały zaprojektowane przede wszystkim w celu zapewnienia pewnego poziomu bezpieczeństwa i prywatności, ale można ich używać jako narzędzia zapobiegającego kryminalistyce, ponieważ mogą ukrywać dane. Pozostałe to:

• Wymazywanie nośników cyfrowych: Prawidłowe wyczyszczenie nośników zawierających dowody cyfrowe spowoduje po prostu ich zniknięcie.

• Steganografia: ktoś może użyć steganografii, aby ukryć plik w innym pliku i uniemożliwić śledczemu skorzystanie z dowodów, ponieważ ten ostatni może nie znaleźć sposobu na ich wyodrębnienie.

• Wycieraczki prywatności: są to narzędzia mające na celu usunięcie wszelkich śladów prywatności z systemów operacyjnych, aplikacji lub obu. W przypadku prawidłowego użycia badacz może nie znaleźć żadnych dowodów w mediach cyfrowych.

• Rootkity: Rootkity mogą osłabić działanie jądra systemu operacyjnego, a nawet reagować na procesy analizy kryminalistycznej, przejmując kontrolę nad sposobem, w jaki system operacyjny wykorzystuje takie obszary, jak zarządzanie procesami lub zarządzanie pamięcią w celu wyodrębnienia dowodów.

• MĄDRY. Ochrona przed kryminalistyką: osoba atakująca może wykorzystać tego rodzaju technologię do podejrzenia, czy dysk twardy został wyjęty w celu przeprowadzenia procesu duplikacji w celach kryminalistycznych.

• Ataki homograficzne: taki atak może wprowadzić badacza w błąd, ponieważ niektóre litery wyglądające podobnie do ludzkiego oka można zastąpić innymi w taki sposób, aby złośliwy plik wyglądał na legalny.

• Ataki polegające na modyfikacji podpisu pliku: ktoś może celowo zmienić podpis pliku, aby wyglądał inaczej.

• Szyfrowanie: Można to zastosować niemal na każdym etapie przeciwdziałania kryminalistyce, aby zaciemnić i uczynić dowody nieczytelnymi i bezużytecznymi.

• Metadata Anti-Forensics: Informacje o danych (metadane) można zmieniać w celu ukrycia działań użytkownika.

• Slack Space Anti-Forensics: Ktoś może ukryć złośliwe oprogramowanie w obszarach, których system operacyjny może nie używać, np. w wolnej przestrzeni, ponieważ mogą one zostać uznane za zarezerwowane lub puste.

• Funkcje bezpiecznego szyfrowania (MD4, MD5 itp.) Generowanie kolizji: Ktoś może zmodyfikować plik, a następnie użyć oprogramowania Anti-Forensic, aby plik ten miał tę samą wartość MD4 lub MD5 jak przed modyfikacją, omijając w ten sposób kryminalistyczną kontrolę integralności.

• Ochrona pamięci cyfrowej: istnieją programy, które potrafią ukryć procesy lub inne dowody z pamięci.

• Dowody wprowadzające w błąd: Ktoś może pozostawić dowód w sposób wprowadzający w błąd dochodzenie.

• Packery/Bindery: Ktoś może użyć takiego programu w celu przekształcenia pliku poprzez zmianę jego struktury, w ten sposób może ominąć mechanizmy bezpieczeństwa, które wyszukują wzorce złośliwego zachowania wewnątrz plików.

• Luki/exploity w narzędziach kryminalistycznych: Dostępne są już implementacje pokazujące, że niektóre z obecnych narzędzi kryminalistycznych można ominąć lub wykorzystać.

• Marnowanie zasobów: Celowe pozostawienie śladów w dużej sieci, aby śledczy marnowali cenne zasoby i czas.

• Wykrywanie kryminalistyczne: Ktoś może zainstalować mechanizm uruchamiający się po każdej obecności związanej z kryminalistyką.

• Działania anonimowe: obejmuje każde działanie, które może wykonać fałszywa lub nieznana tożsamość. W rezultacie badacz nie może wyśledzić szkodliwych działań.

• Ochrona przed kryminalistyką w urządzeniach z możliwością flashowania: ktoś może wykorzystać urządzenia, które można flashować (takie jak karty PCI lub BIOS) i zainstalować w nich złośliwy kod, dzięki czemu mogą pozostać niezauważone.

Z punktu widzenia kryminalistyki anonimowość można uznać za główne podejście antykryminalistyczne. Na przykład poniżej znajdują się najpopularniejsze bezpłatne anonimowe serwery proxy sieci Web :

• Proxify: ten internetowy serwer proxy obsługuje szyfrowanie za pośrednictwem protokołu Secure Socket Layer (SSL), protokołów sieciowych HTTPS i ukrywa adres IP oraz pliki cookie filtrujące pliki cookie.

• Anonimowy: istnieje od wielu lat i obsługuje serwery proxy sieci Web, poczty e-mail i Usenetu (wiadomości).

• Anonimizator: to najbardziej znana nazwa w anonimowych internetowych usługach proxy.

• Ninja Cloak: na stronie głównej możesz wstawić adres URL witryny, którą chcesz odwiedzić. Ten internetowy serwer proxy korzysta z CGI.

Obecnie sieci Wi-Fi są szeroko stosowane; dlatego też złośliwym użytkownikom sieci bardzo łatwo byłoby ukryć swoją prawdziwą tożsamość poprzez losowe wchodzenie na te sieci bezprzewodowe w celu przeprowadzenia ataków. Choć teoretycznie specjalista medycyny sądowej powinien monitorować wszystko, co znajduje się wokół podejrzanego, w rzeczywistości reakcja po zdarzeniu może mieć dość dramatyczny skutek. Może to wynikać z: nieznajomości logów aktywności sieci, barier prawnych pomiędzy punktem dostępu a przejęciem do celów kryminalistycznych, niechętnych do współpracy dostawców usług internetowych itp. Proces kryminalistyczny powinien zostać wzbogacony o mechanizmy bezpieczeństwa, które umożliwiłyby reakcję po zdarzeniu w czasie rzeczywistym. Narzędzia do pozyskiwania danych w czasie rzeczywistym powinny umożliwiać przechwytywanie aktywności wszystkich punktów bezprzewodowych w odpowiedniej odległości. Antykryminalistyka to rzeczywistość, która towarzyszy każdemu poważnemu przestępstwu i obejmuje taktykę „bezpiecznego hakowania" oraz utrzymuje stopień zaawansowania przestępstwa na wysokim poziomie. Badacze zajmujący się kryminalistyką komputerową wraz z twórcami oprogramowania kryminalistycznego powinni zacząć zwracać większą uwagę na narzędzia i podejścia zapobiegające kryminalistyce. Jeśli weźmiemy pod uwagę kryminalistykę komputerową jako działania polegające na gromadzeniu, zabezpieczaniu, identyfikacji i prezentacji dowodów, antykryminalistyka może wpływać na pierwsze trzy etapy. Ponieważ z punktu widzenia zarządzania projektem etapy te można scharakteryzować jako „od początku do końca", niepowodzenie jednego z nich może zakończyć się niepowodzeniem całej partii. Zatem istnieje duży wpływ antykryminalistyki na dochodzenia z zakresu medycyny sądowej. Oficjalnie nie ma czegoś takiego jak dochodzenia antykryminalistyczne, ponieważ przeciwdziałanie kryminalistyce nadal stanowi część umiejętności śledczego.

Główne trudności z jakimi borykają się funkcjonariusze organów ścigania w walce z cyberprzestępczością

Jest oczywiste, że cyberprzestępczość nie jest już w powijakach. Dla przestępczego przedsiębiorcy jest to „wielki biznes", w którym można zarobić potencjalnie dużo pieniędzy przy minimalnym ryzyku. Jednocześnie główne obszary, które uznano za czynniki przyczyniające się do uchybień funkcjonariuszy organów ścigania, są następujące:

• Brak aktualnych wytycznych

• Brak odpowiedniego szkolenia

• Brak funduszy

Organy ścigania Wielkiej Brytanii nie mogą prowadzić dochodzeń we wszystkich zarzucanych przestępstwach, co w związku z tym rodzi pytanie, w jaki sposób podejmowane są decyzje oraz w jakich sprawach należy prowadzić dochodzenie, a w jakich nie, ze względu na skalę i międzynarodowy charakter tych przestępstw. W jakim stopniu interes publiczny jest brany pod uwagę i czy jest to inny sposób radzenia sobie z przestępczością elektroniczną, niezależnie od tego, jak nieskuteczny i zniechęcający się wydaje? Z punktu widzenia organów ścigania zadanie zwalczania cyberprzestępczości jest trudne. Chociaż przestępczość nie ma znaczenia, czy jest duża, czy mała, w każdym przypadku należy podjąć decyzję, czy prowadzenie śledztwa i ściganie leży w interesie publicznym. W kwietniu 2007 roku podjęto decyzję, że wszelkie oszustwa związane z kartami kredytowymi należy zgłaszać bankom, a nie bezpośrednio policji. Banki mogą następnie zdecydować, które z nich skierować do policji w celu przeprowadzenia dochodzenia. Uznaje się, że nie we wszystkich sprawach będą wystarczające dowody, a przy ograniczonych zasobach dostępnych organom ścigania zapewnia to alokację zasobów tam, gdzie są one najbardziej potrzebne (Wytyczne ACPO, 2009). Nie jest to postrzegane jako bardzo dobra decyzja, szczególnie przez polityków, a jednym z powodów podawanych w tej sprawie jest to, że uniemożliwia ona uzyskanie dokładnych statystyk dotyczących przestępczości elektronicznej. Rzeczywiście nigdy nie było to możliwe ze względu na fakt, że nie wszystkie przestępstwa elektroniczne są zgłaszane. nie jest już wystarczające, aby polegać na osobach fizycznych, ponieważ rządy są właścicielami i kontrolują ogromne bazy danych zawierające wrażliwe informacje, zarówno prywatne dla poszczególnych osób, jak i ogólnie istotne dla bezpieczeństwa narodowego. Zrozumienie i zarządzanie procesem informatyki śledczej staje się koniecznością. Niektóre badania (EURIM-IPPR, 2004; Taal, 2007) sformułowały zbiór zasad i zasugerowały w tym celu zaawansowaną metodologię. Wszystkie procedury i wytyczne dotyczące gromadzenia i postępowania z dowodami komputerowymi opierają się na wytycznych Stowarzyszenia Komendantów Policji (ACPO); wiele z nich postępuje zgodnie z Wytycznymi ACPO, także w sektorze prywatnym. ACPO to niezależny, profesjonalnie kierowany organ strategiczny, który kieruje i koordynuje kierunek i rozwój policji w Anglii, Walii i Irlandii Północnej. Niniejsze wytyczne opracowano, aby pomóc organom ścigania w postępowaniu z dowodami komputerowymi (Wytyczne ACPO, 2009). Przyjęło się to w formie czterech następujących zasad:

Zasada 1: Żadne działania podejmowane przez organy ścigania lub ich agentów nie powinny zmieniać danych przechowywanych na komputerze lub nośniku danych, na których można później polegać w sądzie.

Zasada 2: W wyjątkowych okolicznościach, gdy dana osoba uzna za konieczne uzyskanie dostępu do oryginalnych danych przechowywanych na komputerze lub na nośniku pamięci, osoba ta musi posiadać do tego kompetencje i być w stanie przedstawić dowody wyjaśniające znaczenie i konsekwencje swoich działań.

Zasada 3: Należy utworzyć i zachować ścieżkę audytu lub inny zapis wszystkich procesów stosowanych w przypadku elektronicznego materiału dowodowego. Niezależna strona trzecia powinna być w stanie zbadać te procesy i osiągnąć ten sam wynik.

Zasada 4: Osoba odpowiedzialna za dochodzenie (urzędnik prowadzący sprawę) ponosi ogólną odpowiedzialność za zapewnienie przestrzegania prawa i niniejszych zasad.

W sektorze prywatnym wytyczne są zwykle włączane do ich wewnętrznych procedur, ponieważ większość firm zajmujących się kryminalistyką komputerową w sektorze prywatnym zajmuje się pracami obronnymi i sprawami cywilnymi, gdzie wytyczne nie zawsze mają zastosowanie. Tylko nieliczni mogą mieć umowy z Metropolitan Police, Scotland Yardem i innymi organami ścigania, w takim przypadku należy przestrzegać procedur ich, a nie sektora prywatnego. Z powyższego jasno

wynika, że wytyczne są konieczne, lecz bez skutecznego stosowania wytycznych konieczne jest odpowiednie przeszkolenie i zrozumienie wytycznych. Większość funkcjonariuszy organów ścigania znalazła się w tym obszarze dość niechętnie ze względu na duże zapotrzebowanie na walkę z przestępczością elektroniczną.

ZAPEWNIENIE EDUKACYJNE DO STUDIÓW INFORMATYKI ŚLEDCZEJ

Informatyka śledcza nie jest już dziedziną nową, jak niektórzy chcieliby wierzyć, i wiele pozostaje do zrobienia, aby przeszkolić i zachęcić nowych uczestników do pracy w tej dziedzinie, a także ujednolicić umiejętności i doświadczenie zdobyte przez osoby już pracujące w tej dziedzinie. Konieczność szkolenia nie tylko od strony technicznej, ale także prawnej, została w pełni dostrzeżona przez rząd, firmy szkoleniowe i uniwersytety, a większość uniwersytetów oferuje obecnie kursy specjalnie dostosowane do funkcjonariuszy organów ścigania, jednak większość pracowników organów ścigania decyduje się na szkolenia jedynie jako plan awaryjny na okres po przejściu na emeryturę. Osoby rozpoczynające pracę w tym zawodzie będą musiały zrozumieć znaczenie kwalifikacji akademickich, zwłaszcza jeśli nie mają żadnego doświadczenia w tej dziedzinie. Informatyka śledcza nie jest już zawodem, w którym wystarczające jest przeszkolenie w miejscu pracy w celu zdobycia doświadczenia. W przypadku większości innych zawodów wymagane jest posiadanie wyższego wykształcenia, zanim będzie można kontynuować kształcenie w swoim zawodzie, np. nauczyciele, prawnicy, kryminaliści i lekarze itp. To samo powinno dotyczyć informatyki śledczej, ponieważ praca, którą wykonujemy, jest tak samo ważna jak praca w zawodzie innych dziedzinach i niezależnie od tego, czy jest ona pozytywna, czy negatywna, ma wpływ na życie ludzi. Liczne uniwersytety w kraju i za granicą oferują kursy z zakresu informatyki śledczej i bezpieczeństwa informacji na poziomie magisterskim i podyplomowym, które pomogą osobom biorącym udział w tych kursach zdobyć dobre podstawy informatyki, lepsze zrozumienie teorii informatyki śledczej, a przede wszystkim pomóż im rozwinąć się, aby byli bardziej innowacyjni w opracowywaniu nowych, uzasadnionych kryminalistycznie sposobów zwalczania przestępczości elektronicznej i „myślą nieszablonowo". Nadszedł czas, aby rząd aktywnie współpracował z uniwersytetami, aby zachęcić ludzi do podejmowania tych kursów, zwłaszcza tych, którzy już pracują w terenie w sektorze publicznym. W sektorze prywatnym dyplom jest obecnie warunkiem wstępnym, podobnie jak doświadczenie, ponieważ coraz trudniej jest twierdzić, że jest się ekspertem w dziedzinie informatyki śledczej i biegłym sądowym. Dawno minęły czasy, gdy akceptowane były badania kryminalistyczne typu „zrób to sam". Prowadzi nas to do kolejnego obszaru, do którego wielu ekspertów w dziedzinie informatyki śledczej podchodzi z rezerwą, a mianowicie do idei akredytacji. Jest to obszar, w którym bardzo trudno podjąć decyzję. Większość zgadza się i uznaje, że należy powołać zarząd, ale nie ma zgody co do tego, kto powinien nim kierować. Niektórzy sugerują, że powinny nim kierować uniwersytety, rząd, ich koledzy lub wspólnie uniwersytety, rząd i przedsiębiorstwa. Jeżeli jest to uczelnia, obawa polega na tym, że osoby, które przez wiele lat pracowały w danej dziedzinie bez kwalifikacji akademickich, mogą odkryć, że aby zostać uznanym za eksperta w danej dziedzinie i uzyskać pełną akredytację, konieczne może być dodatkowo uzyskanie uznawanych kwalifikacji akademickich do ich doświadczeń, czemu większość jest przeciwna. Jeśli będzie on kierowany przez rząd, bez ustalonych standardów sytuacja nie będzie się różnić od tej, którą mamy obecnie. W nadaniu mu kierunku będą także zaangażowane osoby pracujące w danym zawodzie, przy czym nadal wątpliwe jest, czy osoby te będą w stanie zdecydować, jaką formę akredytacji należy zastosować. To prowadzi nas do ostatniej opcji, czyli wspólnego partnerstwa z rządem, uniwersytetami i przedsiębiorstwami. Jest to najbardziej wykonalna opcja, ale uzyskanie wiarygodnej akredytacji, która będzie akceptowana przez wszystkich, będzie wymagało wiele wspólnego wysiłku. Kiedy w marcu 2007 roku w gazecie Guardian ukazał się artykuł napisany przez Petera Warrena, incydent ten wzbudził ogromne zaniepokojenie specjalistów. „W zeszłym miesiącu nastąpił upadek Gene'a Morrisona". Oszust, który udawał kryminalistykę i składał zeznania w ponad

700 sprawach policyjnych, niektóre z nich dotyczyły gwałtu i jazdy pod wpływem alkoholu, 48-letni Morrison z Hyde w stanie Tameside został uznany winnym 22 zarzutów krzywoprzysięstwa w sądzie koronnym Minshull Street w Manchesterze i skazany na 5 lat więzienia. Jego twierdzenia, że jest specjalistą medycyny sądowej, były fałszywe, a posiadane przez niego tytuły licencjackie i doktoranckie zostały w rzeczywistości zakupione na uniwersytecie, który istniał wyłącznie w Internecie. Jedno jest pewne: posiadanie akredytacji w formie akredytacji zmusi rząd, naukowców, badaczy i osoby pracujące w dziedzinie informatyki śledczej do ustanowienia bardziej odpowiednich standardów i kontroli dla osób zajmujących się, analizujących i badających dowody komputerowe.

METODOLOGIA CFM

CFM składa się z czterech faz, a mianowicie identyfikacji, nabycia, zachowania i zgłoszenia:

1. Zidentyfikuj: Źródło dowodów cyfrowych.

2. Uzyskaj: Wykonanie zdjęcia nośnika w stanie, w jakim został znaleziony.

3. Zachowaj: łańcuch dostaw oraz integralność samych danych, upewniając się, że żadne informacje nie zostały dodane ani zmienione.

4. Raport: Aby zgłosić wszystkie ustalenia i zastosowane procesy.

Osoby dokonujące powyższych czynności muszą przestrzegać standardowych zasad dowodowych, tj. Ustawy o dowodach policyjnych i karnych (PACE) z 1984 r. w sprawach karnych, które są dopuszczalne przed sądem. Obecne kodeksy PACE Ministerstwa Spraw Wewnętrznych weszły w życie 27 października 2013 r. (Ustawa o policji i sprawach karnych, 1984). Etap 4 wymaga bardziej szczegółowego rozłożenia na metody niezbędne do analizy i klasyfikacji danych do wykorzystania jako dowód i zapis historyczny. W dziedzinie informatyki śledczej jest jeszcze wiele do zrobienia, tj. ujednolicenie procedur itp. Dziedzina ta sama w sobie obejmuje różne gałęzie informatyki śledczej, na przykład kryminalistykę Internetu, kryminalistykę sieci i kryminalistykę telefonów komórkowych, żeby wymienić tylko kilka . Indywidualne wytyczne dla tych branż umożliwią naukowcom zapewnienie jakości zarówno procesu, jak i gromadzonych danych. Ważne jest również rozszerzenie CFM o piątą fazę, czyli Przegląd i Poprawa w świetle danych empirycznych, które można klasyfikować, organizować i eksplorować w celu maksymalizacji efektywności procesów.

WNIOSKI

Przy tym wszystkim najważniejszą rzeczą, o której ludzie zapominają i o której wszyscy zapominają, jest to, że w tej dziedzinie praktyczne doświadczenie i umiejętności teoretyczne, które zdobywasz w instytutach akademickich, idą ręka w rękę. Nie możesz nazywać siebie ekspertem, jeśli masz całe doświadczenie świata i brakuje Ci podstawowej wiedzy z zakresu informatyki. Organy ścigania, rząd i sektor prywatny wyrażają obawy związane z brakiem konsensusu w sprawie ujednoliconego podejścia do kursów szkoleniowych oraz brakiem funduszy na badania. Prawnicy obrony nie byli na tyle pewni siebie, aby kwestionować ustalenia z zakresu informatyki śledczej, brak zrozumienia i podstawowej wiedzy na temat komputerów oraz, w końcu, korzyści płynące z szkolenia ekspertów z zakresu informatyki śledczej podczas obrony osób oskarżonych o przestępstwa z użyciem komputerów. W miarę jak obrońcy nabiorą jeszcze większej pewności w kwestionowaniu ustaleń informatyki śledczej, wskaźnik skuteczności ścigania będzie inny, a ci z nas, którzy zajmują się informatyką śledczą, zaczynają dostrzegać zmiany zarówno w sprawach cywilnych, takich jak czyn niedozwolony, naruszenie umów , zniesławienie, spory pracownicze itp., do spraw karnych, kradzieży, szkód karnych, przestępstw związanych z narkotykami i przestępstw związanych z prawami autorskimi i kradzieżą własności intelektualnej. Kluczową kwestią jest tutaj brak zrozumienia i podstawowej wiedzy na temat

komputerów, a wreszcie korzyści płynące z wyszkolenia biegłych z zakresu informatyki śledczej podczas obrony osób oskarżonych o przestępstwa z udziałem komputerów. Rozwój jednego lub większej liczby głównych multidyscyplinarnych ośrodków badawczych, na wzór Centrum Badań nad Technologią Informatyczną na rzecz Społeczeństwa (CITRIS), jest niezbędny, aby przyciągnąć prywatne fundusze i zgromadzić ekspertów z różnych wydziałów akademickich i przemysłu w bardziej zintegrowany, multidyscyplinarny wysiłek badawczy. Zaleca się, aby Rady ds. Badań Naukowych przejęły wiodącą rolę w inicjowaniu rozmów z rządem, uniwersytetami i przemysłem w celu szybkiego utworzenia początkowego centrum w Wielkiej Brytanii.

Zrozumienie świadomości sytuacyjnej w cyberprzestępczości: studia przypadków

WSTĘP

Jak już wspomniano w rozdziałach tej książki, cyberprzestępczość i cyberterroryzm stanowią coraz ważniejsze problemy nie tylko dla decydentów, ale także przedsiębiorstw i obywateli. W wielu krajach społeczeństwa zaczęły korzystać z cyberprzestrzeni do prowadzenia działalności gospodarczej, konsumpcji produktów i usług lub wymiany informacji z innymi osobami w Internecie. W latach 2000–2012 wzrost liczby użytkowników Internetu szacuje się na 393,4% (World Internet Usage and Population Statistics, 2012). Jednak Khoo Boon Hui, były prezydent Interpolu, ogłosił w maju 2012 r., że z powodu cyberprzestępczości na całym świecie straty wynoszą 750 miliardów euro rocznie. Cyberprzestępczość nie tylko kosztuje, ale także zagraża infrastrukturze krytycznej, obywatelom i przedsiębiorstwom, a także bezpieczeństwu, tożsamości i prywatności. W tym rozdziale pokazano, że lepsze zrozumienie motywacji i intencji stojących za cyberprzestępczością/cyberterroryzmem może prowadzić do lepszego zrozumienia sytuacji. Ponadto zapewnia agencjom pierwszej linii (LEA) możliwość rozpoznawania oraz reagować na sytuacje związane z cyberprzestępczością i cyberterroryzmem poprzez zaprojektowanie modelu taksonomii. Zrozumienie sytuacyjne i przypisanie ataków cyberprzestępczości to jeden z kluczowych problemów zdefiniowanych przez Departament Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (2009) na potrzeby badań nad bezpieczeństwem cybernetycznym. W szczególności zrozumienie sytuacji ma kluczowe znaczenie dla kilku powodów:

• Większe bezpieczeństwo systemów

• Ulepszona obrona przed przyszłymi atakami

• Atrybucja ataku

• Identyfikacja potencjalnych zagrożeń

• Lepsza świadomość sytuacyjna

W tym rozdziale proponuje się, aby wnioski wyciągnięte z rzeczywistych scenariuszy można wykorzystać do stworzenia repozytorium wiedzy, które może pomóc w lepszym zrozumieniu cyberprzestępczości i zapewnieniu jej ram wiedzy. Warunkiem wstępnym powstania repozytorium wiedzy jest opracowanie taksonomii, która pomoże w lepszym zrozumieniu sytuacji leżącej u podstaw cyberprzestępstw. Opierając się na perspektywie socjologicznej, w tym rozdziale rozważono pięć odpowiednich przypadków cyberprzestępczości i wykorzystano metodę klasyfikacji taksonomicznej, aby pogrupować je w oparciu o postrzeganą intencję/motywację ataku. W tym rozdziale wykorzystano także koncepcję zarządzania wiedzą Akhgara (1999) – gdzie wiedza jest budowana na kontinuum danych, które najpierw przekształcają się w informacje poprzez interpretację kontekstu przy użyciu inteligencji dziedzinowej, a następnie informacje w wiedzę (która jest abstrakcją proces uczenia się). Aby jeszcze bardziej wesprzeć potrzebę opracowania taksonomii sytuacyjnego zrozumienia

cyberprzestępczości, Departament Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (2009) podkreśla potrzebę „wiedzy warstwy ludzkiej", która składa się z danych znajdujących się poza sieciami i hostami (s. 68). Mając to na uwadze, opracowano taksonomię. Plan działania Departamentu Bezpieczeństwa Wewnętrznego dotyczący raportu z badań nad bezpieczeństwem cybernetycznym również podkreśla potrzebę analizy: powtarzających się wzorców interakcji, które pojawiają się na przestrzeni miesięcy lub lat, oraz nieoczekiwanych powiązań między firmami i osobami. Te uzyskane ilości powinny same zostać zarchiwizowane lub, alternatywnie, umożliwić łatwe odtworzenie (Departament Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych, 2009, s. 70). Podkreślając jednocześnie, że „zrozumienie sytuacyjne wymaga gromadzenia lub wyprowadzania istotnych informacji dane dotyczące zróżnicowanego zestawu atrybutów" (Departament Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych, 2009). Jak zauważono w tej książce, cyberprzestępczość stała się codziennym problemem użytkowników Internetu. W 2012 roku w USA Centrum skarg dotyczących przestępstw internetowych (IC3), które współpracuje z FBI, otrzymało 289 874 skarg konsumentów, co spowodowało łączną stratę ponad 500 milionów dolarów. Bez wątpienia ofiarami przestępstw związanych z cyberprzestępczością są na całym świecie nie tylko firmy, ale także osoby fizyczne. Istnieje wiele motywacji do przeprowadzania cyberprzestępczości: moralna, finansowa, polityczna, wyzysku, samorealizacji i promocji, które opisano poniżej. Jednak przed przedstawieniem studiów przypadku należy zdefiniować cyberprzestępczość. Na potrzeby tej pracy powstało Stowarzyszenie Komendantów Policji e-Crime . Zastosowana zostanie definicja strategii dotycząca e-przestępczości (2012): „Wykorzystanie komputerów połączonych w sieć lub technologii internetowej w celu popełnienia przestępstwa lub ułatwienia jego popełnienia". Według ACPO (2012):

Internet umożliwia przestępcom wybieranie potencjalnych ofiar z dowolnego miejsca na świecie i umożliwia stosunkowo łatwe podejmowanie prób masowej wiktymizacji… Internet zapewnia przestępcy wysoki stopień postrzeganej anonimowości, a także stwarza problemy jurysdykcyjne, które mogą utrudniać szybkie ściganie i ściganie przestępców. Ponadto nie ma jeszcze jasnego rozróżnienia między kwestiami, które najlepiej rozwiązać poprzez lepsze stanowienie prawa, a tymi, które wymagają działań organów ścigania.

To stwierdzenie ma szczególne zastosowanie do studiów przypadku przedstawionych poniżej. Sam fakt, że włamania mają miejsce w różnych strefach czasowych i jurysdykcjach, oznacza, że hakerom, haktywistom, cyberprzestępcom itp. łatwiej jest kontynuować ataki. Pomaga także podkreślić potrzebę jasnych strategii komunikacyjnych i informacji wywiadowczych na temat ataków, które powinny być udostępniane nie tylko pomiędzy dotkniętymi krajami/rządami, ale także sieciami na całym świecie, aby wzmocnić sieci bezpieczeństwa przed przyszłymi atakami i zagrożeniami.

Ważne jest również, aby wyjaśnić, że w następnym rozdziale przedstawiono w zarysie niektóre działania w cyberprzestrzeni – bez uprzedzeń. Autorzy nie popierają ani nie sprzeciwiają się działaniom podsumowanym poniżej. Zarysowane przypadki pokazują zróżnicowanie motywacji cyberprzestępczości i terrorystycznego wykorzystania Internetu, a także pokazują potencjalne trudności w taksonomizacji motywacji stojących za atakami. Należy również podkreślić różnice w jurysdykcji na całym świecie w odniesieniu do definicji cyberprzestępczości (patrz rozdziały 1 i 3). Na przykład istnieje cienka granica pomiędzy tajnymi operacjami a atakami terrorystycznymi, w zależności od tego, gdzie na świecie ma miejsce dana czynność. Dlatego też niniejszy rozdział nie ma na celu poruszania zagadnień prawnych i legislacyjnych leżących u podstaw tego działania. Wykorzystane przypadki podsumowano poprzez przedstawienie publicznie dostępnych informacji na ich temat. Następnie następuje przegląd strategicznych reakcji Wielkiej Brytanii, USA i UE, a następnie omawiana jest ocena zagrożenia.

Taksonomiczna klasyfikacja cyberprzestępczości/cyberterroryzmu

Istnieje wiele taksonomii opracowanych w odniesieniu do cyberprzestępczości i aktywności. Inne taksonomie cyberprzestępczości koncentrują się na charakterystyce ataków , podczas gdy taksonomia Howarda i Longstaffa (1998) uwzględnia motywacje i cele i składa się z pięciu etapów procesu. Jednak kluczowym problemem w obszarze bezpieczeństwa cybernetycznego jest brak uzgodnionej terminologii pomiędzy różnymi organizacjami, dyscyplinami i podejściami badawczymi oraz zainteresowanymi stronami. Dlatego taksonomia ta próbuje pokonać bariery językowe za pomocą języka nietechnicznego. Nabierający podejścia skoncentrowanego na człowieku, taksonomia ta skupia się na sytuacyjnym zrozumieniu cyberprzestępczości i pomaga w praktycznym wdrażaniu środków zaradczych poprzez skupienie się na intencjach (i okolicznościach) związanych z cyberprzestępczością. Proponowana poniżej taksonomia odnosi się do postrzeganych motywacji/zamiarów cyberprzestępczości i ataków, a zatem nie skupia się na technicznych aspektach cyberprzestępczości. Należy opracować taksonomię nie tylko w formie listy słów, ale także w celu odzwierciedlenia atrybutów (i ich wzajemnych powiązań), które są kluczowe dla wszystkich docelowych społeczności użytkowników – na przykład organów ścigania, zwłaszcza funkcjonariuszy dochodzeniowych. Chociaż jest to punkt wyjścia do procesu kategoryzacji, istnieje możliwość rozwoju w miarę zmieniania się i rozwoju wymagań w zakresie bezpieczeństwa cybernetycznego. Obecnie nie jest on wyczerpujący, a ograniczeniem może być brak miejsca na szczegóły techniczne, jednak w jego obecnej formie pomaga ustalić postrzegane motywacje stojące za cyberatakami, co z kolei zapewnia podstawę do zrozumienia sytuacji

Motivations/ intent	Primary	Secondary	Tertiary	Context	Major website has gone down—affected users include public
Financial				Who	British electronic army
Political	✓			What	DDoS attacks
Moral		✓		Where	Website/card system failure
Self-actualization			✓	When	2 pm-4 pm Thursday 21st
Exploitation				How	No technical detail currently known
Promotional		✓		Other	Second attack of its type in 2 days

Do użytku operacyjnego oraz w celu utworzenia repozytorium – powyższą siatkę można wykorzystać w przypadku każdego incydentu cyberprzestępczego. Dołączono próbny przykład, aby pokazać, jak można go wykorzystać. Pierwsza część siatki udostępnia system pól wyboru, w którym można zaznaczyć wiele motywacji. Na przykład może zostać podjęta decyzja, że sprawa ma przede wszystkim motywację polityczną, ale ma motywacje moralne i promocyjne (patrz przykład powyżej). Różni funkcjonariusze dochodzeniowi mogą mieć różne opinie lub dowody na temat motywacji – nie ma ograniczeń co do liczby pól, które można zaznaczyć – zwłaszcza biorąc pod uwagę, że niektóre sprawy mogą mieć złożony charakter – chociaż zaleca się, aby decyzje były podejmowane co do głównych, drugorzędnych i motywacje trzeciorzędne, zamiast skupiać je w jednej kategorii. Możliwe, że nie istnieją motywacje drugorzędne lub trzeciorzędne – w takich przypadkach pola można pozostawić puste. Informacje dotyczące sprawy dotyczącej cyberprzestępczości można umieścić po prawej stronie tabeli i mogą one być tak szczegółowe, jak to konieczne. Pola „kontekst” i „inne” pozwalają na umieszczenie wszelkich notatek terenowych lub ważnych informacji związanych ze sprawą. Pole „kto”

odnosi się do potencjalnych podejrzanych i może obejmować także potencjalne ofiary. Jeśli informacje nie są znane, pola te również można pozostawić puste. Ten projekt został celowo stworzony tak, aby był elastyczny, biorąc pod uwagę, że każdy przypadek będzie się składał z różnych cech. Motywy finansowe cyberprzestępczości mogą mieć charakter oszukańczy i czerpać korzyści finansowe, jednak motywy finansowe mogą również wiązać się z zakłóceniami w systemach finansowych. Motywy polityczne wiążą się ze wsparciem lub przeciwdziałaniem politykom lub działaniom rządu i mogą obejmować sponsorowane przez państwo ataki, szpiegostwo i propagandę. Motywy moralne mogą wiązać się z walką o wolność, prawa i etykę lub przeciwko wyzyskowi i uciskowi. Systemy religijne mogą należeć do tej kategorii i są dwojakie: ataki grup religijnych na inne systemy/przekonania religijne; ataki na grupy religijne przeciwko ich systemom przekonań/wyzysk/religię jako ucisk. Moralne motywacje cyberataków mogą mieć złożony charakter — ta taksonomia pozwala na ogólną kategoryzację, a ograniczeniem jest to, że może być postrzegana jako zbyt uproszczona. Samorealizacja odnosi się do osób lub grup, które przeprowadzają ataki z ciekawości – mogą testować własną wiedzę i umiejętności lub testować systemy bezpieczeństwa – ponownie w celu zdobycia wiedzy, a nie celowego zepsucia lub zakłócenia. Mogą także hakować dla uznania lub rozgłosu. Chociaż wyzysk może być zgodny z motywacjami moralnymi, jest to odrębna kategoria związana z wyzyskiem ludzi (na przykład w przypadkach handlu ludźmi i znęcania się nad dziećmi). Do tej kategorii mogą również należeć sprawy dotyczące cyberprzemocy i/lub molestowania w Internecie. W tym rozdziale nie ma studium przypadku odnoszącego się do tej kategorii, jednakże w Rozdziale 11 omówiono kwestie związane z wykorzystywaniem dzieci. Ostatnią motywacją wymienioną w tej taksonomii jest promocja, która wiąże się z reklamą i w tej taksonomii oznacza gromadzenie świadomości za pośrednictwem mediów informacyjnych i mediów społecznościowych, a w niektórych przypadkach rozwijanie i utrzymywanie obecności w Internecie. Definicje te nie są wyczerpujące, ale dostarczają koncepcji dla operatorów korzystających z siatki do tworzenia repozytorium. W przypadkach, gdy cyberprzestępstwa miały charakter anonimowy, trudno jest sklasyfikować motywacje agenta, chyba że wydał on oświadczenie dla prasy lub publicznie przyznał się do ataku, podając powody jego przeprowadzenia. Chociaż niektórzy hakerzy otwarcie podają przyczyny ataku, należy pamiętać, że ukryte motywacje mogą również istnieć, ale nie zostaną publicznie potwierdzone. Ta taksonomia działa poprzez możliwość zamiany kategorii. Może wydawać się, że cyberatak lub przestępstwo ma motywację pierwotną, ale może też mieć motywację wtórną (która w niektórych przypadkach może być ukryta). W bardziej skomplikowanych kontekstach może istnieć wiele motywacji, w których można zastosować motywacje „trzeciorzędowe". Na przykład atak DDoS na bank może mieć przede wszystkim podłoże moralne (wbrew faktowi, że system bankowy jest skorumpowany i spowodował kryzys gospodarczy), ale motywacją drugorzędną może być rozgłos, a motywacją trzeciorzędną może być samorealizacja. Każdy przypadek należy oceniać indywidualnie i może mieć nawet wiele motywacji pierwotnych i wtórnych.

STUDIUM PRZYPADKU

Poniższe studia przypadków przedstawiają każdą z taksonomicznych motywacji prowadzenia cyberprzestępczości. Syryjska armia elektroniczna kieruje się motywacją „moralną", ale w dużym stopniu kieruje się potrzebą rozgłosu i jest powiązana z kategorią motywów politycznych. Ta grupa hakerów twierdzi, że przeprowadza ataki, aby ich głos został usłyszany. Atak Stuxnetem jest powiązany z potencjalną motywacją polityczną: zapobieżenie rozwojowi broni nuklearnej. Ataki na systemy bankowe są powiązane z motywami finansowymi i moralnymi, a także z rozgłosem. Sprawa Mafiaboya dotyczy „samorealizacji".

POLITYKA/REKLAMA/SAMOREALIZACJA: PRZYPADEK SYRYJSKIEJ ARMII ELEKTRONICZNEJ

SEA zostały oficjalnie umieszczone na liście doradczej FBI po szeregu ataków w 2011 r. FBI określa SEA jako „proreżimową grupę hakerów", która wyłoniła się podczas syryjskich protestów antyrządowych w

2011 r. (Federalne Biuro Śledcze, 2013). Z informacji dołączonych do porady wynika, że głównymi możliwościami SEA są phishing spearphishing; niszczenie sieci i przejmowanie mediów społecznościowych w celu szerzenia propagandy.

KIM ONI SĄ?

Zespół ośmiu osób – prawdopodobnie młodych Syryjczyków (z których pięciu miało własne pseudonimy, gdy można było uzyskać dostęp do ich strony internetowej) – które nie są w żaden sposób powiązane z żadną partią polityczną. Twierdzą, że utworzyli SEA w 2011 r. w odpowiedzi na zachodnie i arabskie media, które ich zdaniem stronniczo donosiły o grupach terrorystycznych, które zabijały cywilów, i opowiadają się za armią syryjską. Obecnie ugrupowanie wierzy, że chroni swoją ojczyznę i zdecydowanie wspiera reformy prezydenta Bashara-Al-Assada. Schneier (2013) spekuluje, ile faktycznie stanowi armia SEA, i sugeruje, że tak naprawdę nie wiemy zbyt wiele na temat ich wieku ani tego, czy w ogóle są Syryjczykami. Nie wiemy na pewno, w jakim stopniu grupa ta jest wspierana przez rząd syryjski, zatem możliwe jest, że SEA to grupa geopolityków-amatorów. W styczniu 2014 r. ich witryna internetowa została usunięta z Wyszukiwarki Google, a ich istniejące profile online na Twitterze, Facebooku i Instagramie zostały usunięte, mimo że 29 stycznia 2014 r. ponownie założyli konta. Prawdopodobnie będzie to coś, co będą musieli stale robić, walcząc z organizacjami na dużą skalę, takimi jak Microsoft (Hanley Frank, 2014). Strony na Facebooku i Twitterze umożliwiają grupie publiczne zgłaszanie roszczeń do ataków, ale także wyrażanie swoich poglądów politycznych. Szczególnie krytycznie odnoszą się do organizacji, które odmawiają użytkownikom prawa do prywatności.

HAKERZY POLITYCZNI CZY MORALNI?

Jest rzeczą oczywistą, że im częściej ta grupa hakuje i przejmuje odpowiedzialność za ataki hakerskie i phishingowe, tym częściej media zaczynają omawiać historie na ich temat i tym bardziej stają się one znane. Powszechnie uważa się, że nie robią oni nic nowego ani niezwykłego w odniesieniu do technicznej strony ataków (podstawowe ataki phishingowe i ataki DOS). Okazały się one jednak na tyle skuteczne, że spowodowały niedogodności dla firm takich jak Microsoft (który uważa, że istnieje możliwość naruszenia bezpieczeństwa kont ich pracowników w mediach społecznościowych — patrz rozdział 3). Z zamknięcia stron SEA w mediach społecznościowych i ich ponownego otwarcia kilka godzin później jasno wynika, że grupa ta rozumie potrzebę obecności w mediach społecznościowych, aby stanowić ciągłe i znane zagrożenie. Na swojej obecnej stronie na Facebooku podają się za organizację pozarządową (NGO) i trzy godziny po ponownym założeniu strony profilowej mieli 1600 „polubień", podczas gdy ich liczba obserwujących na Twitterze wzrosła z 10 000 w pierwszych tygodniach stycznia do 12 500. Bez wątpienia cieszą się one pewnym poparciem społecznym, chociaż bez przeprowadzenia analizy użytkowników Facebooka, którzy polubili tę stronę, oraz analizy ich obserwujących na Twitterze, trudno jest kategorycznie stwierdzić, kto ich popiera (dalsze omówienie można znaleźć w rozdziale 10). Zanim witryna SEA (www.SEA.sy) została usunięta z wyszukiwarek Google, zawierała szczegółowe informacje na temat ataków, które zainicjowali, a także szczegółowe informacje na temat powodów ich przeprowadzenia. Określili hacki mianem osiągnięć, co po raz kolejny ugruntowało argument, że aby zachować skuteczność, muszą zhakować wpływowe organizacje i zadbać o to, by były one transmitowane w mediach, aby umocnić swoją sławę, ale także zadbać o to, aby ich głos był słyszalny. bycia wysłuchanym.

METODY: PHISHING I DDoS

Media donoszą o dwóch głównych metodach stosowanych przez SEA: atakach phishingowych i DDoS. Phishing może polegać na wysyłaniu dużej liczby wiadomości e-mail zawierających wiadomość, która wydaje się pochodzić z legalnego źródła (tj. znanej firmy, takiej jak PayPal lub Twitter). Celem

wiadomości e-mail jest przekonanie potencjalnej ofiary do podania swoich danych osobowych. Niektóre e-maile mogą kierować czytelników do zewnętrznej fałszywej witryny internetowej, która wygląda autentycznie. Witryna może również zachęcać ofiarę do podania poufnych informacji (dane konta bankowego, dane identyfikacyjne, numery ubezpieczenia społecznego, hasła itp.), które następnie mogą zostać wykorzystane przez Phishera do popełnienia szeregu kolejnych oszustw. Niektóre bardziej skomplikowane kampanie phishingowe mogą zawierać szkodliwe złośliwe oprogramowanie w samej wiadomości e-mail lub na fałszywej stronie internetowej, która może bezpośrednio wyodrębnić potrzebne informacje z komputera ofiary, bez wymagania od ofiary bezpośredniego podania poufnych informacji (więcej szczegółów na temat phishingu można znaleźć w rozdziale 12). DDoS (Distributed Denial of Service) lub odmowa usługi (DoS) zwykle wiążą się z przeciążeniem systemu przez jednoczesne żądania online. Może to spowodować, że usługa stanie się niedostępna dla użytkowników. Rozproszone ataki typu „odmowa usługi" są wysyłane przez dwie lub więcej osób lub botów, natomiast ataki typu „odmowa usługi" są wysyłane przez jeden system lub osobę.

KOGO DOTYCHCZAS ZHAKOWALI?

Poniższe informacje stanowią podsumowanie informacji dostępnych w źródłach medialnych. SEA przeniknęła do mediów na całym świecie, jednak nie jest jasne, ile dokładnie ataków i kogo dotknęły. Poniżej przedstawiono kilka przykładów, które miały miejsce w latach 2013 i 2014. W sierpniu 2013 r. Schneier twierdził, że SEA zaatakowała między innymi strony internetowe „New York Timesa", Twittera, „Huffington Post", chociaż nie zrobiły tego bezpośrednio, ale poprzez australijską nazwę domeny o nazwie Melbourne IT. Jednak w styczniu 2014 r. dokonali szeregu „ataków" na następujące organizacje:

CNN

Celem SEA były konta CNN na Twitterze i Facebooku. Ogłosili atak na CNN (styczeń 2014 r.), informując na swoim Twitterze, że dziś wieczorem #SEA zdecydowała się wziąć odwet na zaciekle kłamliwych doniesieniach #CNN, których celem jest przedłużenie cierpień w Syrii… #CNN użyło swojej zwykłej formuły teraźniejszości niemożliwej do sprawdzenia informację za prawdę, przyjęcie raportu Katarczyków przeciwko Syrii… Zamiast prawdziwego dziennikarstwa, #CNN zamieniło się w głośny klakson za zniszczenie państwa syryjskiego… Strategia mediów USA polega teraz na ukrywaniu faktu, że CIA kontroluje i finansuje Al-Kaidę, obwiniając zamiast tego Syrię za jej terror #SEA… #SEA nie przestanie ścigać tych kłamców i ujawni ich i ich metody światu. Biorąc pod uwagę, że za jedną z ich głównych motywacji uważa się mobilizację polityczną, nie jest zaskakujące, że uzasadnienie ataku ze strony SEA odnosi się do rzekomego błędnego informowania CNN o tym, co dzieje się w Syrii. Zanim przywrócono kanał CNN na Twitterze, SEA wysłała pięć tweetów:

Syryjska Armia Elektroniczna była tutaj… Przestań kłamać… Wszystkie twoje raporty są fałszywe! za pośrednictwem @Official_SEA16 #SEA

Niech żyje #Syria za pośrednictwem @Official_SEA16 #SEA ow.ly/i/4nt9l

Obama Bin Laden, władca terroru, kłamie, że państwo syryjskie kontroluje Al-Kaidę

Przez 3 lata Al-Kaida niszczyła państwo syryjskie, ale oni myślą, że jesteście na tyle głupi, żeby w to uwierzyć

NIE ZAPOMNIJ: Al-Kaida to Al CIA da. Finansowane, uzbrojone i kontrolowane. (http://www.buzzfeed.com/michaelrusch/syrian-electronic-army-hacks-cnns-twitter-account)

Oczywiście treści tych tweetów nie można potwierdzić ani zaprzeczyć: są one po prostu nagrywane w celach informacyjnych. W oświadczeniu CNN poinformowano, że tweety zostały natychmiast usunięte, a dotknięte konta zabezpieczone (Shoichet, 2014).

ANGRY BIRDS

W styczniu 2014 r. witryna AngryBirds została zniszczona. Logo Angry Birds zostało zmienione na „szpiegujące ptaki" z logo NSA umieszczonym nad jednym z logo aplikacji. Uważano, że dokonał tego przyjaciel SEA. Na ich koncie na Twitterze widniała następująca informacja:

Znajomy włamał się i zniszczył witrynę @Angrybirds po tym, jak raporty potwierdziły, że szpieguje ona ludzi. Atak przeprowadził haker „Anti-NSA". Wysłał on e-mail na nasz oficjalny adres e-mail z linkiem do zaatakowanej witryny. (www.twitter com/offcial_SEA16)

Atak miał związek z rzekomym raportem NSA, z którego wynikało, że amerykańskie i brytyjskie agencje szpiegowskie (tj. GCHQ) mogą uzyskać dostęp do danych osobowych – takich jak wiek i data urodzenia – od zewnętrznych firm zajmujących się reklamą w aplikacjach mobilnych. Rovio (firma twórcza aplikacji) wydała oświadczenie, w którym stwierdziła, że nie współpracowała ani nie była w zmowie z żadnymi rządowymi agencjami szpiegowskimi na całym świecie (Rovio, 2014). Tak niewielkie uszkodzenie witryny internetowej przez źródło zewnętrzne świadczy o słabości bezpieczeństwa witryny, a jednocześnie pomaga w nagłośnieniu rzekomego naruszenia bezpieczeństwa danych osobowych jej użytkowników.

MICROSOFT (STYCZEŃ 2014)

W styczniu 2014 r. odbyło się kilka ataków SEA na firmę Microsoft. Według doniesień, dzięki taktyce phishingu, SEA uzyskała dostęp do mediów społecznościowych pracowników i kont e-mail, których dotyczyły ataki. Na Twitterze zamieścili następujący wpis z konta @MSFTnews: „Syryjska armia elektroniczna była tutaj za pośrednictwem @Official_SEA16 #sea", który został szybko usunięty. W innym tweecie napisano: „Nie używaj e-maili Microsoftu (hotmail, Outlook). Monitorują Twoje konta i sprzedają dane rządom #SEA @Official_SEA16". Według doniesień Berkman (2014) skontaktował się z SEA i otrzymał następującą odpowiedź na pytanie, dlaczego obrali za cel Microsoft:

Microsoft monitoruje konta e-mail i sprzedaje dane amerykańskiemu wywiadowi i innym rządom. Opublikujemy więcej szczegółów i dokumentów, które to potwierdzają. Microsoft nie jest naszym wrogiem, ale to, co robi, wpłynęło na SEA.

STRONY INTERNETOWE RZĄDU ARABII SAUDYJSKIEJ

Neal (2014) podaje, że SEA była również odpowiedzialna za atakowanie witryny internetowej rządu Arabii Saudyjskiej i przejęcie kontroli nad wieloma jego domenami. SEA dokonały ataku w ramach protestu przeciwko reżimowi Al Saud, który ich zdaniem posługuje się grupą terrorystyczną. Ich kanał na Twitterze po raz kolejny pozwolił im przypisać sobie zasługi i reklamować swoje wysiłki. Przy każdej z 16 zasad Arabii Saudyjskiej wymieniono indywidualność, po czym opatrzono hasztagiem: #ActAgainstSaudiArabiaTerrorism #SaudiArabia. Warto zauważyć, że ten incydent jest mniej nagłośniony w mediach niż w przypadku innych ataków na duże firmy.

OBECNOŚĆ W MEDIACH SPOŁECZNOŚCIOWYCH

Biorąc pod uwagę, że są świadomi konieczności obecności w mediach społecznościowych, członkowie SEA rozmawiali z wieloma źródłami prasowymi. Jednak w szczególności jeden z wywiadów został

opublikowany na Twitterze za pośrednictwem linku odnoszącego się do rozmowy tekstowej, którą odbyli z Matthew Keysem w grudniu 2013 r. W swojej wymianie informują, że są studentami i podkreślają, że SEA wybiera swoje cele w oparciu o stronniczość doniesień mediów – oni w szczególności odnoszą się do artykułu w Timesie, który ich zdaniem donosi tylko o jednej stronie, tj. przeciwko Basharowi Assadowi. W wywiadzie podkreślają, że ogólnie nie ufają mediom, a zwłaszcza temu, że niektóre media nie kierują się żadnymi programami, jeśli chodzi o Syrię. Uważają również, że ich tożsamość musi pozostać nieznana, w przeciwnym razie będą narażeni na groźby ze strony USA. W wywiadzie podkreślają, że robią tylko to, co robią, aby media pokazywały światu prawdę po tym, jak były świadkami ataków terrorystycznych na policję swojego kraju. Trudno jednoznacznie stwierdzić, ile z tego, co mówią w wywiadzie, to propaganda, a ile prawda. Ostatecznie SEA doradza, że chce powstrzymać wojnę czwartej generacji ze swoim krajem, ale ich kontratak jest taki, że chcą ujawnić prawdziwą rękę stojącą za terroryzmem. Kategorycznie zaprzeczają także jakimkolwiek powiązaniom z rządami Syrii, Rosji i Iranu. Pełny zapis wywiadu można znaleźć pod adresem http://thedesk.matthewkeys.net/2013/12/11/alive-conversation-with-the-syrian-electronic-army/ (Keys, 2013) (więcej szczegółów można znaleźć w Rozdziale 15 o mediach społecznościowych). Masi (2013a) twierdziła, że we wrześniu 2013 r. rozmawiała z członkiem SEA o imieniu „Richie", ale sama przyznaje, że nie ma sposobu, aby to potwierdzić. W transkrypcie powtórzono podobne główne przesłania wywiadu z kluczem z grudnia 2013 r.: „Hakowanie zwróci uwagę, opinie i dobrze przekazany komunikat niezależnie od problemu". W drugim wywiadzie z liderem SEA Masi (2013b) podkreśla możliwość, że część obecności w mediach jest prowadzona przez inne osoby, które podają się za SEA, ale nimi nie są. SEA twierdzi, że nie jest powiązana z rządem syryjskim, jednak niektóre z ich ataków były w pewnym stopniu motywowane politycznie. Na potrzeby tej taksonomii wymienione przypadki mogą przede wszystkim należeć do kategorii „moralnej" – a SEA często wydaje publiczne oświadczenia na temat powodów, dla których podejmuje swoje działania – łącząc swoje działania z przyczynami etycznymi. Jednakże fakt, że w dużym stopniu polegają one na mediach społecznościowych i roszczą sobie prawa do ataków, które mają miejsce na całym świecie, prowadzi do dodatkowej motywacji, jaką jest potencjalny rozgłos. Niektóre z ich działań można również powiązać z samorealizacją.

PRZYPADEK STUXNETA

W czerwcu 2010 r. przypuszczano, że wirus komputerowy Stuxnet został stworzony w celu ataku na irańskie obiekty nuklearne. Źródła medialne szeroko spekulują, że Stany Zjednoczone i Izrael współpracowały, aby ułatwić ten atak, chociaż żaden z krajów nigdy nie potwierdził tego oficjalnie. Jest to pierwszy przypadek publicznie znanego zamiaru prowadzenia wojny cybernetycznej. Zespół badawczy NATO w 2013 r. zgodził się, że atak Stuxneta na Iran był „aktem siły" (Schmitt, 2013). Wirus zawierał specjalne złośliwe oprogramowanie, które w szczególności monitoruje systemy przemysłowe, wyrządzając niewielkie szkody komputerom i sieciom, które nie spełniają jego wymagań konfiguracyjnych. Uważa się, że został on zaprojektowany w celu zniszczenia maszyn elektrowni jądrowej, a w rezultacie spowolnienia lub zatrzymania produkcji nisko wzbogaconego uranu. Uważa się, że celem różnych odmian wirusa było pięć irańskich organizacji, w tym obiekt nuklearny w Natanz . Specjaliści ds. bezpieczeństwa uważają, że ze względu na złożoność wdrożenia wirusa i jego wyrafinowany charakter najprawdopodobniej przeprowadzono go przy „wsparciu państwa narodowego". Źródła medialne w Wielkiej Brytanii i USA (The Guardian, BBC i The New York Times) stwierdził również, że (nienazwani) eksperci badający Stuxneta uważają, że tylko państwo narodowe byłoby w stanie go wyprodukować ze względu na złożoność kodu . Borg (2010) z United States Cyber-Consequences Unit stwierdził, że Izrael z pewnością ma możliwość stworzenia Stuxneta i nie ma wielu wad takiego ataku, ponieważ praktycznie niemożliwe byłoby udowodnienie, kto to zrobił. Zatem narzędzie takie jak Stuxnet jest oczywistą bronią Izraela. Jak dotąd Izrael nie skomentował publicznie ataku Stuxnet, ale potwierdził, że wojna cybernetyczna znajduje się obecnie na czele ich doktryny

obronnej, a jednostka wywiadu wojskowego została utworzona specjalnie w celu realizacji zarówno defensywnych, jak i ofensywnych opcji związanych z cyberprzestrzenią. Amerykańscy urzędnicy wskazali, że wirus pochodzi z zagranicy. Tak czy inaczej, charakter cyberprzestrzeni oznacza, że ustalenie, kto jest odpowiedzialny za prowadzone działania, podjęte działania i pochodzenie działań, jest trudne. Szczególnie trudno jest udowodnić, kto stoi za Stuxnetem. Chociaż wydaje się, że Stuxnet został zaprojektowany tak, aby był destrukcyjny i jest pierwszym atakiem tego rodzaju. Biorąc pod uwagę dostępne fakty na temat tego zdarzenia, najprawdopodobniej zaliczałby się on do kategorii politycznej, chociaż mógłby należeć do kategorii moralnych lub finansowych, gdyby dalsze informacje na temat ataku zostały upublicznione.

CYBERATAKI NA BANKI W SKALI GLOBALNEJ

Operacja High Roller obejmowała serię oszustw wymierzonych w system bankowy na całym świecie. Wykorzystywał wieloaspektową automatyzację do gromadzenia danych w celu napadania na konta bankowe, w tym rachunki komercyjne i instytucje każdej wielkości. Ta wyrafinowana metoda gromadzenia danych umożliwiła szybszy przebieg operacji. Przegląd tej operacji przeprowadzony w 2012 r. przeprowadzony przez McAfee i Guardian Analytics wykazał, że w wyniku tego ataku z kont bankowych usunięto prawie 78 milionów dolarów. Serwery operacyjne znajdowały się w Rosji, Albanii i Chinach, ale ataki rozpoczęły się w Europie, przeniosły się do Ameryki Łacińskiej, a następnie wycelowały w Stany Zjednoczone. Chociaż nie ma konkretnych danych liczbowych określających, ile kosztują cyberprzestępstwa, szacunki światowej gospodarki wahają się od 100 do 500 miliardów dolarów rocznie.

W UK

W listopadzie 2013 r. Bank Anglii opublikował raport o stabilności finansowej, w którym szczegółowo opisano szereg ataków na brytyjski sektor bankowy. W raporcie stwierdzono:

Cyberatak w dalszym ciągu grozi zakłóceniem systemu finansowego. W ciągu ostatnich sześciu miesięcy kilka brytyjskich banków i infrastruktury rynków finansowych doświadczyło cyberataków, a niektóre z nich zakłóciły świadczenie usług.

W raporcie przyznaje się również, że sektor bankowy jest podatny na ataki cybernetyczne, ponieważ charakteryzuje się „wysokim stopniem wzajemnych powiązań, jego zależnością od scentralizowanej infrastruktury rynkowej i czasami złożonymi, dotychczasowymi systemami informatycznymi" (Bank of England, 2013).

W raporcie wskazano „systemowe" zagrożenie dla brytyjskiego systemu bankowego i płatniczego: „Chociaż straty były niewielkie w porównaniu z wymogami kapitałowymi brytyjskich banków w zakresie kapitału ryzyka operacyjnego, ujawniły one słabe punkty. Jeżeli te luki zostaną wykorzystane do zakłócenia usług, koszty dla systemu finansowego mogą być znaczące i poniesione przez dużą liczbę instytucji".

Raport został opublikowany po tym, jak brytyjskie banki wzięły udział w jednodniowym ćwiczeniu dotyczącym zagrożeń cybernetycznych zatytułowanym Operacja Waking Shark II, którego celem było sprawdzenie odporności systemów finansowych na poważne ataki cybernetyczne. Tego typu operacje wymagają od konkurentów w całym sektorze dzielenia się informacjami na temat potencjalnych zagrożeń, a tego rodzaju współpraca nie jest jeszcze uważana za praktykowaną. W grudniu 2013 r. banki Natwest i Royal Bank of Scotland z siedzibą w Wielkiej Brytanii padły ofiarą szeregu ataków DDoS, które według doniesień kosztowały je wielomilionowe odszkodowania. DDoS wpłynął na strony internetowe banku i bezpośrednio wpłynął na możliwość korzystania przez klientów banku z jego

usług. Obecnie nie ma jednoznacznych informacji na temat tego, kto był odpowiedzialny za atak ani jaka była jego motywacja. Gdyby za atakiem stała osławiona grupa hakerska, z dużym prawdopodobieństwem zgłosiłaby do niego roszczenia . W październiku 2012 r. grupa haktywistów rzeczywiście zgłosiła zarzuty ataku DDoS na HSBC, który wpłynął na możliwość dostępu milionów użytkowników do ich kont internetowych na całym świecie. W następstwie tego rodzaju ataków powszechne jest, że banki bronią danych klientów, zwykle twierdząc, że ataki nie naruszyły danych osobowych. Grupa hakerska, która nazywa siebie Fawkes Security na Twitterze i działa w powiązaniu z ideologią „anonimową",

twierdzą, że atak DDoS na HSBC uzasadniają tym, że banki są skorumpowane i spowodowały światowy kryzys gospodarczy. Grupa zamieściła na Twitterze informacje sugerujące, że miało to wpływ na dane osobowe:

Kiedy HSBC stwierdziło, że „dane użytkownika nie zostały naruszone", nie jest to do końca poprawne. Udało nam się również zalogować 20 000 danych kart debetowych. #OpHSBC

Nie ma dowodów na poparcie tych twierdzeń. Nie ma również dowodów sugerujących, że miało to związek z oszukańczą działalnością. Chociaż ataki DDoS mogą być wykorzystywane w połączeniu z przejmowaniem systemów banku w celu popełnienia oszustwa lub kradzieży własności intelektualnej. Destrukcyjne ataki DDoS stają się coraz częstsze w wyniku wolumetrycznego zalewania serwerów pomieszanymi lub niekompletnymi danymi. Oznacza to, że istnieje rosnąca potrzeba gromadzenia i udostępniania informacji wywiadowczych i strategii pomiędzy sieciami i całym sektorem finansowym w odniesieniu do ataków tego rodzaju. Chociaż kontekst tego studium przypadku jest finansowy – główna motywacja może nie mieścić się w kategorii „finansowej", jak pokazuje anonimowy atak na HSBC, a zatem można zaliczyć do kategorii „moralnej". Jednak rozgłos może również motywować ataki w przypadku znanych grup. Ataki DDoS są zwykle wysoce destrukcyjne i można je wykorzystać do maskowania innych nieuczciwych działań — w takich przypadkach główną motywacją będą motywy „finansowe".

PRZYPADEK ANONIMOWYCH ATAKÓW NA SCIENTOLOGIĘ

Anonymous to międzynarodowa sieć aktywistów, która powstała w 2003 roku na tablicy ogłoszeń opartej na obrazach (B) 4Chan. W ciągu ostatnich dziesięciu lat stała się znana z dużej liczby ataków DDoS na strony internetowe korporacji, rządów i religii. Anonymous (Anonymous, 2014a) opisują siebie jako „zdecentralizowaną sieć osób skupioną na promowaniu dostępu do informacji, wolności słowa i przejrzystości" (http:www.anonanalytics.com). Według Kelly'ego „jednak nawet pod dyskretnym parasolem haktywizmu Anonimowi charakteryzuje się odrębny skład: zdecentralizowana (prawie nieistniejąca) struktura, bezwstydne motywacje moralistyczne/polityczne i skłonność do łączenia cyberataków online z protestami offline" (s. 1668). Witryna internetowa powiązana z grupą opisuje ją jako „spotkanie internetowe" z „bardzo luźną i zdecentralizowaną strukturą dowodzenia, która działa w oparciu o idee, a nie dyrektywy" (http://anonnews.org/static/faq). Cenzura i kontrola Internetu stanowią sedno filozofii grupy, która zaaranżowała wiele dobrze nagłośnionych akrobacji. To studium przypadku skupi się na Projekcie Chanology – proteście przeciwko praktykom Kościoła scjentologicznego (2008). Projekt Chanology rozpoczął się po tym, jak Kościół Scjentologiczny próbował usunąć z YouTube makietę wywiadu przeprowadzonego przez Toma Cruise'a, mówiącego o scjentologii. Anonimowi oświadczyli, że uważają, że Kościół Scjentologiczny dopuszcza się aktów cenzury Internetu i rozpoczął szereg ataków DDoS, po których nastąpiła seria żartów mających na celu wywołanie jak największych zakłóceń w Kościele Scjentologicznym. Po atakach DDO w lutym 2008 roku ludzie na całym świecie związani z filozofią Anonymous podjęli bezpośrednie działania, protestując na ulicach przeciwko kościołowi. Szacuje się, że w co najmniej 100 miastach na całym świecie

protestowało około 7 000 osób, a tysiące zdjęć z wydarzeń zamieszczono na stronach takich jak flickr. Dalsze protesty miały miejsce w marcu, a następnie w kwietniu 2008 r. Ataki DoS miały wpływ na witrynę internetową Kościoła Scjentologicznego, która pod koniec stycznia wielokrotnie ulegała awariom. W rezultacie witryna scientology.org została przeniesiona do firmy zajmującej się ochroną, aby zapobiec dalszym atakom DDoS, jednak liczba ataków na witrynę wzrosła i w rezultacie ponownie stała się niedostępna (Kaplan, 2008). Anonimowy w komunikacie prasowym i filmie wypowiedział „wojnę scjentologii", doradzając, że będzie kontynuować ataki w celu ochrony wolności słowa (patrz Anonimowy YouTube 2008 Wiadomość do scjentologii). Chociaż tę sprawę można zaliczyć do kategorii „religii", przyczyny leżące u podstaw ataków są znacznie bardziej skomplikowane. Chociaż rozgłos odgrywa rolę w kampanii, twierdzenia dotyczące moralności są kluczowym uzasadnieniem ataków. Sprawa ta jest również interesująca, ponieważ nie ogranicza się do ataków online, ale także do działań bezpośrednich. Haktywiści etyczni, tacy jak Anonymous, utrzymują, że walczą o wzniosłość moralną, mając na celu poprawę jakości życia innych i poprawę świata.

SAMOREALIZACJA: PRZYPADEK „MAFIABOYA"

Michael Calce (Mafiaboy) był 15-letnim uczniem kanadyjskiej szkoły, kiedy w 2000 r. przeprowadził serię ataków DDoS na kilka dużych korporacji, w tym Yahoo, eBay, CNN, Dell i Amazon. Calce zaczął od ataku na Yahoo w ramach operacji, którą nazwał Projekt Rivolta (co po włosku oznacza Riot), a jego celem było ustanowienie dominacji dla siebie i TNT, swojej grupy cybernetycznej. Genosko (2006) tak opisał ten przypadek:

Nie był programistą. Zdobył zautomatyzowany „rootkit" napisany przez kogoś innego, a następnie ustawił go tak, aby działał „anonimowo". Mafiaboy przeprowadził rozproszony atak typu „odmowa usługi" (DDoS) – „zalew" wiadomości (pakietów), który sam w sobie powodował, że serwery nie były w stanie sprostać stawianym im wymaganiom – za pomocą pożyczonego skryptu, w tym przypadku odmowy- program serwisowy, którego autorem jest „Sinkhole" (chociaż wczesne doniesienia prasowe wskazywały na dzieło „miksera" o nazwie Tribal Flood Network). Umieścił szereg agentów DOS na „zombie" – porwanych systemach komputerowych na uniwersytetach i zdalnie sterował pracą za pomocą swojego zautomatyzowanego oprogramowania, wykorzystując przechwycone komputery do zalewania wybranych witryn internetowych pakietami danych (numerowanymi fragmentami plików).

Był to wówczas przełomowy przypadek cyberprzestępczości i udowodnił, że należy radykalnie poprawić bezpieczeństwo w Internecie, biorąc pod uwagę, że największa witryna internetowa na świecie (Yahoo w 2000 r.) może zostać zamknięta przez 15-latka. Włamania dostarczyły dowodów na istnienie poważnych luk w bezpieczeństwie Internetu, co wykorzystano w jego argumentacji na rzecz obrony: chciał zdemaskować takie błędy i zostać specjalistą ds. bezpieczeństwa komputerowego. Calce przyznał, że dopuścił się ataków z ciekawości. „W tym momencie wszyscy przeprowadzali testy i sprawdzali, co mogą zrobić i co mogą przeniknąć". Niezależnie od tego, czy motywacją była samorealizacja, ciekawość, czy metoda testowania słabych punktów w systemach bezpieczeństwa, według różnych źródeł medialnych ataki DDoS firmy Calce kosztują firmy ponad 1 miliard dolarów (CAD).

STRATEGICZNE ODPOWIEDZI NA ATAKI CYBER

Po przeanalizowaniu powyższych różnych przypadków cybernetycznych należy również podkreślić, że różne kraje stosują różne strategie radzenia sobie z tymi atakami. Poniżej znajduje się krótki przegląd strategii walki z cyberprzestępczością Wielkiej Brytanii, USA i UE. Kompleksowa krajowa inicjatywa na rzecz bezpieczeństwa cybernetycznego powołana przez rząd USA w 2008 roku składa się z następujących celów, które mają pomóc w zabezpieczeniu USA:

• Ustanowienie pierwszej linii obrony przed współczesnymi bezpośrednimi zagrożeniami

• Aby chronić się przed pełnym spektrum zagrożeń

• Wzmocnienie przyszłego środowiska bezpieczeństwa cybernetycznego

W dokumencie wymieniono także 12 kluczowych inicjatyw:

• Zarządzaj Federalną Siecią Przedsiębiorstw jako pojedynczym przedsiębiorstwem sieciowym z zaufanymi połączeniami internetowymi

• Wdróż system wykrywania włamań obejmujący czujniki w całym przedsiębiorstwie federalnym

• Kontynuowanie wdrażania systemów zapobiegania włamaniom w całym przedsiębiorstwie federalnym

• Koordynowanie i przekierowywanie wysiłków badawczo-rozwojowych (B+R).

• Połącz obecne centra operacji cybernetycznych, aby zwiększyć świadomość sytuacyjną

• Opracowanie i wdrożenie ogólnorządowego planu kontrwywiadu cybernetycznego (CI).

• Zwiększ bezpieczeństwo naszych tajnych sieci

• Rozwiń edukację cybernetyczną

• Definiowanie i rozwijanie trwałych, przełomowych technologii, strategii i programów

• Zdefiniuj i opracuj trwałe strategie i programy odstraszania

• Opracuj wielotorowe podejście do zarządzania ryzykiem w globalnym łańcuchu dostaw

• Zdefiniowanie roli federalnej w rozszerzaniu bezpieczeństwa cybernetycznego na domeny infrastruktury krytycznej (Biały Dom, 2009).

Departament Strategii Obrony na rzecz Działań w Cyberprzestępczości (2011) ma pięć inicjatyw strategicznych:

1. Traktuj cyberprzestrzeń jako domenę operacyjną do organizowania, szkolenia i wyposażania, aby Departament Obrony mógł w pełni wykorzystać potencjał cyberprzestrzeni

2. Stosować nowe koncepcje operacyjne w zakresie obronności w celu ochrony sieci i systemów Departamentu Obrony

3. Współpracuj z innymi departamentami i agencjami rządowymi USA oraz z sektorem prywatnym, aby umożliwić realizację strategii cyberbezpieczeństwa obejmującej cały rząd

4. Buduj solidne relacje z sojusznikami USA i partnerami międzynarodowymi, aby wzmacniać zbiorowe cyberbezpieczeństwo

5. Wykorzystaj pomysłowość narodu dzięki wyjątkowej kadrze cybernetycznej i szybkim innowacjom technologicznym

Brytyjska strategia bezpieczeństwa cybernetycznego (2011) składa się z czterech głównych celów:

• Zwalczanie cyberprzestępczości i uczynienie Wielkiej Brytanii jednym z najbezpieczniejszych miejsc na świecie do prowadzenia działalności gospodarczej w cyberprzestrzeni.

• Zwiększenie odporności Wielkiej Brytanii na ataki cybernetyczne i umożliwienie lepszej ochrony naszych interesów w cyberprzestrzeni.

• Pomoc w kształtowaniu otwartej, tętniącej życiem i stabilnej cyberprzestrzeni, z której społeczeństwo Wielkiej Brytanii może bezpiecznie korzystać i która wspiera otwarte społeczeństwa.

• Budowanie w Wielkiej Brytanii przekrojowej wiedzy, umiejętności i możliwości, aby wspierać wszystkie nasze cele w zakresie cyberbezpieczeństwa.

Strategia brytyjska zakłada skupienie się na osobach fizycznych i przedsiębiorstwach. W brytyjskiej strategii przyznano, że zagrożenia się zmieniają, ale jako aktualne zagrożenia w cyberprzestrzeni wyszczególniono następujące elementy:

• Przestępcy (oszustwo/kradzież tożsamości)

• Inne państwa (szpiegostwo/propaganda)

• Terroryści (propaganda/radykalizacja potencjalnych zwolenników/komunikowanie/planowanie)

• Haktywiści (zakłócenia/zarządzanie reputacją/szkody finansowe/zyskowanie rozgłosu)

W brytyjskiej strategii podkreślono również trudności w wycelowaniu w sprawców cyberprzestępstw:

„Jednak ze względu na bezgraniczny i anonimowy charakter Internetu dokładne przypisanie jest często trudne, a rozróżnienie między przeciwnikami coraz bardziej się zaciera” .

Europejska strategia cyberbezpieczeństwa Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń (2013), co zrozumiałe, uwzględnia obawy wielu krajów, a nie jednego, i dlatego podkreśla wielowarstwowy charakter Internetu bez granic. Ma pięć kluczowych priorytetów strategicznych:

• Osiągnięcie cyberodporności

• Drastyczne ograniczenie cyberprzestępczości

• Rozwój polityki i zdolności w zakresie cyberobrony związanych ze Wspólną Polityką Bezpieczeństwa i Obrony (WPBiO)

• Rozwój zasobów przemysłowych i technologicznych na rzecz cyberbezpieczeństwa

• Ustanowienie spójnej międzynarodowej polityki cyberprzestrzeni dla Unii Europejskiej i promowanie podstawowych wartości UE.

Różne strategie podkreślają potrzebę istnienia silnej globalnej sieci wspólnych informacji wywiadowczych i komunikacji na temat cyberprzestępczości. Za sieci odpowiedzialne są nie tylko rządy i eksperci, ale także przemysł i szersze społeczeństwo. Silne partnerstwa wraz ze wspólną wiedzą i informacjami mogą wzmocnić trudną sytuację w obliczu cyberprzestępczości i ataków, które każdego roku kosztują światową gospodarkę miliardy dolarów . Istnieją trzy różne strategie zarządzania cyberprzestępczością przedstawione powyżej; jednakże na całym świecie istnieje o wiele więcej inicjatyw (patrz na przykład strategia Australii z 2009 r. lub strategia Kanady z 2010 r.). Aby stworzyć strategię obejmującą różne domeny, z tych (i innych) strategii można wydobyć odpowiednią wiedzę i wykorzystać ją do zalecenia coraz bardziej skonsolidowanego punktu widzenia. Mające zastosowanie luki i pokrywanie się obszarów pomogłyby w zapewnieniu skutecznych i zintegrowanych rozwiązań (regulacyjnych, technicznych, etycznych, prawnych lub społecznych) istniejących zagrożeń, a także mogłyby pomóc w przewidywaniu przyszłych zagrożeń (a tym samym zapobieganiu im).

UWAGI KOŃCOWE

Omówiono szereg przykładów cyberataków. W oparciu o różne jurysdykcje prawne i polityczne, mogą one stanowić przestępstwo. Na przykład w przypadku SEA prowadzenie „haktywizmu" uważa się za metodę sprawiającą, że głosy osób, które normalnie nie miałyby głosu, zostają usłyszane. Przeprowadzanie ataków phishingowych i DDoS na rzecz tej grupy wydaje się być formą mobilizacji politycznej, ale w wielu przypadkach – rządowe strony internetowe nie są na czele tych ataków – są to przedsiębiorstwa. Zwiększa rozgłos ich sprawy – jednocześnie podkreślając, że naruszenia bezpieczeństwa zdarzają się nawet w największych organizacjach, które mają być liderami bezpieczeństwa – zwiększając w ten sposób ich rozgłos. Nie tolerując ani nie potępiając ich działań, wydaje się, że jest to prosty sposób na spowodowanie zakłóceń w firmach i zastępuje protesty na ulicach. Kluczem do tego, aby ich głos został usłyszany, jest świadomość, że istnieje potrzeba obecności w mediach społecznościowych – do tego stopnia, że czasami muszą codziennie tworzyć nowe strony w mediach społecznościowych. Dzięki stałej obecności w mediach społecznościowych oraz ciągłym atakom phishingowym i atakom DDOS ukierunkowanym na różne rynki udaje im się zapewnić nie tylko obecność w mediach społecznościowych, ale także obecność w mediach, a co za tym idzie, w pewnym stopniu świadomość ich przyczyny. Z drugiej strony SEA może obierać za cel strony internetowe o charakterze niepolitycznym, ponieważ stwarzają one wrażliwe możliwości i mogą powoływać się na znaczenie moralne w celu uzyskania rozgłosu. Tak czy inaczej, nieco niedorzeczne jest twierdzenie, że ogólnie nie ufają mediom, ale wykorzystują je do własnych celów. Uważa się, że Stuxnet to pierwszy publicznie znany przypadek wojny cybernetycznej i choć ma podłoże polityczne, może mieć także motywy moralne i finansowe. Sprawa jest owiana spekulacjami – eksperci przypuszczali, że było to dzieło państwa narodowego i gdyby istniały niezbite dowody na poparcie tych twierdzeń, sprawa zostałaby sklasyfikowana jako polityczna. Chociaż z prawnego punktu widzenia nie jest jasne, kto przeprowadził atak, można zastosować motywy moralne (w odniesieniu do punktu ataku: zakłócenie produkcji energii jądrowej), jednocześnie zakłócając finanse kraju poprzez niszczenie systemów przemysłowych. Operacja High Roller bezpośrednio wskazuje na motywacje finansowe, gdyż podczas ataków doszło do oszustw. Chociaż ataki DDoS zakłócają usługi bankowe, mogą również ukrywać oszukańcze działania i można je sklasyfikować jako finansowe, można je również sklasyfikować jako moralne, ponieważ hakerzy twierdzą również, że banki są skorumpowane. Zagrożenie w tym przypadku pozostaje po stronie sektora bankowego, ale może mieć bezpośredni wpływ na osoby fizyczne. W przypadkach, gdy następuje samorealizacja – tj. hakerzy atakują, aby przetestować systemy lub robią to, ponieważ mogą – jak w przypadku Mafiaboy – zagrożenie można sklasyfikować jako poważne. Operacyjnie, aby rozpocząć ocenę zagrożeń, przedstawiono metodę gromadzenia informacji i danych z wykorzystaniem systemu taksonomii do zrozumienia sytuacji. Model ten koncentruje się na zamiarach i motywacji cyberprzestępstw, a nie na podejściu technicznym, skupia się na czynniku ludzkim. Pięć przypadków z życia codziennego nie tylko pokazuje różnorodność, a czasem złożoność poszczególnych przestępstw, ale także pokazuje różnicę w motywacjach poszczególnych przestępstw. Dlatego proponowana taksonomia tworzenia repozytorium wiedzy skupia się szczególnie na postrzeganych motywacjach i zamiarach potencjalnych podejrzanych i sprawców. Korzystanie z powyższego modelu taksonomii stanowi punkt wyjścia w kierunku uzyskania jaśniejszego zrozumienia sytuacyjnego cyberprzestępczości. Obecnie, przy wielu strategiach cyberprzestępczości na całym świecie i bez uzgodnionych definicji ani przepisów, gromadzenie wiedzy na temat cyberprzestępczości, w tym wiedzy sytuacyjnej, pomoże w wypracowaniu praktycznych konsekwencji dla środków zaradczych. Jest to szczególnie prawdziwe, jeśli weźmiemy pod uwagę naszą wcześniejszą definicję wiedzy. Biorąc pod uwagę brak uzgodnionych definicji i liczne strategie zwalczania cyberprzestępczości, model został zaprojektowany tak, aby był elastyczny dla funkcjonariuszy pierwszej linii, zwłaszcza w świetle faktu, że sprawy mają różny charakter. W modelu zastosowano

również prosty język, ponieważ nie uzgodniono jeszcze uniwersalnego systemu językowego dla cyberprzestępczości.

Terrorystyczne wykorzystanie Internetu

TERRORYSTYCZNE WYKORZYSTANIE INTERNETU

Rozdział ten stanowi nie tylko próbę opisu sposobu wykorzystania Internetu przez grupy terrorystyczne, ale także dostarcza informacji o tym, w jaki sposób Internet mógłby zostać wykorzystany w najbliższej przyszłości, biorąc pod uwagę najnowsze osiągnięcia technologiczne. Na ten temat napisano już wiele artykułów, ale potraktowano je częściowo, skupiając się na stronie propagandowej lub hakerskiej i „technicznej". W tym rozdziale zostanie opisana propaganda i techniki szyfrowania stosowane przez terrorystów.

PROPAGANDA – INDOKTRYNACJA – REKRUTACJA

Od wielu lat trend rosnący określany jest wykorzystaniem Internetu przez terrorystów. W rzeczywistości zjawisko to jest bardziej ograniczone niż się wydaje. W artykułach przekazywanych przez media i tzw. ekspertów podjęto próbę oszacowania liczby stron internetowych o charakterze terrorystycznym. Jednak te statystyki same w sobie nic nie znaczą; należy je porównać z całkowitą liczbą stron internetowych dostępnych w sieci. Organizacje terrorystyczne na ogół korzystają z Internetu w celach propagandowych. Światowa sieć internetowa i stały rozwój sieci Web 2.0 dały społeczeństwu możliwość łatwego dostępu do informacji i ich publikowania. Wysokie umiejętności informatyczne nie są już konieczne do publikowania i publikowania informacji, zdjęć i filmów w Internecie, a także są bardzo istotna opłacalna metoda komunikacji. Propaganda terrorystyczna w Internecie jest rozpowszechniana za pośrednictwem kilku rodzajów platform; strony internetowe do udostępniania wideo, takie jak YouTube; usługi sieci społecznościowych online, takie jak Facebook; oraz poprzez tradycyjne fora i blogi internetowe.

ROLA WIDEO

Wideo odgrywa kluczową rolę w propagandzie; pokazują zdolność grupy terrorystycznej do przeprowadzania skutecznych operacji, takich jak ataki samobójcze. Stanowią one także dowód dla darczyńców i sponsorów, potwierdzający, że przekazane przez nich pieniądze są dobrze wykorzystywane, na przykład na „sprawę dżihadu" związaną z terroryzmem typu Al-Kaida. Według monitoringu grup syryjskich z wykorzystaniem otwartego źródła przez organy ścigania, w ciągu roku większość umiarkowanych syryjskich grup bojowych, których celem były demokratyczne wybory po upadku Bashara al-Assada, zwróciła się obecnie w stronę ideologii dżihadu, których celem jest ustanowienie prawa szariatu . Wszystkie te grupy bojowe opublikowały w Internecie oświadczenia, aby nagłośnić zmianę swojej ideologii – najprawdopodobniej po to, aby zwrócić uwagę (i fundusze) sponsorów opowiadających się za Syrią rządzoną przez prawo szariatu.

FORA INTERNETOWE – BLOGI

Fora są najpowszechniejszą metodą promowania terroryzmu w Internecie, ponieważ stanowią platformę, na której gromadzą się ludzie o tym samym sposobie myślenia; niemniej jednak fora te wiążą się również z pewnymi niedogodnościami, które należy wyjaśnić. W przeszłości każde forum terrorystyczne było kontrolowane tylko przez jednego administratora, ale sukcesy kilku organów egzekwowania prawa w aresztowaniu administratorów zahamowały lub zakłóciły działanie kilku forów terrorystycznych. W związku z tymi aresztowaniami pojawił się nowy trend, którego celem jest podzielenie administrowania forum terrorystycznym pomiędzy kilku administratorów. Wszyscy albo mają ten sam login/hasło, albo mają wielu administratorów i wszyscy wiedzą, jak zarządzać forum.

Jeżeli któryś z nich zostanie aresztowany, forum będzie mogło kontynuować swoją zwykłą działalność. Dokładnie tak się stało, gdy kilka lat temu władze hiszpańskie aresztowały administratora forum terrorystycznego „Ansar al Mujahideen". Główną zaletą posiadania własnego forum przez te grupy terrorystyczne jest całkowita kontrola nad cenzurą, a mianowicie nad komunikacją między jej członkami: wiadomości i wątki można modyfikować i usuwać. Mają także całkowitą swobodę w wyborze działającej platformy, lokalizacji hostingu, dzienników aktywności i kontroli dostępu użytkowników, dzięki czemu członkowie mogą zostać zablokowani lub awansowani na podstawie sposobu, w jaki się zachowują.

USŁUGI SPOŁECZNOŚCIOWE ONLINE

Najnowszym rosnącym trendem są internetowe serwisy społecznościowe, z których korzystają terroryści; coraz więcej zwolenników terroryzmu docenia swobodę wymiany lub komentowania wszelkich działań terrorystycznych bez ograniczeń ze strony administratorów forum, jak opisano powyżej. Rosnąca liczba sympatyków terrorystów korzystających z serwisów społecznościowych pokazała już, że społeczność terrorystyczna nie jest tak zjednoczona i wspierająca, jak mogłoby się wydawać. Istnieje kilka nieporozumień co do twierdzeń o atakach, a nawet celu ataku; na przykład rozłam między Islamską Armią Iraku, która twierdziła, że syryjski Dżabhat al-Nusra jest jedną z jej stowarzyszonych grup, podczas gdy Jabhat al-Nusra odrzuca to powiązanie i twierdzi, że konflikt syryjski nie ma nic wspólnego z Irakiem, jest przykładem wśród wiele. Wzrost liczby kont terrorystycznych na Twitterze rodzi kwestię identyfikacji osób lub grup, na przykład kilka kont na Twitterze uznawanych za oficjalny podmiot medialny somalijskiej organizacji terrorystycznej; al-Shabab, jednak trudno jest określić, kto jest autentyczny, a kto podszywa się pod niego. Stwarza to poważny problem dotyczący tego, kogo monitorować dla służb wywiadowczych. Na początku 2012 r. w kilku postach na forum „Ansar al Mujahideen" omawiano możliwość stworzenia strony internetowej Jihadi Social Network. Ta „strona internetowa" powielałaby główne usługi i funkcje oferowane przez Facebooka lub Google + w nadziei na zwiększenie liczby sympatyków, a w konsekwencji naśladowanie społeczności terrorystycznej w publikowaniu większej liczby postów. Początkowy pomysł nie uwzględniał następujących kwestii: ilości pracy potrzebnej do stworzenia i utrzymania takiej strony internetowej; hosting takiej usługi; lub kontrolę tożsamości użytkowników uzyskujących dostęp do tej platformy. Pojawienie się niezależnej, godnej zaufania usługi sieci społecznościowej bez ingerencji agencji rządowych lub organów ścigania jest w rzeczywistości mało prawdopodobne i dość trudne do urzeczywistnienia.

PROCES RADYKALIZACJI W INTERNECIE

Internautów lub sympatyków terrorystów początkowo przyciąga środowisko terrorystyczne za pośrednictwem witryn do udostępniania plików wideo, takich jak YouTube, gdzie wyświetlane są filmy przedstawiające ataki terrorystyczne. Konta YouTube odnoszą się do adresu URL forum terrorystycznego, na które można kliknąć, aby uzyskać dostęp do forum, a także dołączyć do forum, wysyłając wiadomość e-mail do jego administratorów. Kiedy „młodszy członek" dołączy do forum, zostanie przetestowany pod kątem wykonywania podstawowych zadań. Zostaną wówczas poddani ocenie i na podstawie dobrych wyników otrzymają wyższą rangę, np. „członek", „członek zatwierdzony", „członek senior" itp. Jednocześnie otrzymają też większe przywileje, np. mogliby otrzymać zadanie administrowania nowymi osobami na forum. Po pewnym czasie jeden z czołowych administratorów poprosi „starszego członka" o fizyczne spotkanie w celu dalszej oceny i potwierdzenia, że osoba ta jest dobrym kandydatem. Po tym kluczowym spotkaniu „nowy rekrut" zostaje przedstawiony bardzo małej sieci znacznie zradykalizowanych osób za pośrednictwem VoIP, takiej jak Skype lub Paltalk. Na tym etapie kandydatowi powierza się wrażliwe informacje, m.in. dotyczące planowania ataków lub wyznaczania celów.

PRZYPADEK SZCZEGÓLNY: SAMOTNY WILK

Z definicji Samotne Wilki są osobnikami najtrudniejszymi do wykrycia, ponieważ działają samotnie i nie korzystają z Internetu do komunikowania się z rówieśnikami. Wykorzystują jednak Internet do przygotowywania ataków, a także do reklamowania swoich roszczeń na przykład w filmach lub e-mailach. Korzystają również z Internetu do interakcji z osobami/grupami wyznającymi podobne ideologie i czasami wyrażają swoje niezadowolenie w sieciach społecznościowych. Samotne wilki można badać, wykrywając odchylenia od przeglądania, a także zakup online produktów takich jak materiały wybuchowe, prekursory w celu zbudowania IED (improwizowanego urządzenia wybuchowego) lub broni. Ponadto w niektórych przypadkach zgłoszono, że nie należy lekceważyć zagrożenia „wewnętrznego". Zwykle są to osoby o wysokich kwalifikacjach lub wiedzy, które mają dostęp do środowiska zajmującego się niebezpiecznymi materiałami lub mają dobrą pozycję w organizacji i zamieniają się w Samotne Wilki, aby przeprowadzić jednorazowy atak, korzystając ze swojej specjalistycznej wiedzy. Najbardziej znanym jak dotąd przypadkiem jest z pewnością sprawa Ivinsa i ataki bioterrorystyczne Anthrax w 2001 r. (nazwane Amerithrax). Motywacja samotnego wilka może być dwojaka:

• Osoba wewnętrzna lub motywująca: Niezadowolona z przyjęcia ideologii, związana z załamaniem nerwowym lub problemami ze zdrowiem psychicznym.

• Wpływ zewnętrzny: Cel inżynierii społecznej, a następnie indoktrynacja.

UDOSTĘPNIANIE INFORMACJI

Początkowo zgłaszano, że grupy typu Al-Kaida stosowały steganografię do ukrywania wiadomości na zdjęciach i/lub filmach. Chociaż steganografia jest metodą zaciemniania i nie można jej uważać za technologię szyfrowania, służy ona ukryciu wiadomości przed wzrokiem, co z kolei zapewnia względną prywatność i jest jednym z celów szyfrowania. Ten sposób działania był wysoce prawdopodobny, lecz nigdy nie udowodniono, że jest powszechnie stosowany. Rozmiar informacji, które można ukryć na obrazie, jest bardzo ograniczony, ponieważ na przykład obraz niskiej jakości składający się z dużej liczby mega bitów byłby bardzo podejrzany. Po zamachach bombowych na pociągi w Madrycie 11 marca 2006 r. aresztowani podejrzani ujawnili, że stosowali podstęp, aby uniknąć wykrycia przez monitoring poczty elektronicznej. Koncepcja polegała na udostępnieniu członkom grupy jednego konta e-mail (takiego jak Hotmail, Yahoo!), na którym mogliby pisać e-maile, a następnie zostawiać je w folderze Wersja robocza. W ten sposób nie pozostawiono żadnych śladów, ponieważ nie wysłano żadnych e-maili. Obecnie ta technika jest mniej prawdopodobna, ponieważ sztuczka jest obecnie dobrze znana i dostęp do jednego konta z kilku różnych lokalizacji jednocześnie lub z bardzo odległych miejsc lokalizacji geograficznych w krótkim czasie z pewnością zwróci uwagę dostawcy poczty, że dane konto jest współdzielone przez kilka osób. W przeszłości grupy terrorystyczne typu Al-Kaida również próbowały stosować pewne technologie szyfrowania. Jednakże brak zaufania do gotowych do użycia narzędzi, takich jak PGP, które zostało opracowane prywatnie lub TrueCrypt, które było narzędziem open source opracowanym przez społeczność, oraz potencjalne backdoory umieszczone przez rządy, nie zapewniły im całkowitego ubezpieczenia ochrony poufności. Dlatego postanowili opracować własne narzędzie „Mujahideen Secrets" (lub „Asrar al-Mujahedeen"), a później Mujahideen Secrets 2. Pierwsze wydanie zostało wydane przez Global Islamic Media Front w 2007 r., a wkrótce potem pojawiła się druga wersja w 2008. Oczywiście posiadanie własnego narzędzia ma pewne zalety, takie jak większe zaufanie do jego użycia ale z pewnością przyniósł więcej wad. W związku z tym posiadanie zastrzeżonego narzędzia, które nie zostało dokładnie przetestowane przez szerszą społeczność, czyni je bardziej podatnym na luki w zabezpieczeniach. Kiedy już stało się znane, narzędzie to było również głównym celem inżynierii wstecznej prowadzonej przez różne wydziały wywiadu antyterrorystycznego

i organy ścigania na całym świecie. Wreszcie posiadanie takiego narzędzia daje dodatkowe wskazówki, że dana osoba potencjalnie należy do grupy terrorystycznej lub jest z nią w jakiś sposób powiązana. W lutym 2013 r. Global Islamic Media Front udostępnił nowe narzędzie szyfrujące „Asrar al-Dardashah", tym razem jako wtyczkę do klienta komunikatorów internetowych Pidgin, którego można używać w połączeniu z kontami użytkowników na popularnych platformach, takich jak Google Talk, MSN, Yahoo, AOL Instant Messenger i Jabber/XMPP. Chociaż można to postrzegać jako zmianę strategii korzystania z Internetu poprzez wdrożenie warstwy szyfrowania na istniejących usługach, główną wadą jest to, że klucze publiczne mają bardzo wyraźny nagłówek „# — Rozpocznij sieć Al-Ekhlaas ASRAR El Moujahedeen V2 .0 Public Key 2048 bit—", co prowadzi do zwiększonych trudności w przechowywaniu kluczy na serwerze publicznym lub wymianie tych kluczy bez zwracania uwagi jednostek antyterrorystycznych. Ta sama grupa, Global Islamic Media Front, udostępniła także aplikację na Androida do wysyłania/odbierania zaszyfrowanych SMS-ów i plików. Rzeczywiście, tego narzędzia nie można pobrać bezpośrednio z oficjalnego sklepu, ale jest ono dostępne na ich stronie internetowej, a dla potencjalnych użytkowników dostępny jest samouczek. Wreszcie w grudniu 2013 r. odkryto nowe narzędzie, które zostało udostępnione przez Al-Fajr Media Centre. To narzędzie szyfrujące to najnowszy program dostępny dla terrorystów typu Al-Kaida i nosi kryptonim „Amn al-Mujahid" (tajemnica mudżahedinów). Jest to oprogramowanie podobne do PGP, które umożliwia użytkownikom wybór spośród zestawu dobrze znanych algorytmów szyfrowania i generowanie par kluczy.

PRZYSZŁY ROZWÓJ CYBERTERRORYZMU

Możemy sobie wyobrazić, że w niedalekiej przyszłości grupy terrorystyczne i/lub powiązane z nimi grupy będą chciały wykorzystać swoje ataki, aby móc osiągnąć niespotykaną dotąd skalę wpływu strachu i zniszczenia. Mając to na uwadze, Internet można bez wątpienia wykorzystać jako narzędzie do bezpośredniego odparcia poważnego ataku. Najbardziej oczywistym celem będą z pewnością systemy infrastruktury krytycznej, w których zakłócenia mogą zagrażać życiu i/lub powodować masowe zakłócenia, wywołując jednocześnie brak zaufania ze strony szerszej populacji (np. włamanie do systemu transportowego). Dość trudno ocenić, czy grupy terrorystyczne są bliskie przeprowadzenia takich ataków. Jeżeli jednak tradycyjne grupy terrorystyczne wyrażą na to chęć, oznacza to, że będą musiały albo zrekrutować osoby posiadające dużą wiedzę, albo poprosić o pomoc z zewnątrz, np. w celu zakupu określonych umiejętności za pośrednictwem platformy takiej jak CaaS (Crime as a Service) lub osoby takie jak hakerzy -do wynajęcia. Jednakże, jak wspomniano wcześniej, największym problemem jest zaufanie, a ilość czasu potrzebna na opracowanie tego typu ataku może być dość znaczna. Nie można także ignorować wycieku informacji o operacji. Atak musiałby również zostać zbudowany (np. w ramach tworzenia oprogramowania itp.) i przetestowany. Problem z testowaniem polega na tym, że jest on wykonywany „off-line" lub poza systemem docelowym. W opcji „off-line" wymaga to najpierw rozpoznania/wywiadu, ale także ogromnych zasobów, aby odtworzyć docelowy system, a w większości przypadków jest to niemożliwe (np. systemy SCADA). Drugi problem z testowaniem, jeśli jest przeprowadzany na działającym systemie, polega na tym, że pozostawia szumy (np. ślady/dzienniki), które mogą zwrócić uwagę docelowych funkcji monitorowania systemu. Opcja ta jest zbyt ryzykowna i mało prawdopodobne, aby grupy terrorystyczne wybrały ją. Z drugiej strony grupy ekstremistyczne lub aktywistyczne mogą mieć odmienne spojrzenie na kwestie zaufania i nie wahać się zwrócić się o pomoc z zewnątrz i zakupić na nielegalnym rynku brakujące umiejętności potrzebne do przeprowadzenia cyberataku. Dodatkowo, jeśli weźmiemy konkretny przypadek haktywizmu, to grupy skupiające niezwykle wykwalifikowanych i znających się na IT ludzi zwiększają prawdopodobieństwo odniesienia sukcesu w ataku cyberterrorystycznym w porównaniu z innymi wymienionymi do tej pory grupami. Biorąc przykład za udane wydarzenie STUXNET, które miało miejsce w 2010 r. Był to bardzo wyrafinowany kod, który został opracowany w celu wykorzystania systemu SCADA w celu uszkodzenia wirówek w celu spowolnienia irańskiego programu wzbogacania

uranu (zob. rozdział 3). Po inżynierii odwrotnej kodu okazuje się, że wymagane zasoby i wiedza o celu potrzebne do pomyślnego zakończenia takiej operacji były ogromne i wydaje się, że nie są jeszcze w zasięgu grup terrorystycznych, ekstremistycznych ani aktywistów i mogą pochodzić wyłącznie od sponsorowanych przez państwo lub państwowe CyberTeams.

FINANSOWANIE

Głównym elementem umożliwiającym grupie terrorystycznej przeprowadzenie ataków jest potrzeba finansowania przez partnerów, sponsorów lub partnerów. Dlatego też państwa i społeczności organów ścigania nalegały na wprowadzenie zasad, przepisów i technik wykrywania podejrzanych transakcji finansowych w celu identyfikacji potencjalnych osób uczestniczących w działaniach terrorystycznych. Biorąc to pod uwagę, możemy wziąć za przykład porozumienie USA i Europy, program śledzenia środków finansowych należących do terrorystów UE-USA TFTP (2010), podpisane w sierpniu 2010 r. w celu rozwiązania tej kwestii. Komisja Europejska analizuje obecnie porozumienie europejskie, EU TFTS (system śledzenia finansów terrorystów). Chociaż umowy te mogą być istotne i dość skuteczne, nie dotyczą pojawiających się problemów technologicznych, takich jak rozwój walut wirtualnych. Waluty wirtualne to waluty alternatywne, które nie są zatwierdzone ani produkowane przez żaden rząd. Można je podzielić na dwa główne strumienie: pieniądze elektroniczne z gier internetowych, takich jak Second Life i kryptowaluty (lub waluty cyfrowe typu open source). Elektroniczne pieniądze oparte na grach internetowych można wykorzystać do przesyłania dużych ilości wirtualnych pieniędzy między osobami fizycznymi i wymieniania ich na prawdziwe pieniądze. Jednak szczególnie po rewelacjach Snowdena (2013) tego rodzaju gry zostały zinfiltrowane przez NSA i GCHQ w poszukiwaniu działalności terrorystycznej. Ponadto osoby grające w te gry muszą zapoznać się z zasadami gry i sposobem korzystania z wirtualnych pieniędzy. Muszą na przykład wiedzieć, kto stoi za postacią i dokąd wysyłane są pieniądze. Kolejną wadą jest to, że rodzaj pieniędzy jest oczywiście powiązany z sukcesem gry i jej przyszłym rozwojem. Druga alternatywa, kryptowaluta, wydaje się bardziej prawdopodobna i szybko się rozwinęła w ciągu ostatnich 3 do 4 lat. Wśród wielu dostępnych obecnie walut, liderem jest Bitcoin. Składa się z systemu płatności zorganizowanego w formie sieci peer-2-peer opartej na kryptografii klucza publicznego. Narzędzie to jest coraz bardziej interesujące dla przestępców, a także terrorystów, ponieważ portfele są w pewnym stopniu anonimowe i zależne od przepisów walutowych dotyczących prywatności oraz zapewniają ułatwione sposoby spieniężenia i wypłaty wirtualnych pieniędzy na twarde pieniądze bez możliwości śledzenia przez instytucje finansowe i dlatego obecne systemy nadzorujące są nieefektywne. Z drugiej strony waluty te istnieją jeszcze stosunkowo niedawno i regulacje dotyczące legalności ich używania są niepewne (i przyszłości wypłaty prawdziwych pieniędzy). Drugi punkt, koncepcja sieci peer-2-peer, sprawia, że anonimowość właściciela portfela jest dość ograniczona. Aby waluta działała, a ponieważ nie ma centralnego punktu sprawdzania poprawności, wszystkie transakcje są upubliczniane, aby każdy węzeł w każdej chwili wiedział, jakie jest saldo portfela i jakie transakcje zostały wykonane przez właściciela portfela . Aby odbierać i/lub wysyłać wirtualne pieniądze, użytkownik ma adres(y) transakcji. Tak więc, gdy tylko właściciel adresu transakcji zostanie zidentyfikowany, wszystkie transakcje dokonane przez tę osobę z tym adresem transakcji będą znane w całej sieci. Oczywiście, aby zachować anonimowość, użytkownicy często zmieniają adres transakcji. Waluty cyfrowe charakteryzują się również dużą zmiennością, więc pomiędzy momentem, gdy dana osoba wstrzyknie pieniądze do systemu, a inna osoba je wypłaci, strata może być dość znacząca. Wydaje się jednak, że przestępcy uważają ten rodzaj waluty za niezwykle praktyczny/atrakcyjny i coraz częściej go używają. Na przykład likwidacja podziemnego rynku przestępczego SilkRoad doprowadziła do przejęcia przez FBI 175 000 Bitcoinów (o wartości wówczas 33 milionów dolarów). Udowodniono, że w maju 2013 r. likwidacja Liberty Reserve, najstarszego i największego serwisu obsługującego waluty cyfrowe, przyniosła korzyści głównie działalności przestępczej, umożliwiając pranie pieniędzy na kwotę 4,4 miliarda € (6 miliardów dolarów).

Kolejną zaletą dla terrorystów jest możliwość przełączania się pomiędzy wirtualnymi walutami (takimi jak Litecoin, Peercoin czy Namecoin, żeby wymienić tylko kilka innych), aby lepiej zatrzeć ślady. Zadanie badania i śledzenia transakcji staje się złożone, ponieważ obecnie istnieje już około 70 kryptowalut (Coinmarketcap.com). Ten rodzaj waluty jest tak atrakcyjny, że przestępcy zaczęli tworzyć złośliwe oprogramowanie i botnety, które skanują komputery celów w poszukiwaniu portfeli w celu kradzieży ich zawartości, a także wykorzystują moc obliczeniową swoich celów do „wydobywania" (tj. generowania) cyfrowej waluty. Pomimo tych wad kryptowaluta z pewnością będzie atrakcyjna dla sieci terrorystycznych do przesyłania dużych ilości pieniędzy od jednej strony do drugiej, zachowując przy tym dyskrecję. Istnieje wiele sposobów wypłaty środków (od rzeczywistych do wirtualnych) i można je wykonać anonimowo. Na przykład korzystając z Western Union, MoneyGram za pośrednictwem platformy takiej jak CoinMama (coinmarketcap.com) lub bezpośrednio kupując wirtualne pieniądze od osoby do osoby w pobliżu, na przykład na LocalBitoins.com. Podobnie jak w przypadku wypłaty, Localbitcoins.com również sprzedaje wirtualne pieniądze bezpośrednio osobie fizycznej w zamian za prawdziwe pieniądze. Jest to najłatwiejszy sposób, ale niezbyt wygodny w przypadku dużych kwot. Alternatywą jest użycie muła jednorazowego do wypłaty pieniędzy z oficjalnej giełdy, takiej jak VirCurEx. Tak czy inaczej, kryptowaluty otwierają przed przestępcami i terrorystami nowe możliwości anonimowej wypłaty prawnego środka płatniczego. Wreszcie, niewątpliwie po rewelacjach Edwarda Snowdena (2013) i PRISM, jest bardzo prawdopodobne, że wspomniane powyżej systemy będą dążyć do ewolucji i wprowadzenia jeszcze większej prywatności, co z kolei przyniesie oczywiście korzyści ich użytkownikom – wśród których niektórzy to przestępcy i terroryści . Podsumowując, kryptowaluty będą bardzo atrakcyjne dla organizacji terrorystycznych, gdy osiągną kombinację wysokiej anonimowości lub niskiej identyfikowalności (w celu uniemożliwienia identyfikacji nadawców/odbiorców transakcji), stabilności waluty (w celu zminimalizowania ryzyka utraty pieniędzy zainwestowanych w kryptowaluta) i elastyczność (różne opcje zamiany/wypłaty kryptowaluty na prawdziwe pieniądze).

CIEMNA SIEĆ

Na początku 2000 r. w wyniku rozwoju sytuacji powstały sieci alternatywne działające równolegle z Internetem. Pierwotnym ich celem była pomoc ludziom żyjącym pod opresyjnymi reżimami i pozbawionym wolności słowa w możliwości komunikowania się, zapewniając im większą anonimowość i możliwość ominięcia krajowej inwigilacji. Takie sieci zapewniają anonimizację ruchu między klientem a serwerem, ale także pozwalają na tworzenie/hostowanie usług ukrytych, takich jak usługi internetowe, wymiana plików, logowanie, czatowanie ukryte przed Internetem. W rezultacie taka szansa przyciągnęła nie tylko uciskanych ludzi, ale także przestępców i terrorystów, którzy znaleźli za pośrednictwem tych sieci nowy sposób wymiany informacji i szerzenia wiedzy itp. Obecnie istnieją dwie główne anonimowe sieci: TOR (The Onion Router), najstarszy i I2P. W przeciwieństwie do sieci społecznościowych i forów/blogów, na których grupy terrorystyczne zamieszczają ogłoszenia, przypisują sobie odpowiedzialność za ataki i rekrutują w Internecie, sieci darknet służą do dostarczania określonych treści, takich jak filmy i materiały szkoleniowe, które można znaleźć w ukrytych usługach TOR.

DRUKOWANIE 3D

Druk 3D, choć nie jest bezpośrednim wykorzystaniem Internetu, staje się dostępny dla szerszej publiczności. Udowodniono już, że technologia ta pozwala na produkcję broni, takiej jak noże i pistolety. W takich przypadkach Internet jest zwykle używany do wyszukiwania obiektów wirtualnych lub planów 3D. Można tworzyć pojedyncze lub wielokrotne obiekty. Choć stworzona broń jest dość prymitywna, zaletą jest to, że jest niewykrywalna podczas bieżących kontroli bezpieczeństwa na lotniskach. Na przykład izraelski reporter przeprowadził test, drukując broń, pomyślnie przeszedł

kontrolę bezpieczeństwa w Knesecie i był w stanie wyciągnąć ją przed premierem . W 2013 r. policja podczas przeszukiwania domów znalazła części broni. Można się spodziewać, że w najbliższej przyszłości nastąpi gwałtowny postęp w jakości i możliwościach druku 3D, a także pomnożenie dostępnych projektów. Już teraz niektóre strony internetowe udostępniają wyszukiwarki i/lub funkcję wyszukiwania torrentów dla planów 3D. Na przykład DEFCAD, witryna internetowa poświęcona hostowaniu projektów planów, wyraźnie zdecydowała się ograniczyć projekty, które mogą wytwarzać szkodliwe produkty, takie jak broń. Chociaż Biuro Kontroli Handlu Obronnego Departamentu Stanu zwróciło się do tej witryny internetowej z formalną prośbą o wycofanie tych projektów, jest już za późno, ponieważ przedmiotowe plany były pobierane tysiące razy w okresie, w którym były dostępne. I nieuchronnie te plany można teraz znaleźć w sieciach peer-to-peer i w The Pirate Bay.

PEŁNA SIEĆ VPN

Ponieważ komunikacja i wymiana informacji między członkami komórki lub organizacji terrorystycznej ma kluczowe znaczenie, niektóre istniejące urządzenia można wykorzystać do lepszego egzekwowania anonimowości. Na przykład dzięki pełnej usłudze VPN dla wszystkich członków i prowadzeniu całej komunikacji przez ten centralny punkt VPN. Obecnie urządzenia takie jak NAS (Network Dołączony magazyn danych) zapewniają szereg dodatkowych usług, które są łatwe do zainstalowania oprócz zapewnienia pamięci masowej. Możemy sobie wyobrazić instalację takiego NASa w bezpiecznym lub nieoczekiwanym miejscu lub w placówce opieki z szerokopasmowym dostępem ADSL. Jeśli organizacja terrorystyczna obdarzy urządzenie NAS wystarczającym zaufaniem, urządzenie to można skonfigurować tak, aby umożliwiało komunikację wyłącznie VPN i za pośrednictwem tego kanału zapewniało dodatkową dedykowaną telefonię VoIP (Voice over IP), serwery poczty e-mail, serwer WWW, serwer wideo, pliki udostępnianie/przechowywanie, każdy inny rodzaj aplikacji potrzebny komórce i/lub grupie do funkcjonowania i przygotowania ataku. Ma to tę zaletę, że jest dostępne nie tylko dla laptopów i stacji roboczych, ale także dla smartfonów, które obsługują teraz funkcje VPN. Dzięki temu członkowie komórki/grupy mogą korzystać z różnych usług bez konieczności wykonywania prawdziwej rozmowy telefonicznej lub wymiany informacji poza siecią VPN, dzięki czemu pozostają niewykrywalni. Z tej perspektywy dość trudno jest zidentyfikować, czy dane połączenie VPN jest wykorzystywane przez grupę/komórkę terrorystyczną. W przypadku jego zidentyfikowania dostęp do treści wymiany poprzez wdrożenie szyfrowania w drodze nadzoru elektronicznego byłby utrudniony. Wreszcie, jeśli punkty końcowe są używane wyłącznie do komunikacji VPN, zwiększa to trudność w identyfikacji osób łączących się z serwerem NAS. Chyba że jeden lub kilku z tych członków popełni błędy, które mogą prowadzić do ich identyfikacji za pomocą dozoru elektronicznego; Organy ścigania muszą stosować bardziej tradycyjne metody dochodzeniowe, aby zidentyfikować grupę terrorystyczną.

WNIOSEK

Na dzień dzisiejszy, jak widać, organizacje terrorystyczne korzystają z Internetu głównie w celu szerzenia swoich idei i komunikowania się. Jednak wraz z rozwojem technologii dostępność różnorodnych ofert na rynku podziemnym oraz malejące umiejętności wymagane do przeprowadzania cyberataków z pewnością zachęcą te grupy do wykorzystania swoich tradycyjnych ataków w cyberatakach. Widzieliśmy, że atak na wzór cyberterroryzmu jest już możliwy, ale nie jest jeszcze w zasięgu organizacji terrorystycznych, co pozostaje na poziomie zespołów lub zdolności sponsorowanych przez Tate. Choć jest to nadal bardzo ekspansywne i wymaga dużej wiedzy specjalistycznej i zasobów, za kilka lat niewątpliwie będzie w zasięgu terrorystów. W tym rozdziale widać także, że przestępcy jako pierwsi wdrażają nowe technologie nie tylko po to, aby wykorzystać te technologie dla własnych korzyści, ale także po to, aby wyprzedzić organy ścigania i regulacje. Niemniej jednak grupy terrorystyczne są bardziej ostrożne i będą raczej szukać sprawdzonych technologii lub

naśladować istniejące, opracowując własne. Wreszcie grupy terrorystyczne mogą nie być pierwszymi w zasięgu ataku przypominającego cyberterroryzm, ale raczej ekstremizm lub aktywizm (w tym haktywizm), które są bardziej skłonne do korzystania z łatwo dostępnych zasobów na nielegalnym rynku, takich jak Crimeas-a-Service i Hacker-for - wynajem, który można kupić i skoordynować w celu przeprowadzenia takich ataków.

ICT jako narzędzie ochrony przed wykorzystywaniem dzieci

WSTĘP

Cytowano wypowiedź Alberta Einsteina: „Stało się przerażająco oczywiste, że nasza technologia przekroczyła nasze człowieczeństwo". Rzeczywiście rok 2013 był rokiem znaczących odkryć na temat dominacji technologii informacyjno-komunikacyjnych w naszym życiu. Dominacja technologii komunikacji mobilnej, życie, w którym żyjemy przez całą dobę, 7 dni w tygodniu, a także zmieniające się wzorce tego, jak nawiązujemy kontakty towarzyskie, robimy zakupy, uczymy się, bawimy, komunikujemy, a nawet jak się odżywiamy i jesteśmy coraz bardziej świadomi swojego zdrowia i dobrego samopoczucia, wskazuje na to, co niektórzy chcieliby nazwać „trzecim przemysłem". Fenomenalny postęp technologii oznacza, że pojęcia takie jak prywatność i prywatne informacje są dla miliardów ludzi, którzy odważyli się wejść w sieć technologii, jedynie mirażem. Doniesienia o agencjach bezpieczeństwa na całym świecie monitorujących każdy nasz ruch cyfrowy (od wiadomości tekstowych po nasze tweety, rozmowy na Facebooku, a nawet nasze wzorce zakupów) potwierdziły, że jako jednostki nie mamy prawa, a w rzeczywistości bardzo niewiele, jeśli w ogóle, ochrony przed tymi niechcianymi i nieuzasadnione włamania. The Guardian (16 stycznia 2014 r.) doniósł, że: „Agencja Bezpieczeństwa Narodowego zbierała dziennie prawie 200 milionów wiadomości tekstowych z całego świata, wykorzystując je do wydobywania danych, w tym lokalizacji, sieci kontaktów i szczegółów karty kredytowej, zgodnie z ściśle tajnymi dokumentami…. " Kolejnym rosnącym problemem w ostatnich latach były kwestie związane z bezpieczeństwem dzieci w globalnej sieci cyfrowej. Od „cyberprzemocy" po narażenie dzieci na przemoc i pornografię, po „sieć" wykorzystywaną jako kanał handlu dziećmi i innej działalności przestępczej – rosną obawy i wyzwania dotyczące tego, w jaki sposób możemy zapewnić dzieciom bezpieczne środowisko cyfrowe. Raport opublikowany przez „Childhoo Wellbeing Research Centre" w Wielkiej Brytanii w 2011 roku stwierdza, że: „Dziewięćdziesiąt dziewięć procent dzieci w wieku 12–15 lat korzysta z Internetu, przy czym 93% dzieci w wieku 8–11 lat i 75% dzieci w wieku 5–7 lat". W raporcie podkreślono ponadto, że badanie przeprowadzone w USA wykazało, że 42% młodych ludzi w wieku 10–17 lat miało kontakt z pornografią w Internecie w ciągu jednego roku, a 66% z tego było niepożądane. W raporcie „E-Crime" Komisji Spraw Wewnętrznych Izby Gmin czytamy: „Jesteśmy głęboko zaniepokojeni faktem, że ludzie w dalszym ciągu zbyt łatwo uzyskują dostęp do nieodpowiednich treści w Internecie, w szczególności nieprzyzwoitych zdjęć dzieci… Nie ma usprawiedliwienia dla samozadowolenie. Wzywamy osoby odpowiedzialne do podjęcia bardziej zdecydowanych działań w celu usunięcia takich treści. Powtarzamy nasze zalecenie, aby rząd opracował obowiązkowy kodeks postępowania z firmami internetowymi w celu usuwania materiałów naruszających dopuszczalne standardy zachowania… [jest] ważne, aby dzieci uczyły się, jak zachować bezpieczeństwo w Internecie, tak samo jak uczą się, jak bezpiecznie przechodzić przez ulicę " (Izba Gmin ds. przestępczości elektronicznej, 2013). Chociaż pozostaje wiele do zrobienia, aby opracować ramy prawne określające, co można, a czego nie, blokować, a także wdrożyć niezbędne technologie, sama sieć szybko się rozwija i pojawiają się nowe wyzwania technologiczne. Magazyn Time (listopad 2013 r.) opublikował specjalny raport na temat tak zwanej „głębokiej sieci". Podobnie jak historia Internetu, historia „Deep Web" jest również kojarzona z wojskiem USA i badaniami prowadzonymi przez naukowca związanego z Laboratorium Badawczym Marynarki Wojennej Stanów Zjednoczonych, których celem było „ukrywanie informacji o trasach". W raporcie stwierdzono, że opracowywane

elementy: „określały cechy techniczne systemu, dzięki któremu użytkownicy mogliby uzyskać dostęp do Internetu bez ujawniania swojej tożsamości jakiemukolwiek serwerowi sieci Web lub routerom, z którymi mogliby po drodze wchodzić w interakcję". „Głęboka sieć", jak niepokojąco sugeruje raport, to miejsce, w którym przestępczość zorganizowana lub sieci terrorystyczne współpracują z zamaskowanymi tożsamościami, a także tam organizowane są narkotyki, fałszywe paszporty, wyrafinowany SPAM, prozopografia dziecięca i inna działalność przestępcza za pomocą niewykrywalnej waluty, takiej jak „Bitcoin". Biorąc zatem pod uwagę złożoność ram prawnych i stale rosnące wyzwania techniczne, jakie kluczowe kwestie musimy rozwiązać nie tylko po to, aby zapewnić dzieciom bezpieczniejszy cyfrowy świat, ale także wykorzystać samą technologię do opracowania rozwiązań?

KLUCZOWE ZAGADNIENIA I WYZWANIA

Kluczowe problemy i wyzwania stojące przed rządami, organizacjami opieki nad dziećmi i rodzicami można ogólnie podzielić na następujące kategorie:

• Informacje i świadomość problemów

• Ramy prawne i trudności związane z kwestiami transgranicznymi oraz globalnie uzgodnionymi metodami pracy

• Wyzwania techniczne (przepływ informacji, dostęp i przetwarzanie) Być może warto rozważyć, co nadrzędne ramy prawne, stosowane we wszystkich krajach, przewidują w odniesieniu do dzieci w odniesieniu do tych kluczowych kwestii. Konwencje Narodów Zjednoczonych o prawach dziecka (CRC) (ONZ, 1989) stanowią między innymi następujące postanowienia:

• Artykuł 3 – dotyczący najlepszego interesu dziecka – stanowi, że we wszystkich okolicznościach dotyczących dziecka należy się na nim skupiać w pierwszym rzędzie, niezależnie od tego, czy ma to miejsce w instytucjach publicznych czy prywatnych, czy też w środowisku prawnym lub administracyjnym. W każdej sytuacji, przy każdej decyzji dotyczącej dziecka należy rozważyć różne możliwe rozwiązania i zwrócić należytą uwagę na dobro dziecka. „Dobro dziecka" oznacza, że organy ustawodawcze muszą rozważyć, czy przyjmowane lub zmieniane przepisy przyniosą dzieciom możliwie najlepsze korzyści.

• Artykuł 16 (Prawo do prywatności): Dzieci mają prawo do prywatności. Prawo powinno chronić ich przed atakami na ich sposób życia, dobre imię, rodziny i domy. 5 Artykuł 17 (Dostęp do informacji; środki masowego przekazu): Dzieci mają prawo do informacji ważnych dla ich zdrowia i dobrego samopoczucia. Rządy powinny zachęcać środki masowego przekazu – radio, telewizję, gazety i źródła treści internetowych – do dostarczania informacji zrozumiałych dla dzieci i do niepromowania materiałów, które mogą zaszkodzić dzieciom. Należy w szczególności zachęcać środki masowego przekazu do dostarczania informacji w językach które dzieci z mniejszości i ludności tubylczej mogą zrozumieć. Dzieci powinny mieć także dostęp do książek dla dzieci.

Hick i Halpin (2001), rozważając kwestię dzieci, praw dziecka oraz postępu w zakresie „Praw dziecka w Internecie", zwracają uwagę, że prawa są zrównoważone, a nie absolutne, oraz że postęp technologiczny będzie w dalszym ciągu powodował taką samą potrzebę przeglądu i odzwierciedlać zmiany, aby chronić dzieci i zapewnić im korzyści z technologii.

ŚWIADOMOŚĆ INFORMACYJNA I LEPSZA EDUKACJA

Dostępna literatura wskazuje na fakt, że brak świadomości i przydatnych informacji na temat związanych z tym zagrożeń, a także prywatności i konsekwencji naszego zachowania dość często

prowadzi do zwiększonego ryzyka, szczególnie w przypadku dzieci i młodzieży. W badaniu przeprowadzonym przez Innocenti Research Center (IRC) i opublikowanym przez UNICEF, zatytułowanym: „Globalne wyzwania i strategie dotyczące bezpieczeństwa dzieci w Internecie", w 2011 roku wyrażono poważne obawy dotyczące braku zrozumienia zagadnień i zagrożeń związanych z korzystaniem przez dzieci z Internetu informacje o sobie są tak publicznie dostępne. W dalszej części raportu stwierdza się:

Dorośli często wyrażają obawy dotyczące zagrożeń związanych z publikowaniem informacji i zdjęć w Internecie. Dlatego też wiele badań wychodzi z założenia, że zamieszczanie informacji samo w sobie jest zachowaniem ryzykownym. Młodzi ludzie rzeczywiście publikują informacje, które dorośli mogą uznać za niepokojące. Bogactwo dowodów z całego świata pokazuje, że wielu młodych ludzi, szczególnie w wieku od 12 do 16 lat, umieszcza w Internecie bardzo osobiste dane. Na przykład badania w Brazylii wskazują, że 46 procent dzieci i nastolatków uważa za normalne regularne publikowanie osobistych zdjęć w Internecie, natomiast badanie przeprowadzone w Bahrajnie wskazuje, że dzieci często umieszczają w Internecie dane osobowe, nie rozumiejąc pojęcia prywatności.

W raporcie zauważono ponadto, że:

Ponadto znaczna liczba nastolatków przesyła swoje wizualne przedstawienia o zabarwieniu seksualnym. Czasami dzieje się tak w odpowiedzi na uwodzenie, które polega na zachęcaniu do umieszczania takich zdjęć w Internecie, po czym może nastąpić szantaż lub groźba narażenia się na zmuszenie nastolatków do przesyłania coraz większej liczby wyraźnych zdjęć. Jednak w innych przypadkach początkowe umieszczenie jest niechciane i może zachęcać i przyciągać potencjalnie agresywne drapieżniki.

Jest oczywiste, że chociaż zasięg i wykorzystanie sieci społecznościowych rośnie, a publikowanie wysoce spersonalizowanych informacji jest postrzegane jako „normalne", potrzebna jest znacznie lepsza edukacja, a także bardziej odpowiedzialne protokoły sieci społecznościowych regulujące korzystanie z dzieci.

OBOWIĄZKI RZĄDU I RAMY PRAWNE

Organizacja Współpracy Gospodarczej i Rozwoju (OECD) w raporcie opublikowanym w maju 2011 r. przyznaje, że ramy prawne i polityczne dotyczące ochrony dzieci w globalnej sieci cyfrowej są niezwykle niebezpieczne i złożone. Złożone wyzwania polityczne obejmują: jak łagodzić ryzyko bez ograniczania możliwości i korzyści dla dzieci w Internecie; jak zapobiegać zagrożeniom, zachowując jednocześnie podstawowe wartości dla wszystkich użytkowników Internetu; jak zapewnić, aby polityki były proporcjonalne do problemu i nie zakłócały warunków ramowych, które umożliwiły rozkwit gospodarki internetowej? Co więcej, rządy mają tendencję do zajmowania się wykorzystywaniem i molestowaniem seksualnym w internecie, kładąc nacisk na budowanie „architektury" mającej na celu ochronę lub ratowanie dzieci – ustanawianie przepisów, ściganie i ściganie sprawców przemocy, podnoszenie świadomości, ograniczanie dostępu do krzywdy i wspieranie dzieci w powrocie do zdrowia nadużycie lub wyzysk. Są to istotne elementy reakcji ochronnej. Warto również zauważyć, że pomimo różnych wysiłków daleko nam do uzgodnionego na całym świecie zestawu wytycznych i ram prawnych, które chronią dzieci przed poważnymi zagrożeniami, na jakie narażają się w Internecie. Najwyraźniej jest to poważna luka wykorzystywana przez przestępców i osoby, które mają żywotny interes w wykorzystywaniu obecnych „wolności" do celów osobistego monitorowania.

PROBLEMY I WYZWANIA TECHNICZNE STUDIUM PRZYPADKU ZASTOSOWANIA TECHNOLOGII I PROPONOWANEJ METODOLOGII

W badaniu przeprowadzonym przez Lannona i Halpina (2013) mającym na celu zbadanie rozwoju i realizacji programu powiadamiania o zaginionych dzieciach (MCA), inicjatywy zainicjowanej i kierowanej przez Plan International (zwanej Planem) w 2012 r., zbadano wykonalność opracowania Zbadano system oparty na technologii, który działałby jako cyfrowy system ostrzegania zapewniający wsparcie odpowiednim agencjom rządowym i pozarządowym zajmującym się handlem dziećmi w Azji Południowo-Wschodniej. Jednym z kluczowych zagadnień i wyzwań w ramach badania był sposób, w jaki klasyfikujemy zaginione dzieci. Dzieci znikają z wielu powodów. W Azji Południowej wiele osób zostaje uprowadzonych i zmuszonych do pracy przymusowej. Inni są namawiani do opuszczenia domu przez kogoś, kogo znają, po czym są wykorzystywani w handlu seksualnym lub sprzedawani do pracy w charakterze pomocy domowej. Niektórzy po prostu uciekają z domu lub są zmuszeni do opuszczenia go z powodu trudnych okoliczności, takich jak przemoc w rodzinie lub śmierć rodzica. Problem zaginięć dzieci jest również powiązany, choć nie wyłącznie, z handlem dziećmi. Jest to wysoce tajny i tajny handel, którego przyczyny są różnorodne i często złożone. Ubóstwo jest główną przyczyną, ale zjawisko to jest również powiązane z szeregiem innych czynników „wypychających" (strona podaży) i „przyciągających" (strona popytowa). Czynniki wypychające obejmują złe warunki społeczno-ekonomiczne; dyskryminacja strukturalna ze względu na klasę, kastę i płeć; przemoc domowa; migracja; analfabetyzm; klęski żywiołowe, takie jak powodzie; oraz zwiększoną podatność na zagrożenia wynikającą z braku świadomości. Czynnikami przyciągającymi są skutki gospodarki wolnorynkowej, a w szczególności reform gospodarczych generujących popyt na tanią siłę roboczą; urbanizacja; oraz żądanie, aby młode dziewczęta były wykorzystywane seksualnie i zawierały małżeństwa. Handel ludźmi to złożone zjawisko, ale wiele dzieci trafia do branży rekreacyjnej, która może obejmować pornografię, z rynkiem międzynarodowym za pośrednictwem technologii. W raporcie UNICEF z 2008 roku wskazano, że brakuje synergii i koordynacji pomiędzy planami działania a wieloma podmiotami zaangażowanymi w inicjatywy przeciwdziałające handlowi ludźmi w regionie, w tym rządami, agencjami ONZ i organizacjami pozarządowymi. Według raportu różnorodność ich mandatów i podejść sprawia, że koordynacja na poziomie krajowym i międzynarodowym jest wyzwaniem. Próby rozwiązania problemu transgranicznego handlu dziećmi okazały się szczególnie problematyczne ze względu na brak wspólnych definicji i interpretacji oraz istnienie różnych punktów widzenia na tę kwestię. Po pierwsze, nie ma powszechnie uzgodnionej definicji handlu ludźmi (UNODC, 2011). Ponadto definicja „dziecka" może się różnić, jak już zauważono. Ma to wpływ na sposób, w jaki policja, sądy i inne zainteresowane strony zajmują się prawami, potrzebami, bezbronnością dziecka i podejmowaniem decyzji. Handel dziećmi jest często postrzegany w kontekście wykorzystywania w pracy lub wykorzystywania seksualnego, przy czym to drugie skupia się przede wszystkim na kobietach i dziewczętach, ale w coraz większym stopniu może obejmować także chłopców. W niektórych przypadkach traktuje się je jako kwestię migracji lub jako podkategorię handlu ludźmi. Co więcej, władze często postrzegają to jako kwestię związaną z egzekwowaniem prawa, w związku z czym ich reakcje skupiają się głównie na ściganiu karnym i ściślejszych kontrolach granicznych. Na całym świecie najpowszechniej akceptowaną definicją handlu ludźmi jest ta zawarta w Protokole ONZ w sprawie handlu ludźmi (protokół z Palermo). Definiuje „handel ludźmi" jako:

werbowanie, transport, przekazywanie, przechowywanie lub przyjmowanie osób z zastosowaniem groźby lub użyciem siły, bądź też z zastosowaniem innych form przymusu, uprowadzenia, oszustwa, wprowadzenia w błąd, nadużycia władzy lub wykorzystania słabości, lub wręczanie lub otrzymywanie płatności lub korzyści dla uzyskania zgody osoby sprawującej kontrolę nad inną osobą, w celu wyzysku.

Jak zauważono w raporcie UNODC (2011), w przepisach krajowych w regionie Azji Południowej brakuje wspólnego rozumienia handlu ludźmi. Najczęściej stosowaną definicją jest ta przyjęta przez Konwencję SAARC dotyczącą handlu ludźmi, która, jak już wspomniano, ogranicza się do handlu w celu wykorzystania seksualnego. Niemniej jednak ważne jest, aby rządy i inne zainteresowane strony

uczestniczące w programie MCA osiągnęły wspólne zrozumienie, aby zapewnić skuteczność wysiłków w zakresie współpracy i rozwój przyszłej polityki. Przez „zaginione dziecko" rozumie się ogólnie osobę w wieku poniżej 18 lat, której miejsce pobytu jest nieznane. Definicja ta obejmuje szereg podkategorii zaginionych dzieci. Międzynarodowe Centrum ds. Dzieci Zaginionych i Wykorzystywanych (ICMEC) zidentyfikowało szereg z nich, w tym między innymi: „Zagrożona ucieczka", „Uprowadzenie przez rodzinę", „Uprowadzenie przez osobę spoza rodziny", Zagubienie, obrażenia lub zaginięcie z innego powodu oraz „ Porzucony lub małoletni bez opieki." ICMEC podkreśla znaczenie zrozumienia, co oznacza zaginięcie dziecka:

Wspólna definicja „zaginionego dziecka" zawierająca jasne kategorie ułatwia koordynację i komunikację między jurysdykcjami oraz zapewnia, że polityki i programy kompleksowo uwzględniają wszystkie aspekty kwestii zaginionych dzieci. Chociaż wszystkie przypadki zaginięcia dzieci wymagają natychmiastowej uwagi, procedury dochodzeniowe stosowane po zgłoszeniu wstępnym mogą się różnić w zależności od okoliczności sprawy.

Istnieje już obszerny zasób wiedzy na temat rejestrowania i powiadamiania o zaginionych dzieciach. Na poziomie regionalnym istnieje niezliczona ilość formatów stosowanych do opisu zaginionego dziecka. Osiągnięcie porozumienia w sprawie wspólnego, kompleksowego modelu danych, zawierającego zakodowane typologie opisujące status zaginionego dziecka, znajdujące się na nim fizyczne oznaczenia identyfikacyjne itp. zapewni spójność i konsekwentność informacji oraz ułatwi szybsze przeszukiwanie systemów. Ten model danych powinien także umożliwiać wykorzystanie danych niekodowanych, w szczególności danych fotograficznych i biometrycznych. Stosowanie zakodowanych typologii zagwarantuje, że rejestracja dzieci zaginionych i odnalezionych będzie spójna we wszystkich językach oraz że będzie można znaleźć zgodności między wpisami wprowadzonymi w różnych językach. Program MCA powinien odgrywać aktywną rolę w wysiłkach na rzecz opracowania zakodowanych typologii lub tezaurusów w celu wspierania spójnego i standardowego zgłaszania zaginięć dzieci w Azji Południowej, zgodnie z normami i najlepszymi praktykami w zakresie ochrony dzieci. Należy tego dokonać we współpracy z ICMEC, która już pracuje w wielu powiązanych obszarach badawczych.

OBIEKTYWNOŚĆ, SPÓJNOŚĆ I WIARYGODNOŚĆ

Ponadto, aby móc tworzyć sensowne statystyki, podstawowym wymogiem jest kontrolowane słownictwo. Przekształca dane dotyczące przypadków handlu dziećmi w policzalny zestaw kategorii, nie odrzucając ważnych informacji i nie wprowadzając w błąd zebranych informacji. Opracowanie standardowego modelu danych powinno być podstawą do projektowania wszelkich technologicznie wspomaganych systemów informatycznych wdrażanych w ramach inicjatywy MCA.

SYSTEMOWE PODEJŚCIE DO OCHRONY DZIECI

System to zbiór komponentów lub części zorganizowanych wokół wspólnego celu. Ponieważ celem MCA jest lepsza ochrona dzieci przed handlem ludźmi i wykorzystywaniem, można go opisać jako system ochrony dzieci. Komponenty systemu można najlepiej zrozumieć w kontekście wzajemnych relacji, a nie w izolacji. Kilka kluczowych elementów systemów ma zastosowanie do systemów ochrony dzieci. Należą do nich:

• Systemy istnieją w innych większych systemach, w strukturze zagnieżdżonej. Dzieci są osadzone w rodzinach lub krewnych, które żyją w społecznościach istniejących w szerszym systemie społecznym.

• Biorąc pod uwagę zagnieżdżony charakter systemów, należy zwrócić uwagę na koordynację interakcji powiązanych systemów, tak aby ich praca wzajemnie się wzmacniała.

• Systemy wykonują swoją pracę poprzez określony zestaw struktur i możliwości, których charakterystyka jest określona przez kontekst, w którym system działa. W przypadku transgranicznego handlu dziećmi kontekst jest różny w zależności od kraju, departamentu rządowego, a w niektórych przypadkach nawet interwencji.

• Zmiany w dowolnym systemie mogą potencjalnie zmienić kontekst, podczas gdy zmiany w kontekście zmienią system.

• Dobrze funkcjonujące systemy zwracają szczególną uwagę na pielęgnowanie i utrzymywanie aktów współpracy, koordynacji i współpracy pomiędzy wszystkimi poziomami interesariuszy.

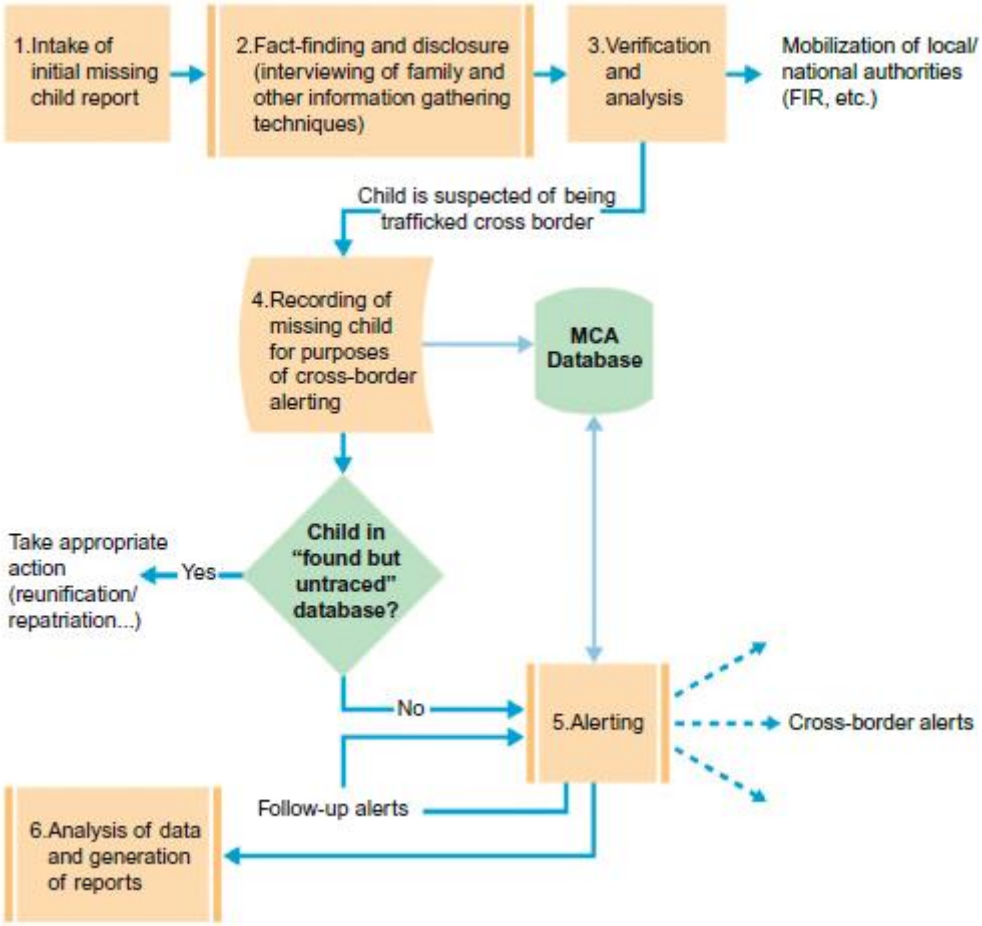
• Systemy osiągają pożądane wyniki, projektując, wdrażając i utrzymując skuteczny i wydajny proces opieki, w którym interesariusze są pociągani do odpowiedzialności zarówno za swoje indywidualne wyniki, jak i działanie całego systemu.

• Skuteczne struktury zarządzania w każdym systemie muszą być elastyczne i solidne, aby stawić czoła niepewności, zmianom i różnorodności.

Przyjęcie podejścia systemowego oznacza, że wyzwania stawiane przez inicjatywę MCA są rozpatrywane całościowo. Pod uwagę brane są role i aktywa wszystkich kluczowych aktorów, w tym rządów, organizacji pozarządowych, struktur społecznych, rodzin i opiekunów, dostawców technologii, a co najważniejsze, samych dzieci.

PRZEPŁYW INFORMACJI SKONCENTROWANYCH W DZIECIACH

Holistyczne podejście do ochrony dzieci stanowi, że transgraniczny system zarządzania informacjami o dzieciach i ochrony dzieci powinien wspierać pełen zakres działań podejmowanych w związku ze zgłoszeniem zaginięcia dziecka, co do którego istnieje podejrzenie, że padło ofiarą handlu ludźmi. Przyjmując podejście oparte na wydarzeniach, preferowane przez organizacje praw człowieka, można zidentyfikować szereg wydarzeń na wysokim szczeblu. Należą do nich między innymi: zgłoszenie zaginięcia dziecka; dziecko wyzdrowiało; odnaleziono ciało dziecka; dziecko zostaje skierowane na rehabilitację; dziecko jest bezpiecznie zintegrowane z nowym środowiskiem w kraju, w którym zostało uratowane; rozpoczęto proces repatriacji; repatriacja została zakończona/rozpoczął się proces reintegracji; a dziecko może bezpiecznie powrócić do swojej rodziny i społeczności. Każde zdarzenie wyzwala zestaw działań skoncentrowanych na dziecku i przepływów informacji, które można skonfigurować na podstawie szczegółów zdarzenia i kontekstu, w którym zdarzenie ma miejsce. Rysunek 11.1 opisuje przepływ informacji, który powinien mieć miejsce w kraju źródła w przypadku pierwszego zdarzenia w procesie, czyli zgłoszenia zaginięcia dziecka.

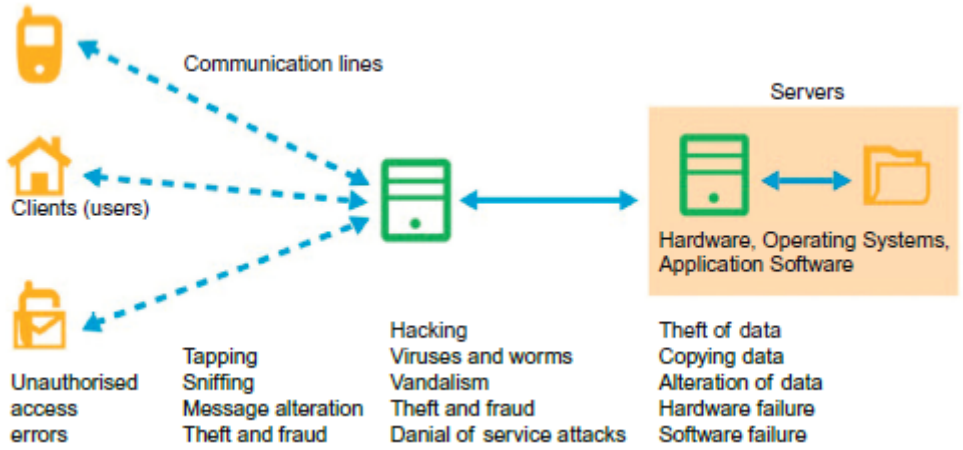


Pokazuje serię sześciu podstawowych działań, które powinny nastąpić w następujący sposób:

Przyjęcie wstępnego zgłoszenia zaginięcia dziecka. Dzieje się tak, gdy członek rodziny zgłasza się na policję lub inną instytucję, aby zgłosić zaginięcie dziecka.

Analizą i weryfikacją informacji dotyczących zaginionego dziecka powinna zajmować się policja w państwie źródła, natomiast rejestracją dziecka będącego ofiarą handlu ludźmi, wysyłaniem komunikatów ostrzegawczych, a następnie analizą danych i generowaniem raportów okresowych może zająć się policja regionalny transgraniczny system reagowania. Procesy raportowania i alarmowania można wdrożyć jako jeden system technologiczny o odrębnej funkcjonalności i rolach użytkowników. Funkcjonalność i interfejsy użytkownika systemów zgłaszania, rejestrowania i ostrzegania należy określić w drodze dyskusji z kluczowymi stronami zainteresowanymi, w szczególności z policją, która będzie rejestrować i inicjować powiadomienia w przypadku zaginionego dziecka. Chociaż nieuchronnie spowolni to proces wdrażania, niezastosowanie się do tego może spowodować, że system nie zostanie zaakceptowany przez władze, od których zależy jego powodzenie. Oznacza to, że niezbędne jest wsparcie państwa dla koncepcji i ich zaangażowanie od samego początku, podobnie jak organizacje pozarządowe znajdujące się wzdłuż prawdopodobnych szlaków tranzytowych. Musi także zaplanować powiadomienia uzupełniające, jeśli po pewnym czasie dziecko nie zostanie odnalezione/uratowane. Konfiguracja harmonogramu alertów jest istotnym elementem systemu, którego wymaga fachowego zrozumienia. Kwestią wymagającą dalszej dyskusji z zainteresowanymi stronami jest kwestia powiadamiania o dzieciach, które zostały zgłoszone jako zaginione i mogły stać się przedmiotem handlu ludźmi lub uprowadzonych na terenie kraju. Sprawami tymi mogłyby zająć się wewnętrzne systemy policyjne. Alternatywnie transgraniczny system

reagowania można zaprojektować tak, aby wspierał reagowanie na handel wewnętrzny. Proponowany system reagowania CBCT (scentralizowany transgraniczny ruch dzieci) powinien ograniczać swoje działania do tych, które wymagają komunikacji i współpracy transgranicznej. Oznacza to, że powinien wspierać przepływ informacji dotyczących dzieci będących ofiarami handlu ludźmi, które mogły zostać przewiezione przez granicę, dzieci odnalezionych, których tożsamość nie jest znana (co doprowadziło do przeszukania istniejących baz danych, w tym bazy danych odpowiedzi CBCT) oraz dzieci uratowanych, których potrzeby mogą zostać najlepiej rozwiązać poprzez repatriację i ponowne zjednoczenie. Jak zachowują się handlarze i jakie są ich trasy. Ponadto skorzysta na proaktywnym podejściu, w ramach którego identyfikuje się odbiorców ostrzeżeń wraz z najodpowiedniejszymi sposobami ich ostrzegania. Na potrzeby tych prac należy zarządzać kontrolowaną bazą danych odbiorców ostrzeżeń. Powszechnie przyjmuje się, że pierwsze godziny po zabraniu dziecka dają najlepsze możliwości ratunkowe. Dlatego istotne jest, aby powiadomienia ostrzegawcze były wysyłane tak szybko, jak to możliwe, do władz i organizacji pozarządowych znajdujących się wzdłuż prawdopodobnej trasy handlu ludźmi. Jednakże zaletę natychmiastowego powiadamiania należy zrównoważyć koniecznością zapewnienia prawdziwości zgłoszenia zaginięcia dziecka. Co ważniejsze, decyzja o wysłaniu powiadomienia ostrzegawczego musi uwzględniać bezpieczeństwo, dobro i godność dziecka. Podstawową zasadą przyjętą w systemach powiadamiania o zaginięciu dziecka na całym świecie jest to, że odbiorcy muszą dysponować wystarczającymi informacjami, aby móc zareagować na powiadomienie. Chociaż większość alertów można zautomatyzować, poprzednie działania mogą być wspomagane technologią, ale w dużej mierze opierają się na działaniu człowieka. Proces decyzyjny prowadzący do wydania ostrzeżenia musi być jasno zdefiniowany i zrozumiany. Wiele zainteresowanych stron MCA jest zdania, że pomocny byłby system koordynacji wszystkich działań związanych z ratowaniem, rehabilitacją, repatriacją i reintegracją ofiar handlu transgranicznego. Z badania wynika, że MCA miałby odgrywać rolę w aktywnym wspieraniu ścigania. Chociaż wszystko to jest pożądane, próba koordynowania wszystkich tych działań w jednym systemie technologicznym lub bazie danych jest zbyt ambitna i niepotrzebna. Zamiast tego należy wzmocnić systemy krajowe (krajowe), aby uwzględnić takie obszary, jak dobro dzieci i wymiar sprawiedliwości. Każda sprawa zarejestrowana w transgranicznym systemie reagowania powinna pozostać otwarta do czasu uzyskania informacji, że prawa i potrzeby dziecka zostały w pełni zaspokojone. Może to zająć wiele lat i może obejmować szereg interwencji, w tym schronisko .



W raporcie wyciągnięto wniosek wskazujący zapotrzebowanie na rozwiązanie technologiczne i przedstawiono strategię jego dostarczenia, ale przypomniano o złożonym otoczeniu społecznym, gospodarczym, prawnym i politycznym, w którym taka technologia musi zostać wdrożona i zostanie wdrożona. To rozpoznanie prowadzi nas z powrotem do trzech kluczowych kwestii zidentyfikowanych na wstępie.

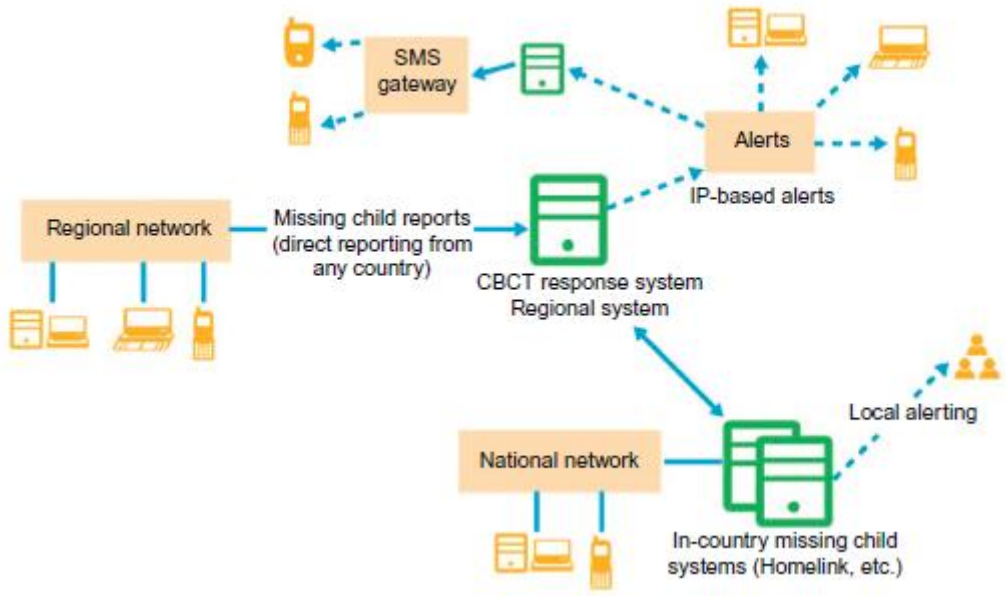
• Informacje i świadomość problemów

• Ramy prawne i trudności związane z kwestiami transgranicznymi oraz globalnie uzgodnionymi metodami pracy

• Wyzwania techniczne (przepływ informacji, dostęp i przetwarzanie)

SYSTEM REAGOWANIA CBCT

Jedną z opcji rozważanych w badaniu był scentralizowany system reagowania CBCT mający na celu zaspokojenie potrzeb dzieci będących ofiarami handlu ludźmi przez granicę. W tym celu należy uruchomić regionalną bazę danych zawierającą skuteczne krajowe mechanizmy ostrzegania. Mieszkańcy, domy kultury itp. mogą zgłaszać zaginięcia dzieci; są one początkowo badane przez policję w państwie źródła, która następnie może uruchamiać krajowe i transgraniczne wnioski o alerty za pośrednictwem scentralizowanego systemu regionalnego na podstawie analizy zgłoszenia zaginięcia dziecka. Model ten skupia się w szczególności na transgranicznym handlu dziećmi. Program MCA wdrożyłby i uruchomiłby system regionalny umożliwiający rozwiązanie tego problemu w skoordynowany sposób. Ten regionalny system reagowania CBCT zajmowałby się sprawą każdego dziecka od wstępnego logowania do repatriacji uratowanego dziecka.



Przewiduje się, że ten system regionalny będzie działał w następujący sposób:

1. Bezpieczny, scentralizowany serwer rejestruje zaginione (handel) dzieci. W systemie tym można również rejestrować znalezione dzieci. Alternatywnie znalezione dzieci można rejestrować w systemach krajowych, które w razie potrzeby będą sprawdzane przez system reagowania CBCT.

2. Interfejsy przeglądarki internetowej do wstępnego zgłaszania, aktywacji alarmów i zarządzania nimi (przez policję lub inną upoważnioną instytucję) oraz dostarczania aktualizacji związanych ze wstępnym poszukiwaniem i statusem zaginionego dziecka. Mimo że zaginięcie dziecka można zgłosić za pośrednictwem interfejsu internetowego, należy je sprawdzić (przez policję), zanim zostanie ono potwierdzone i zaakceptowane jako ważny dokument dotyczący zaginięcia dziecka.

3. Dane dziecka pozostają dostępne w systemie do czasu pomyślnej repatriacji dziecka (kiedy dziecko może mieć ukończone 18 lat).

4. Baza danych odbiorców ostrzeżeń prowadzona jest przez koordynatora systemu, a dla każdego wpisu o zaginięciu dziecka może zostać utworzony harmonogram wpisów przez upoważnionego agenta (np. określonych funkcjonariuszy policji uprawnionych do dokonywania wpisów). Przynajmniej w pierwszej fazie alarmowanie opiera się na adresie IP i może składać się z:

A. powiadomienia e-mailowe;

B. Kanały informacyjne RSS;

C. Przesyłanie danych w formacie XML do systemów partnerskich. Mogą one obejmować media nadawcze, krajowe/lokalne systemy osób zaginionych oraz sieci, takie jak policja i policja kolejowa w Indiach.

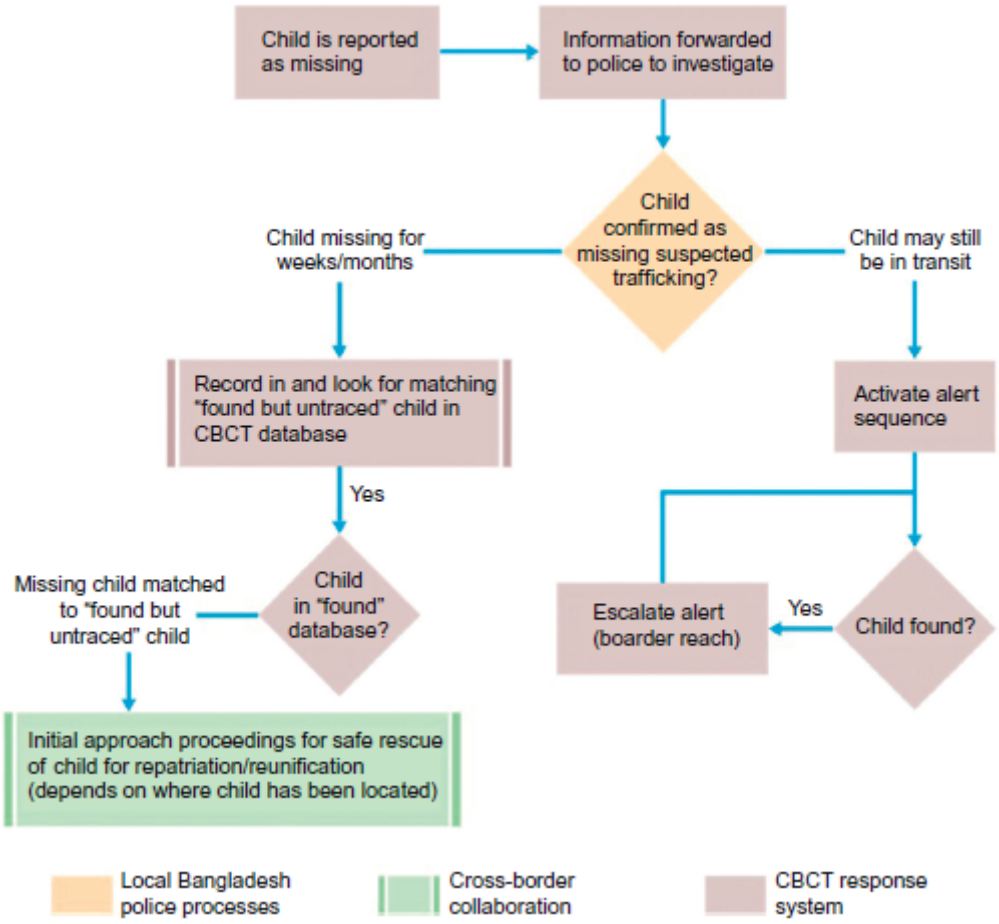
Powiadamianie oparte na protokole IP może być realizowane przez scentralizowany system regionalny hostowany w dowolnej części świata. Jeśli jednak alarmowanie odbywa się za pomocą wiadomości głosowych lub SMS-ów, ze względu na koszty należy je inicjować w kraju. Wymagałoby to: a) odzwierciedlenia transgranicznej bazy danych ostrzeżeń w każdym z trzech krajów, przy czym powiadomienia byłyby wysyłane z lokalnie odzwierciedlanych miejsc; lub b) alarmowanie lokalne realizowane przez lokalnych agentów lub węzły w każdym z krajów. Te lokalne węzły ostrzegawcze mogą otrzymywać informacje o alertach pocztą elektroniczną itp. i odpowiadać, wysyłając wiadomość SMS za pomocą własnego oprogramowania bramy lub wykonując połączenia telefoniczne.

5. Zostaną udostępnione łącza do krajowych systemów śledzenia dzieci w Nepalu i Bangladeszu (jeśli/kiedy takie istnieją), a także do innych systemów partnerskich, takich jak Homelink i system osób zaginionych AP-NIC), aby:

A. Dane mogą być z nich automatycznie przekazywane do systemu regionalnego, jeśli zaginięcie dziecka zostało już odnotowane.

B. W poszukiwaniu zgłoszonego zaginięcia dziecka można przeszukiwać krajowe/lokalne bazy danych partnerów. Wyszukiwanie zaginionych dzieci można przeprowadzić z/do systemów krajowych (takich jak na przykład Homelink).

Program MCA musi aktywnie zachęcać potencjalnych partnerów do otrzymywania ostrzeżeń i podejmowania działań w związku z nimi, zaczynając od proponowanych okręgów objętych projektem pilotażowym. Należy zauważyć, że system regionalny nie zastępuje systemów zarządzania sprawami wykorzystywanych przez policję, podmioty świadczące usługi w zakresie opieki nad dziećmi, infolinie, domy schronisk lub inne zainteresowane strony, ani nie zastępuje krajowych systemów poszukiwania zaginionych dzieci/osób. Jest to odrębny system, który koncentruje się na transgranicznym handlu dziećmi, a w szczególności na koordynacji akcji ratowniczych i repatriacji. Typowy scenariusz zgłoszenia zaginięcia dziecka przedstawiono na rysunku.



Zalety opcji scentralizowanej to:

1. Nie jest to uzależnione od wdrożenia krajowych systemów dotyczących zaginionych dzieci. Aby interwencja zakończyła się sukcesem, nadal wymaga wsparcia i współpracy ze strony władz, ale system technologiczny można wdrożyć niezależnie od nich. Prawdopodobnie doprowadzi to do szybszego wdrożenia i lepszej koordynacji działań we wszystkich trzech krajach.

2. Ponieważ powiadomienia o alertach są kontrolowane centralnie, reakcja na zgłoszenie zaginięcia dziecka może być skoordynowana i mieć szeroki zasięg. Możliwe jest np. takie skonfigurowanie bazy powiadomień, aby wysyłała powiadomienia według z góry ustalonego harmonogramu (np. natychmiast do BGB w Bangladeszu, do policji kolejowej i innych osób na znanych trasach tranzytowych w Indiach po określonej liczbie godzin, oraz później zaufanym organizacjom działającym w prawdopodobnych miastach docelowych).

3. Podobnie jak w przypadku opcji 1, może to wymagać opracowania i wdrożenia standardowych procedur operacyjnych w celu obsługi przepływu informacji i współpracy między rządami. Jednakże wymiana informacji ma większe szanse powodzenia, jeśli jest koordynowana na poziomie regionalnym.

4. Z czasem system będzie dostarczał dokładnych danych dotyczących transgranicznego handlu dziećmi.

Niektóre z zagrożeń/wad to:

1. Bez krajowych systemów wykrywania zaginionych dzieci lub pewnych mechanizmów umożliwiających skuteczne, skoordynowane reagowanie przez władze Nepalu i Bangladeszu, a także

bez krajowego systemu w Indiach, model ten ma ograniczone możliwości w zakresie przekazywania ostrzeżeń wśród policji, straży granicznej, policja kolejowa itp.

2. Zarządzanie i działanie systemu reagowania CBCT wymaga znacznych zasobów, które program MCA musiałby zapewnić.

3. Istnieje ryzyko, że system będzie postrzegany jako inicjatywa prywatna, co może utrudniać zaangażowanie rządów i udział władz państwowych.

4. Koszty związane z wdrożeniem regionalnego systemu reagowania CBCT zależą przede wszystkim od komponentów technologicznych użytych do jego budowy oraz miejsca/sposobu jego hostowania. Przyjmując takie samo podejście, jakie zastosowano w przypadku krajowych systemów śledzenia zaginionych dzieci, oczekuje się, że całkowity koszt posiadania wyniesie około 400 000 USD w ciągu trzech lat fazy pilotażowej.

WNIOSKI

Postęp technologii i społeczeństwa niesie ze sobą, jak zawsze, zarówno zagrożenia, jak i możliwości; odkrywając ogień i wykorzystując go dla korzyści, zawsze istniała możliwość zagrożenia w postaci użycia lub złośliwego użycia. Możemy rozszerzyć tę analogię na dzisiejszą technologię, ale istnieje wyraźna potrzeba zajęcia się wszechobecnością dostępu i mechanizmów zastosowania, jakie zapewnia technologia. Organizacja Narodów Zjednoczonych, jako głos społeczności międzynarodowej, artykułuje prawa zarówno do informacji, jak i do prywatności, z nadrzędnym prawem do ochrony. Obejmuje to prawo do informacji i świadomości zagadnień, którymi zajęli się między innymi Hick i Halpin (2001). Chociaż przedstawione wcześniej studium przypadku ilustruje wyzwania techniczne i równie złożone kwestie społeczne, którymi należy się zająć jednocześnie, stawiając czoła wyzwaniom technicznym; studium przypadku rzuca światło na te kwestie i może być postrzegane jako przykład wielu innych zagadnień technicznych, kwestie wymagające rozwiązania, jeśli spojrzymy na pojawiające się technologie, wykorzystywanie dzieci i możliwe wykorzystanie ICT do ochrony. Konkluzja badania stwierdza, że

Systemy technologiczne mające rozwiązać problem handlu transgranicznego należy postrzegać jedynie jako część rozwiązania. Aby były skuteczne, należy wprowadzić niezbędne rozwiązania prawne i instytucjonalne, a także rozwiązania polityczne i administracyjne, aby mogły działać.

Ta ostatnia kwestia dotycząca ram prawnych, pracy transgranicznej i wyraźnego stosowania konwencji międzynarodowych, takich jak Konwencja ONZ o prawach dziecka, wydaje się na tym etapie najtrudniejsza do rozwiązania, a jednocześnie najważniejsza, jeśli konieczne jest skuteczne przyjęcie ochrony dzieci; technologia może dostarczyć odpowiedzi, ustawodawstwo i wola polityczna muszą to ułatwić.

Klasyfikacja i charakterystyka cyberprzestępczości

WSTĘP

Nowe cechy przestępczości powstałe w wyniku działania cyberprzestrzeni stały się znane jako cyberprzestępczość. Cyberprzestępczość rośnie, a obecne modele techniczne jej zwalczania są nieskuteczne w powstrzymywaniu wzrostu cyberprzestępczości. Wskazuje to, że w celu ograniczenia cyberprzestępczości potrzebne są dalsze strategie zapobiegawcze. Tak jak ważne jest zrozumienie cech charakterystycznych przestępców, aby zrozumieć motywy stojące za przestępstwem, a następnie opracować i wdrożyć strategie zapobiegania przestępczości, ważne jest również zrozumienie ofiar, tj.

cech użytkowników systemów komputerowych, aby aby zrozumieć, w jaki sposób ci użytkownicy stają się ofiarami cyberprzestępczości. Terminu „cyberprzestępczość" używa się do opisania szeregu różnych koncepcji o różnym stopniu szczegółowości. Czasami i w najszerszym zakresie termin ten jest używany w odniesieniu do wszelkiego rodzaju nielegalnych działań, które skutkują stratą pieniężną. Obejmuje to przestępstwa z użyciem przemocy przeciwko osobie lub jej mieniu, np. z użyciem broni, rabunek, wandalizm lub szantaż. W najszerszym ujęciu termin h jest używany wyłącznie w odniesieniu do przestępstw nie związanych z przemocą, które skutkują stratą pieniężną. Obejmuje to przestępstwa, w przypadku których strata finansowa była niezamierzoną konsekwencją działań sprawcy lub gdy sprawca nie miał zamiaru osiągnięcia korzyści finansowej dla siebie lub podmiotu powiązanego. Na przykład, gdy sprawca włamuje się do komputera banku i przypadkowo lub celowo usuwa dane z konta niepowiązanego deponenta. Wall (2007) twierdzi, że aby zdefiniować cyberprzestępczość, musimy zrozumieć wpływ technologii informacyjno-komunikacyjnych na nasze społeczeństwo oraz sposób, w jaki zmieniły one nasz świat. Cyberprzestrzeń dzięki swoim unikalnym cechom stwarza przestępcom nowe możliwości popełniania przestępstw. Cechy te są postrzegane przez Wall (2005) jako „klucze transformacyjne" i są następujące:

1. „Globalizacja", która zapewnia przestępcom nowe możliwości przekraczania konwencjonalnych granic.

2. „Sieci rozproszone", które generują nowe możliwości wiktymizacji.

3. „Synoptyzm i panoptyzm", które wzmacniają zdolność zdalnego nadzoru nad ofiarami.

4. „Ślady danych" stwarzające dla przestępców nowe możliwości popełnienia kradzieży tożsamości.

Aby w pełni zrozumieć, w jaki sposób Internet stwarza dla przestępców nowe możliwości popełniania nowych cyberprzestępstw, Wall (2005) opracował matrycę cyberprzestępczości, która ilustruje różne poziomy możliwości, jakie zapewnia każdy rodzaj przestępstwa. Istnieją trzy poziomy wpływu Internetu na możliwości przestępcze, jak pokazano na osi Y tabeli. Po pierwsze, Internet stworzył więcej możliwości dla tradycyjnych przestępstw, takich jak phreaking, chipowanie, oszustwa i prześladowanie. Tego rodzaju przestępstwa istniały już w świecie fizycznym lub „prawdziwym", ale Internet umożliwił wzrost wskaźnika i rozpowszechnienia tych przestępstw. Tradycyjne gangi przestępcze wykorzystują Internet nie tylko do komunikacji, ale także jako narzędzie do popełniania „klasycznych" przestępstw, takich jak oszustwa i pranie pieniędzy, w sposób bardziej efektywny i przy mniejszym ryzyku. Po drugie, wpływ Internetu stworzył nowe możliwości dla tradycyjnej przestępczości, takie jak crackowanie/hakowanie, wirusy, oszustwa na dużą skalę, handel płcią w Internecie (seks) i mowa nienawiści. Hakowanie to tradycyjna udokumentowana forma popełniania przestępstw przeciwko CIA (poufność, integralność i dostępność). Jednakże ostatnie zmiany obejmują przetwarzanie pasożytnicze, w ramach którego przestępcy wykorzystują szereg zdalnych komputerów do wykonywania operacji, w tym przechowywania nielegalnych danych, takich jak zdjęcia pornograficzne lub piracki oprogramowanie. Po trzecie, wpływ Internetu jest tak ogromny, że stworzył nowe możliwości pojawienia się nowych rodzajów przestępstw, takich jak spam, odmowa usługi, piractwo własności intelektualnej i oszustwa na aukcjach elektronicznych. Istnieją cztery rodzaje przestępstw: związane z uczciwością (szkodliwe naruszenie); związane z komputerem (kradzież/oszustwo nabycia); merytoryczny (wulgaryzmy); i związane z treścią (przemoc). Jak argumentuje Wall, dla każdego rodzaju tych przestępstw istnieją trzy poziomy szkody: najmniejszy; środek; i najbardziej szkodliwe. Na przykład w przypadku typu związanego z integralnością (szkodliwe wtargnięcie) phreaking i chipowanie są najmniej szkodliwe, podczas gdy najbardziej szkodliwe są odmowa usługi i wojna informacyjna.

CZYM JEST CYBERPRZESTĘPCZOŚĆ?

W ostatnich latach wiele dyskusji dotyczyło natury przestępczości komputerowej i sposobów jej zwalczania. Istnieje zamieszanie co do zakresu przestępczości komputerowej, debata na temat jej zasięgu i powagi oraz obawy co do tego, gdzie leży nasza siła, aby ją pokonać. Istnieje wiele dostępnych dokumentów politycznych i badań, które dotyczą zmian charakteru wojny wraz z pojawieniem się powszechnej technologii komputerowej. Wall w 2005 r. zadał pytania dotyczące tego, co rozumiemy pod pojęciem „cyberprzestępczość", argumentując, że samo to pojęcie w rzeczywistości nie oznacza nic więcej, jak tylko oznacza występowanie szkodliwego zachowania, które jest w jakiś sposób powiązane z komputerem i nie ma konkretnego odniesienia według prawa. Ponad 10 lat później ten argument jest nadal aktualny w przypadku wielu krajów, które nadal mają w swoich konstytucjach bardzo niejasne koncepcje dotyczące cyberprzestępczości. Ten brak jasności definicji jest problematyczny, ponieważ wpływa na każdy aspekt zapobiegania i zaradzania, podczas gdy liczba osób i firm dotkniętych różnymi rodzajami postrzeganej cyberprzestępczości „rośnie bez oznak spadku". Komisarz Metropolitan Police Sir Bernard Hogan-Howe w swoim komentarzu opublikowanym w dzienniku „Evening Standard" w listopadzie 2013 r. podkreślił, że w latach 2012–2013 liczba zgłoszeń dotyczących cyberprzestępczości wzrosła o 60%. W tym samym roku finansowym cyberprzestępczość i inne rodzaje oszustw kosztowały brytyjską gospodarkę 81 miliardów funtów. „Przestępcy zdali sobie sprawę, że oszustwa internetowe mogą przynieść ogromne korzyści, podczas gdy ryzyko aresztowania jest znacznie mniejsze niż w przypadku na przykład uzbrojonych rabusiów" (Hogan-Howe, 2013). W przeciwieństwie do tradycyjnych przestępstw popełnianych w jednym miejscu geograficznym, cyberprzestępczość popełniana jest w Internecie i często nie jest wyraźnie powiązana z żadnym położeniem geograficznym. Dlatego konieczna jest skoordynowana globalna reakcja na problem cyberprzestępczości. Wynika to w dużej mierze z faktu, że istnieje szereg problemów, które utrudniają skuteczne ograniczanie cyberprzestępczości. Niektóre z głównych problemów wynikają z niedociągnięć technologii, prawodawstwa i cyberkryminologii. Wiele perspektyw kryminologicznych definiuje przestępczość na podstawie cech społecznych, kulturowych i materialnych oraz postrzega przestępstwa jako mające miejsce w określonym miejscu geograficznym. Ta definicja przestępstwa pozwoliła na scharakteryzowanie przestępczości, a następnie dostosowanie metod zapobiegania przestępczości, mapowania i pomiaru przestępczości do konkretnej grupy docelowej. Jednak tej charakterystyki nie można przenieść na cyberprzestępczość, ponieważ środowiska, w którym dochodzi do cyberprzestępczości, nie można przypisać do lokalizacji geograficznej ani do wyróżniających się grup społecznych lub kulturowych. Na przykład tradycyjne przestępstwa, takie jak znęcanie się nad dziećmi i gwałt, pozwalają na scharakteryzowanie napastnika na podstawie cech przestępstwa, w tym określenia statusu społecznego napastnika, położenia geograficznego w obrębie kraju, stanu, okręgu, miejskich lub wiejskich obszarów mieszkalnych , i tak dalej. Jednak w przypadku cyberprzestępczości nie można dokonać takiej charakterystyki atakującego, ponieważ Internet jest „antyprzestrzenny". W rezultacie identyfikacja lokalizacji o charakterystycznych cechach sprzyjających przestępstwom jest w przypadku cyberprzestępczości prawie niemożliwa. To z kolei powoduje, że perspektywy kryminologiczne oparte na rozróżnieniach przestrzennych stają się bezużyteczne. Kryminologia pozwala zrozumieć motywacje przestępców poprzez analizę cech społecznych przestępców i ich rozmieszczenia przestrzennego. Na przykład ubóstwo można uznać za przyczynę przestępczości, jeśli na biednych obszarach występuje wysoki poziom przestępczości lub jeśli okaże się, że wysoki odsetek przestępców pochodzi z biednych środowisk. Kryminologia pomaga zrozumieć przyczyny przewagi przestępstw popełnianych przez osoby o określonych cechach, takie jak nadreprezentacja sprawców z grup osób marginalizowanych społecznie, ekonomicznie czy edukacyjnie. Następnie wyjaśniono, że związek między położeniem geograficznym a cechami społecznymi doprowadził do związku między przestępczością a wykluczeniem społecznym w głównym nurcie kryminologii. Jednak w przypadku

cyberprzestępczości taka korespondencja wydaje się załamywać. Jedną z najważniejszych kwestii do rozważenia jest to, że dostęp do Internetu jest nieproporcjonalnie niski wśród zmarginalizowanych grup społeczeństwa, które uznawano za wykluczone społecznie i w związku z tym bardziej skłonne do popełnienia przestępstwa. Co więcej, popełnienie cyberprzestępstwa wymaga, aby przestępca posiadał poziom umiejętności i wiedzy wyższy niż poziom umiejętności i wiedzy przeciętnego użytkownika komputera. Można zatem powiedzieć, że cyberprzestępcy to ci, którzy są stosunkowo bardziej uprzywilejowani i posiadający dostęp do Internetu, wiedzę i umiejętności na poziomie wyższym niż przeciętny człowiek. Dlatego związek między wykluczeniem społecznym a przestępczością, który był powszechnie akceptowany w tradycyjnej przestępczości, nie może być prawdziwy w przypadku cyberprzestępczości, a cyberprzestępcy są dość „nietypowi" z punktu widzenia tradycyjnych oczekiwań kryminologicznych. Dlatego obecne perspektywy kryminologii, które łączą marginalizację i wykluczenie społeczne z przestępczością, nie mają zastosowania w wyjaśnianiu motywacji stojących za cyberprzestępczością. Bez zrozumienia motywów organom ścigania i rządom trudno jest podjąć skuteczne działania w celu zwalczania cyberprzestępczości. Brytyjskie organy ścigania dzielą wszelkie przestępstwa z udziałem komputerów na jedną z trzech kategorii. Po pierwsze, komputer może stać się celem działalności przestępczej, np. gdy witryna internetowa stanie się ofiarą ataku typu „odmowa usługi" lub gdy laptop zostanie skradziony. Po drugie, komputery mogą pełnić rolę medium pośredniczącego, gdy komputer jest wykorzystywany jako narzędzie przestępstwa przeciwko firmie lub osobie, na przykład włamania się na stronę internetową w celu kradzieży dokumentów lub funduszy. Po trzecie, może pełnić funkcję pośrednika, na przykład gdy przestępcy wykorzystują komputer do działań związanych z przestępstwem, które same w sobie nie mają charakteru przestępczego, takich jak planowanie i badania. Jako medium komputer może służyć jako modus operandi przestępcy, a jako pośrednik systemy komputerowe działają jako bufor między przestępcami a ich ofiarami, wpływając na sposób popełnienia i wykonania przestępstwa. Jako ułatwienie, komputer może umożliwić komunikację pomiędzy przestępcami w globalnie dostępnej przestrzeni, która jest niemal stosunkowo natychmiastowa. Kiedy komputer pełni rolę przestępczego medium, należy wziąć pod uwagę kontakt sprawcy z ofiarą/spiskowcem, natomiast gdy pełni rolę pośrednika w przestępstwie, ułatwia kontakty między przestępcami. Często podkreśla się różnicę między tymi kategoriami, a komputer może odgrywać obie role w przypadku jednego przestępstwa, ponieważ oszustwo oparte na handlu elektronicznym w Internecie może również obejmować znaczną komunikację online między przestępcami. W 2001 r. Rada Europy (RE) przyjęła swoją Konwencję o Traktacie o cyberprzestępczości, znaną jako Konwencja Budapeszteńska, która określa kilka działań jako przestępstwa cyberprzestępcze (CoE, 2001).

• Zamierzony dostęp bez prawa do całej części dowolnego systemu komputerowego.

• Celowe przechwytywanie, bezprawnie, niepublicznych transmisji danych komputerowych.

• Celowe uszkodzenie, usunięcie, pogorszenie, modyfikacja lub zatajenie danych komputerowych bez prawa.

• Zamierzone i poważne utrudnianie funkcjonowania systemu komputerowego poprzez wprowadzanie, przesyłanie, uszkadzanie, usuwanie, pogarszanie, zmienianie lub ukrywanie danych komputerowych.

• Produkcja, sprzedaż, pozyskiwanie do użytku, import lub dystrybucja urządzeń przeznaczonych do popełnienia któregokolwiek z powyższych przestępstw lub haseł lub podobnych danych używanych do uzyskania dostępu do systemów komputerowych, z zamiarem popełnienia któregokolwiek z powyższych przestępstw.

1 marca 2006 roku wszedł w życie Protokół dodatkowy do Konwencji o cyberprzestępczości. Państwa, które ratyfikowały protokół dodatkowy, są zobowiązane do uznania za przestępstwo rozpowszechniania materiałów rasistowskich i ksenofobicznych za pośrednictwem systemów komputerowych, a także gróźb i obelg na tle rasizmu lub ksenofobii. W dodatkowej definicji wykorzystano istniejącą teorię kryminologiczną w celu wyjaśnienia, co należy rozumieć pod pojęciem przestępczości komputerowej. Gordona i in. zaadaptowali teorię rutynowej aktywności według stylu życia (LRAT) Cohena i Felsona, która stwierdza, że do przestępstwa dochodzi, gdy istnieje odpowiedni cel, brak zdolnych opiekunów i zmotywowany przestępca, aby określić, kiedy ma miejsce przestępstwo komputerowe. W ich interpretacji przestępczość komputerowa jest skutkiem tego, że przestępcy „…dostrzegają możliwości wtargnięcia do systemów komputerowych w celu osiągnięcia celów przestępczych lub wykorzystują komputery jako narzędzie przestępstwa, obstawiając, że „opiekunowie" nie posiadają środków ani wiedzy umożliwiającej zapobieganie lub wykrywanie czynów przestępczych (Gordon i Ford, 2006; Jahankhani i Al-Nemrat, 2010; Wilson i Kunz, 2004). Definicja powinna mieć na celu ochronę i wskazanie naruszeń poufności, integralności i dostępności systemów komputerowych. Każda nowa technologia stymuluje potrzebę określenia przez społeczność norm zachowania w odniesieniu do danej technologii, dlatego ważne jest rozważenie, w jaki sposób te normy powinny zostać odzwierciedlone w naszym prawie, jeśli w ogóle.

JAKIE SĄ KLASYFIKACJE I RODZAJE CYBERPRZESTĘPCZOCI?

Drugie podejście do definiowania cyberprzestępczości polega na opracowaniu schematu klasyfikacji, który łączy przestępstwa o podobnych cechach w odpowiednie grupy, podobne do tradycyjnych klasyfikacji przestępstw. Na przestrzeni lat opracowano kilka schematów. Istnieją sugestie, że istnieją tylko dwie ogólne kategorie: aktywne i pasywne przestępstwa komputerowe. Przestępstwo czynne ma miejsce wtedy, gdy ktoś używa komputera do popełnienia przestępstwa, na przykład gdy uzyskuje dostęp do zabezpieczonego środowiska komputerowego lub urządzenia telekomunikacyjnego bez zezwolenia (hakowanie). Do biernego przestępstwa komputerowego dochodzi, gdy ktoś używa komputera do wspierania i wspierania nielegalnej działalności. Przykładem może być sytuacja, gdy podejrzany o narkotyki używa komputera do śledzenia dostaw narkotyków i zysków. W literaturze szeroko kategoryzuje się cztery ogólne typy cyberprzestępczości ze względu na związek komputera z przestępstwem:

• Komputer jako cel: kradzież własności intelektualnej, kradzież informacji marketingowych (np. listy klientów, danych cenowych lub planu marketingowego) oraz szantaż na podstawie informacji uzyskanych z plików komputerowych (np. informacji medycznych, historii osobistej lub preferencji seksualnych)).

• Komputer jako narzędzie przestępstwa: oszukańcze użycie kart i kont bankomatowych, kradzież pieniędzy z rachunków rozliczeniowych, konwersyjnych lub transferowych, oszustwa związane z kartami kredytowymi, oszustwa związane z transakcjami komputerowymi (przenoszenie zapasów, sprzedaż lub fakturowanie)) oraz oszustwa telekomunikacyjne.

• Komputer ma charakter przypadkowy w związku z innymi przestępstwami: praniem pieniędzy i nielegalnymi transakcjami bankowymi, rejestrami lub księgami dotyczącymi przestępczości zorganizowanej oraz zakładami bukmacherskimi.

• Przestępczość związana z rozpowszechnieniem komputerów: piractwo/podrabianie oprogramowania, łamanie praw autorskich do programów komputerowych, podrabiany sprzęt, sprzęt i programy komputerowe działające na czarnym rynku oraz kradzież sprzętu technologicznego.

Yar (2006), który podzielił cyberprzestępczość na cztery obszary szkodliwej działalności, zamiast skupiać się na konkretnych przestępstwach, ilustruje szereg działań i zachowań. Odzwierciedla to nie tylko różne akty prawne, ale także specyficzne kierunki debaty publicznej. Cztery kategorie są następujące:

Cyberwtargnięcie: przekraczanie granic cybernetycznych do systemów komputerowych innych osób do przestrzeni, w których ustanowiono już prawa własności lub tytuły, powodując szkody, np. włamania i dystrybucję wirusów.

Cyberoszustwa i kradzieże: różne rodzaje szkód nabytych, które mogą mieć miejsce w cyberprzestrzeni. Na jednym poziomie występują bardziej tradycyjne wzorce kradzieży, takie jak oszukańcze użycie kart kredytowych i (cyber) gotówki, ale obecnie istnieją również szczególne obawy dotyczące rosnącego potencjału włamań na internetowe konta bankowe w miarę jak bankowość elektroniczna staje się coraz bardziej popularna. popularny.

Cyberpornografia: łamanie przepisów dotyczących nieprzyzwoitości i przyzwoitości.

Cyberprzemoc: brutalny wpływ działań cybernetycznych innych osób na grupy indywidualne, społeczne lub polityczne. Choć takie działania nie muszą mieć bezpośrednich przejawów, ofiara mimo wszystko odczuwa przemoc czynu i w konsekwencji może ponieść długotrwałe blizny psychiczne. Działania, o których tu mowa, obejmują cyberprześladowanie i mowę nienawiści, a także rozmowy technologiczne.

Oprócz powyższego Yar (2006) dodał nowy rodzaj działalności, jakim jest „przestępczość przeciwko państwu", opisując ją jako obejmującą te działania, które naruszają przepisy chroniące integralność infrastruktury państwa, takie jak terroryzm, szpiegostwo i ujawnianie informacji tajemnic urzędowych. Gordon i Ford (2006) podjęli próbę stworzenia ram pojęciowych, które prawodawcy będą mogli wykorzystać przy opracowywaniu definicji prawnych znaczących zarówno z technicznego, jak i społecznego punktu widzenia. W ramach swojego programu dzielą cyberprzestępczość na dwa typy:

1. Pierwszy typ ma następujące cechy:

• Z perspektywy ofiary jest to zazwyczaj pojedyncze lub odrębne zdarzenie.

• Często ułatwia to wprowadzenie do systemu komputerowego użytkownika programów stanowiących oprogramowanie przestępcze, takich jak rejestratory naciśnięć klawiszy, wirusy, rootkity lub konie trojańskie.

• Wprowadzenie może (ale nie musi) być ułatwione dzięki lukom w zabezpieczeniach.

2. Na drugim końcu spektrum znajduje się drugi rodzaj cyberprzestępczości, który obejmuje między innymi takie działania, jak prześladowanie i nękanie w Internecie, szantaż, manipulacje na giełdzie, złożone szpiegostwo korporacyjne oraz planowanie lub przeprowadzanie działań terrorystycznych online. Charakterystyka tego typu jest następująca:

• Zwykle ułatwiają to programy, które nie mieszczą się w klasyfikacji oprogramowania przestępczego. Na przykład rozmowy mogą odbywać się za pomocą komunikatorów internetowych, a klienci lub pliki mogą być przesyłane za pomocą protokołu FTP.

• Z perspektywy użytkownika zazwyczaj występują powtarzające się kontakty lub zdarzenia.

KATEGORIE CYBERPRZESTĘPNOŚCI

Wyłudzanie informacji

Jest to próba nakłonienia klientów do ujawnienia ich osobistych informacji bezpieczeństwa; numery kart kredytowych, dane kont bankowych lub inne poufne informacje, podając się w wiadomościach e-mail za wiarygodne firmy. Ich wiadomości mogą prosić odbiorców o „aktualizację", „potwierdzenie" lub „potwierdzenie" informacji o koncie. Phishing to oszustwo dwukrotne: najpierw kradnie tożsamość firmy, a następnie wykorzystuje ją do nękania konsumentów poprzez kradzież ich tożsamości kredytowej. Termin phishing (zwany także spoofingiem) wywodzi się z faktu, że oszuści internetowi wykorzystują coraz bardziej wyrafinowane przynęty, „łapiąc" informacje finansowe użytkownika i dane dotyczące haseł. Phishing staje się obecnie najpowszechniej stosowanym atakiem socjotechnicznym ze względu na fakt, że jest dość łatwy do przeprowadzenia, nie wymaga bezpośredniej komunikacji pomiędzy hakerem a ofiarą (tj. haker nie musi dzwonić do swojej ofiary, udając, że jest personel wsparcia technicznego itp.). Wysyłanie masowych wiadomości e-mail do tysięcy potencjalnych ofiar zwiększa ryzyko uzależnienia kogoś. Aby takie ataki zadziałały, zwykle składają się z trzech oddzielnych kroków:

1. Zakładanie witryny internetowej przypominającej.

2. Wysyłanie przekonująco fałszywego e-maila w celu zwabienia użytkowników na stronę podszywającą się pod tę witrynę.

3. Uzyskanie informacji, a następnie przekierowanie użytkowników do prawdziwej witryny.

W kroku 1 haker kradnie tożsamość organizacji i tworzy podobną witrynę internetową. Można to łatwo zrobić, przeglądając kod źródłowy docelowej witryny, a następnie kopiując wszystkie grafiki i linie HTML z prawdziwej witryny internetowej. Ze względu na tę taktykę nawet doświadczonemu użytkownikowi bardzo trudno byłoby dostrzec różnice. Na stronie mimicznej zazwyczaj znajduje się formularz logowania, zachęcający użytkownika do wprowadzenia tajnych danych osobowych. Po wprowadzeniu danych skrypt po stronie serwera zajmie się przesłaniem, zbierze dane i wyśle je do hakera, a następnie przekieruje użytkowników na prawdziwą witrynę internetową, aby wszystko wyglądało podejrzanie. Najtrudniejsza część ataku phishingowego, która stanowi wyzwanie dla większości hakerów, znajduje się w drugim kroku. Nie oznacza to, że jest to trudne technicznie, ale gramatycznie tak! Na tym etapie haker wyśle przekonująco fałszywy e-mail, który później zostanie wysłany przez „ducha" program pocztowy, umożliwiający hakerowi sfałszowanie adresu źródłowego wiadomości e-mail. Głównym celem tej fałszywej wiadomości e-mail jest nakłonienie użytkowników do odwiedzenia fałszywej witryny internetowej i wprowadzenia danych, które hakerzy chcieli przechwycić. Powszechnie stosowana taktyka polega na proszeniu użytkowników o reakcję w sytuacjach awaryjnych, takich jak ostrzeżenie, że klienci muszą się natychmiast zalogować, w przeciwnym razie ich konta mogą zostać zablokowane; powiadomienie, że ktoś właśnie wysłał użytkownikowi pieniądze i aby je otrzymać, musi się teraz zalogować (zwykle jest to skuteczna pułapka dla użytkowników PayPal) itp. W tej fałszywej wiadomości e-mail użytkownicy często znajdują hiperłącze, które po kliknięty, otworzy witrynę internetową mimika, aby mogli się „zalogować". Jak wspomniano wcześniej, najłatwiejszym sposobem szybkiego zidentyfikowania fałszywej wiadomości e-mail jest nie tylko sprawdzenie źródła adresu (ponieważ można go zmienić na dowolny), ale sprawdzenie gramatyki języka angielskiego w wiadomości e-mail. Może się to wydawać zaskakujące, jednak 8 na 10 fałszywych e-maili zawiera oczywiste błędy gramatyczne. Niezależnie od tego, sztuczka nadal działa. W ostatnim kroku, gdy użytkownik otworzy witrynę mimiczną i „zaloguje się", jego informacje zostaną przetworzone przez skrypt po stronie serwera. Informacje te zostaną później przesłane do hakera e-mailem, a użytkownik zostanie przekierowany na prawdziwą stronę internetową. Jednak poufność danych finansowych użytkownika lub tajne hasło zostały teraz naruszone. W związku z ostatnimi kryzysami finansowymi, fuzjami i przejęciami nastąpiło wiele zmian

miało miejsce na rynku finansowym. Zmiany te zachęciły oszustów do wyłudzania danych klientów. Kluczowe punkty to:

• Ataki socjotechniczne mają najwyższy wskaźnik skuteczności

• Zapobieganie obejmuje edukowanie ludzi na temat wartości informacji i szkolenie ich w zakresie ich ochrony

• Zwiększanie świadomości ludzi na temat działania inżynierów społecznych

• Nie klikaj łączy zawartych w wiadomości e-mail

• Wygląda na to, że oszustwo polegające na phishingu za pośrednictwem poczty e-mail istnieje w tej czy innej formie od lutego 2004 roku i wydaje się, że nadal ewoluuje, podobnie jak twórcy wirusów dzielą się i rozwijają kod.

Według globalnego badania phishingowego przeprowadzonego przez grupę roboczą ds. przeciwdziałania phishingowi opublikowanego w 2013 roku (APWG, 2013)

1. Wrażliwi dostawcy usług hostingowych nieumyślnie przyczyniają się do phishingu. Masowe naruszenia bezpieczeństwa doprowadziły do 27% wszystkich ataków phishingowych.

2. Phishing nadal kwitnie w Chinach, gdzie rosnąca klasa średnia coraz częściej korzysta z handlu elektronicznego.

3. Liczba celów phishingu (marek) rośnie, co wskazuje, że e-przestępcy spędzają czas na poszukiwaniu nowych możliwości.

4. Phisherzy w dalszym ciągu wykorzystują nieuważnych lub obojętnych rejestratorów nazw domen, rejestrów i sprzedawców subdomen. Liczba rejestrów najwyższego szczebla ma wzrosnąć pięciokrotnie w ciągu najbliższych dwóch lat.

5. Rośnie średni i średni czas sprawności ataków phishingowych.

Według raportu Symantec Intelligence Report (2013) fałszywe oferty w dalszym ciągu dominują w atakach w mediach społecznościowych, a liczba ujawnionych luk w zabezpieczeniach wzrosła o 17% w porównaniu z tym samym okresem w 2012 r.

SPAM

Inną formą cyberprzestępczości jest poczta spamowa, która jest prawdopodobnie najgłębszym efektem zdolności Internetu do przekazania niespotykanej władzy w ręce jednej osoby. Spam to masowa dystrybucja wiadomości e-mail reklamujących produkty, usługi lub programy inwestycyjne, które mogą okazać się fałszywe. Celem spamu jest oszukanie lub oszukanie klientów, aby uwierzyli, że otrzymają prawdziwy produkt lub usługę, zwykle po obniżonej cenie. Jednak przed zawarciem transakcji spamer prosi o pieniądze lub rozsądne informacje zabezpieczające, takie jak numer karty kredytowej lub inne dane osobowe. Po ujawnieniu informacji dotyczących bezpieczeństwa klient nigdy nie otrzyma wiadomości od spamera. Obecnie spamerzy rozpowszechniający złośliwy kod i wiadomości e-mail typu phishing w dalszym ciągu szukają najlepszego sposobu dotarcia do użytkowników komputerów przy użyciu inżynierii społecznej i postępu technicznego, jednak według raportu Symantec Intelligence Report (Symantec, 2012) poziom spamu w dalszym ciągu spada spadł do 68% światowego ruchu e-mail w 2012 r. z 89% najwyższego w 2010 r. W kwietniu 2012 r. ponownie do akcji powrócił spam polityczny, którego adresatami byli głównie mieszkańcy Stanów Zjednoczonych i Francji. Tematem spamu stała się także złożona sytuacja w Syrii. W 2012 r. Stany Zjednoczone

znajdowały się na drugim miejscu po Indiach pod względem pochodzenia spamu, a Chiny uplasowały się na piątym miejscu

HAKERSTWO

Hakowanie jest jedną z najczęściej analizowanych i dyskutowanych form działalności cyberprzestępczej i stanowi główny przedmiot obaw opinii publicznej związanych z zagrożeniem, jakie taka działalność stanowi dla społeczeństwa. Jasna definicja hakowania to „nieuprawniony dostęp i późniejsze wykorzystanie systemów komputerowych innych osób" (Yar, 2006). Pierwsi hakerzy pasjonowali się technologią i nieodpartą potrzebą wiedzy, jak to wszystko działa, a ich celem było wypchnięcie programów poza to, do czego zostały zaprojektowane. Słowo haker nie miało tak negatywnej konotacji, jak ma to miejsce dzisiaj. Ataki przebiegają w kilku fazach, takich jak zbieranie informacji lub rozpoznanie, skanowanie i ostatecznie przedostanie się do docelowego systemu. Gromadzenie informacji obejmuje metody uzyskiwania informacji lub otwierania luk w zabezpieczeniach. Przypomina to sposób, w jaki dokonuje się tradycyjnego rodzaju napadu. Złodziej uzyska wszystkie informacje na temat miejsca, które chce okraść, zanim podejmie próbę. W ten sposób atakujący komputer będzie próbował zdobyć informacje o celu. Inżynieria społeczna to jedna z metod wykorzystywanych przez osobę atakującą w celu uzyskania informacji. Istnieją dwie główne kategorie, do których można zaklasyfikować wszelkie próby inżynierii społecznej: oszustwo oparte na komputerze lub technologii oraz oszustwo oparte na działaniu człowieka. Podejście oparte na technologii polega na oszukaniu użytkownika, aby uwierzył, że wchodzi w interakcję z „prawdziwym" systemem komputerowym (takim jak wyskakujące okienko informujące użytkownika, że wystąpił problem z aplikacją komputerową) i nakłonienie go do podania poufnych informacji. Ludzkie podejście opiera się na oszustwie, wykorzystaniu niewiedzy ofiary i naturalnej ludzkiej skłonności do bycia pomocnym i lubianym. Zorganizowani przestępcy mają zasoby, aby pozyskać usługi niezbędnych osób. Zagrożenie przestępczością zorganizowaną i działalnością terrorystyczną staje się coraz bardziej wyrafinowane w miarę wzrostu możliwości wnikania do naszych systemów elektronicznych i systemów bezpieczeństwa, ich kontrolowania i niszczenia. Z pewnością dzisiaj poczta elektroniczna i Internet są najpowszechniej stosowanymi formami komunikacji i wymiany informacji. Z Internetu codziennie korzysta nieco ponad 2 miliardy ludzi. Gangi przestępcze „kupują" żądnych wrażeń hakerów i „dzieci skryptów", aby zapewnić im wiedzę specjalistyczną i narzędzia. Nazywa się to cyberpracą dzieci.

CYBER NĘKANIE LUB ZNĘCANIE SIĘ

Cybernękanie lub znęcanie się to wykorzystanie elektronicznych urządzeń informacyjnych i komunikacyjnych, takich jak poczta elektroniczna, komunikatory internetowe, wiadomości tekstowe, blogi, telefony komórkowe, pagery, wiadomości błyskawiczne i zniesławiające strony internetowe w celu znęcania się lub innego nękania osoby lub grupy poprzez ataki osobiste lub w inny sposób. „Przynajmniej w przypadku fizycznej bójki jest początek i koniec, ale kiedy drwiny i upokorzenie podążają za dzieckiem do jego domu, jest to „tortura" i nie ma końca" (Early, 2010). Cyberprzemoc, drwiny, obelgi i nękanie za pośrednictwem Internetu lub wiadomości tekstowych wysyłanych z telefonów komórkowych stały się powszechne wśród młodych ludzi, w niektórych przypadkach z tragicznymi skutkami. Derek Randel, mówca motywacyjny, były nauczyciel i założyciel StoppingSchoolViolence.com, uważa, że „cyberprzemoc stała się tak powszechna w nowych mediach społecznościowych, takich jak Facebook i wiadomości tekstowe, że dotknęła każdą szkołę i każdą społeczność"

KRADZIEŻ TOŻSAMOŚCI

jest to najszybciej rozwijający się rodzaj oszustwa w Wielkiej Brytanii. Kradzież tożsamości to czynność polegająca na uzyskaniu wrażliwych informacji o innej osobie bez jej wiedzy i wykorzystaniu tych

informacji do popełnienia kradzieży lub oszustwa. Internet dał cyberprzestępcom możliwość uzyskania takich informacji z baz danych firm podatnych na ataki. Umożliwiło im to również przekonanie ofiar, że ujawniają wrażliwe dane osobowe legalnej działalności; czasami jako odpowiedź na e-mail z prośbą o aktualizację informacji rozliczeniowych lub członkostwa; czasami przybiera formę aplikacji na (fałszywe) ogłoszenie o pracę w Internecie. Według Grupy Parlamentarnej All Party dostępne badania, zarówno w Wielkiej Brytanii, jak i na całym świecie, wskazują, że oszustwa dotyczące tożsamości stanowią poważny i narastający problem ze względu na eskalację i ewolucję metod zdobywania i wykorzystywania danych osobowych. W związku z tym w nadchodzących latach oczekuje się dalszego wzrostu tego wskaźnika. Jest to kwestia dostrzegana na najwyższych szczeblach władzy. Tylko w 2012 r. CIFAS, brytyjska służba ds. zapobiegania oszustwom, zidentyfikowała i ochroniła ponad 150 000 ofiar tych przestępstw związanych z tożsamością (CIFAS, 2012).

OSZUSTWO KARTAMI PLASTIKOWYMI

Oszustwo związane z kartami plastikowymi to nieuprawnione użycie kart plastikowych lub kredytowych bądź kradzież numeru karty plastikowej w celu uzyskania pieniędzy lub mienia. Według APACS (analiza działań policji i ram bezpieczeństwa społeczności), brytyjskiego stowarzyszenia płatniczego, straty z tytułu kart plastikowych w 2011 r. wyniosły 341 mln GBP, z czego 80 mln GBP wynikało z oszustw za granicą (Financial Fraction Action UK, 2012). Zwykle dotyczy to przestępców wykorzystujących dane skradzionych brytyjskich kart w bankomatach i sklepach detalicznych w krajach, które nie wprowadziły jeszcze chipa i PIN-u. Największym typem oszustwa w Wielkiej Brytanii jest oszustwo polegające na braku karty (CNP). W 2011 r. 65% całkowitych strat stanowił CNP, który wyniósł 220,9 mln GBP (spadek o 3%) (Financial Fraction Action UK, 2012). Oszustwo CNP obejmuje wszelkie oszustwa polegające na płatnościach online, telefonicznych lub wysyłkowych. Problem w zwalczaniu tego typu oszustw polega na tym, że ani karta, ani posiadacz karty nie są obecni przy kasie w sklepie. Istnieje wiele metod stosowanych przez oszustów w celu uzyskania zarówno kart, jak i ich szczegółów, takich jak phishing, wysyłanie spamu lub włamywanie się do baz danych firm, jak wspomniano powyżej.

OSZUSTWO NA AUKCJACH INTERNETOWYCH

Oszustwo na aukcjach internetowych ma miejsce wtedy, gdy zakupione przedmioty są podróbkami lub kradzionymi towarami lub gdy sprzedawca reklamuje na sprzedaż nieistniejące przedmioty, co oznacza, że towar został opłacony, ale nigdy nie dotarł. Oszuści często korzystają z usług przekazów pieniężnych, ponieważ łatwiej jest im otrzymać pieniądze bez ujawniania swojej prawdziwej tożsamości. Oszustwa aukcyjne to klasyczny przykład przestępców polegających na anonimowości w Internecie. Według oszustw związanych z działaniami z 2013 r. niektóre z najczęstszych skarg obejmują:

• Kupujący odbierający towar z opóźnieniem lub wcale

• Sprzedający nie otrzymują płatności

• Kupujący otrzymujący towary albo mniej wartościowe niż te reklamowane, albo znacząco różniące się od pierwotnego opisu

• Nieujawnienie odpowiednich informacji o produkcie lub warunkach sprzedaży.

Ci nieuczciwi „sprzedawcy" używają skradzionych identyfikatorów podczas rejestracji w serwisach aukcyjnych, dlatego ich śledzenie jest na ogół bardzo trudnym zadaniem.

METODY I NARZĘDZIA CYBERATAKU

Każda aplikacja internetowa jest potencjalnym nośnikiem robaków i innego złośliwego oprogramowania; dlatego przesyłanie wiadomości internetowych nie jest wyjątkiem. Przestępcy wykorzystują te popularne metody czatu do kradzieży tożsamości, poznając osoby, z którymi się komunikują, lub poprzez rozprzestrzenianie złośliwego oprogramowania, oprogramowania szpiegującego i wirusów. E-maile są kluczowym narzędziem w rękach przestępców. Jednym z nich jest nie tylko e-mail m najszybsze i najtańsze media służą do spamowania i phishingu, ale można je łatwo zmanipulować w celu przeprowadzenia śmiercionośnych ataków wirusowych, które w ciągu kilku minut mogą zniszczyć całą sieć korporacyjną. Niektóre wirusy są przesyłane za pośrednictwem nieszkodliwie wyglądających wiadomości e-mail i mogą działać automatycznie, bez konieczności interwencji użytkownika (np. wirus „I Love You"). Z technicznego punktu widzenia ataki na „bezpieczeństwo systemu, które można przeprowadzić za pośrednictwem poczty elektronicznej" można podzielić na następujące kategorie:

• Ataki z aktywną zawartością, które wykorzystują różne aktywne HTML (hipertekstowy język znaczników) oraz inne funkcje i błędy skryptowe.

• Ataki związane z przepełnieniem bufora, podczas których osoba atakująca wysyła plik, który jest zbyt duży, aby zmieścił się w buforze pamięci odbiorcy poczty e-mail o stałym rozmiarze, w nadziei, że nie mieszcząca się część zastąpi krytyczne informacje, a nie zostanie bezpiecznie wyrzucona.

• Ataki za pomocą skryptów powłoki — podczas których w nagłówkach wiadomości umieszczany jest fragment skryptu powłoki systemu Unix w nadziei, że niepoprawnie skonfigurowany klient poczty Unix wykona polecenia.

Programy pobierania etapowego to zagrożenia, które pobierają i instalują inne złośliwe kody na zaatakowanym komputerze. Zagrożenia te umożliwiają atakującym zmianę pobieranego komponentu na dowolny rodzaj zagrożenia, który odpowiada ich celom lub odpowiada profilowi komputera będącego celem. Na przykład, jeśli docelowy komputer nie zawiera żadnych interesujących danych, osoby atakujące mogą zainstalować trojana przekazującego spam, a nie kradnącego poufne informacje. W miarę zmiany celów atakujących mogą oni zmieniać wszelkie późniejsze komponenty, które zostaną pobrane w celu wykonania wymaganych zadań. Wirus to program lub kod, który replikuje się w innych plikach, z którymi ma kontakt. Wirus może uszkodzić zainfekowany komputer, usuwając bazy danych lub pliki, uszkadzając ważne części komputera, takie jak BIOS, lub przesyłając wiadomości pornograficzne do wszystkich osób wymienionych w książce adresowej zainfekowanego komputera. Rok 2007 był rokiem pierwszego użycia botnetów. Bot zostaje wystrzelony z robota, podczas którego cyberprzestępcy przejmują kontrolę nad komputerem ofiary bez jej wiedzy. Dzieje się tak, gdy cyberprzestępcy lub hakerzy instalują programy na komputerze celu za pośrednictwem robaka lub wirusa. Kolekcje tych zainfekowanych komputerów nazywane są botnetami. Haker lub spamer kontrolujący te botnety może wynajmować je cyberprzestępcom lub innym hakerom, co z kolei bardzo utrudnia władzom wyśledzenie prawdziwego sprawcy. W marcu 2009 roku dziennikarz BBC zbadał świat botnetów. Zespół BBC zbadał tysiące zainfekowanych koni trojańskich, głównie komputerów domowych z systemem Windows, połączonych szerokopasmowymi połączeniami internetowymi, które są wykorzystywane do wysyłania większości spamowych wiadomości e-mail na świecie, a także do ataków typu Distributed Denial of Service i szantażu wobec poczty elektronicznej. witryny handlowe. Zespołowi BBC udało się wynająć botnet składający się z ponad 21 000 komputerów na całym świecie zainfekowanych złośliwym oprogramowaniem. Botnet ten uznano za stosunkowo tani, ponieważ infekował głównie komputery w krajach mniej rozwiniętych, w których zainstalowano mniej zabezpieczeń. Keylogger to program komputerowy lub urządzenie sprzętowe służące do monitorowania i rejestrowania każdego klawisza wpisywanego przez użytkownika na klawiaturze komputera. Użytkownik, który zainstalował program lub urządzenie sprzętowe, może następnie

wyświetlić wszystkie wprowadzone przez niego klucze. Ponieważ te programy i urządzenia sprzętowe monitorują wprowadzane klucze, haker może łatwo znaleźć hasła użytkowników i inne informacje, które użytkownik może sobie życzyć i które uważa za prywatny. Keyloggery, jako narzędzie nadzoru, są często wykorzystywane przez pracodawców, aby zapewnić pracownikom korzystanie z komputerów służbowych wyłącznie w celach służbowych. Niestety, keyloggery mogą być również osadzone w oprogramowaniu szpiegującym, umożliwiając przesyłanie informacji do nieznanej strony trzeciej. Cyberprzestępcy korzystają z tych narzędzi, aby oszukać potencjalny cel, aby udostępnił swoje wrażliwe dane osobowe i przywrócił je w celu późniejszego dostępu do komputera użytkownika, jeśli uzyskane dane zawierały identyfikator celu i hasło. Co więcej, keylogger ujawni zawartość wszystkich e-maili utworzonych przez użytkownika. Istnieją również inne sposoby przechwytywania informacji o aktywności użytkownika.

• Niektóre keyloggery przechwytują ekrany, a nie naciśnięcia klawiszy.

• Inne keyloggery potajemnie włączają rejestratory wideo lub audio i przesyłają to, co przechwycą, przez Twoje połączenie internetowe.

WNIOSEK

Wszystkie kraje stoją przed tym samym dylematem, jak walczyć z cyberprzestępczością i jak skutecznie promować bezpieczeństwo swoich obywateli i organizacji. Cyberprzestępczość, w przeciwieństwie do tradycyjnych przestępstw popełnianych w jednym miejscu geograficznym, popełniana jest w Internecie i często nie jest wyraźnie powiązana z żadnym położeniem geograficznym. Dlatego konieczna jest skoordynowana globalna reakcja na problem cyberprzestępczości. Wynika to w dużej mierze z faktu, że istnieje szereg problemów, które utrudniają skuteczne ograniczanie cyberprzestępczości. Niektóre z głównych problemów wynikają z niedociągnięć technologii, prawodawstwa i cyberkryminologii. Wiele perspektyw kryminologicznych definiuje przestępczość na podstawie cech społecznych, kulturowych i materialnych oraz postrzega przestępstwa jako mające miejsce w określonym miejscu geograficznym. Ta definicja przestępstwa pozwoliła na scharakteryzowanie przestępczości, a następnie dostosowanie metod zapobiegania przestępczości, mapowania i pomiaru przestępczości do konkretnej grupy docelowej. Jednak tej charakterystyki nie można przenieść na cyberprzestępczość, ponieważ środowiska, w którym dochodzi do cyberprzestępczości, nie można przypisać do lokalizacji geograficznej ani do wyróżniających się grup społecznych lub kulturowych. W 2014 r. w Wielkiej Brytanii zostanie utworzona wiodąca na świecie jednostka do walki z przestępcami internetowymi, której zadaniem będzie zmiana sposobu, w jaki policja radzi sobie z cyberprzestępczością, jak poinformował Komisarz Metropolitan Police w listopadzie 2013 r. Cele są pięć:

1. Postawienie przed sądem większej liczby oszustów i cyberprzestępców;

2. Aby poprawić usługi dla swoich ofiar;

3. Zwiększenie pomocy i porad w zakresie profilaktyki dla osób fizycznych i przedsiębiorstw

4. Wyznaczyć więcej zespołów zajmujących się przestępczością zorganizowaną w celu powstrzymania szkód wyrządzanych przez najbardziej płodnych cyberprzestępców;

5. Zachęcić biznes i przemysł do dołączenia do determinacji policji metropolitalnej i współpracy w celu zwalczania oszustw i cyberprzestępczości.

Jest oczywiste, że tradycyjny sposób zwalczania cyberprzestępczości nie sprawdza się pomimo mnóstwa przepisów dotyczących Internetu. Dzieje się tak ze względu na dużą liczbę przestępstw w Internecie.

Cyberterroryzm: studia przypadków

WSTĘP

Jeśli przyjrzymy się jednej z kluczowych koncepcji cyberprzestrzeni – a mianowicie radzeniu sobie z zagrożeniami terrorystycznymi – odnajdziemy uzasadnienie leżące u podstaw tej koncepcji (która pojawiła się m.in. po wydarzeniach kształtujących na początku XXI wieku, takich jak Y2K bug i ataki terrorystyczne z 11 września 2001 r.) na świecie wydaje się znajdować u szczytu procesu należącego do ery postmodernistycznej i posttechnologicznej, ery pozbawionej granic dających się obronić, w której kraje są podatne na inwazję za pośrednictwem informacji , pomysły, ludzie i materiały – krótko mówiąc, otwarty świat. W tym świecie zagrożenie terroryzmem przybiera nową formę: terrorysta w odległej, odległej piwnicy, mający potencjalną zdolność do wyrządzania szkód, całkowicie zmieniając równowagę sił poprzez penetrację ważnych systemów bezpieczeństwa lub gospodarki w każdym kraju na świecie i dostępu do wrażliwych informacji lub nawet powodując zniszczenie kluczowych systemów. Nikt nie kwestionuje aktorów niepaństwowych, takich jak organizacje terrorystyczne wykorzystujące cyberprzestrzeń jako pole umożliwiające małym indywidualnym graczom wywieranie wpływu nieproporcjonalnego do ich wielkości. Ta asymetria stwarza różne zagrożenia, które w przeszłości nie przyciągały uwagi i nie prowokowały do działań głównych mocarstw. Pytanie brzmi, czy działalność tych graczy w cyberprzestrzeni stanowi zagrożenie mogące spowodować poważne i rozległe szkody, posiadające zdolność do posługiwania się cyberbronią o znaczeniu strategicznym – bronią mogącą wyrządzić na dużą skalę lub trwałe szkody tego rodzaju, które powodują systemy krytyczne upaść i „rzucić kraje na kolana". A jeśli tak, to dlaczego do takich uszkodzeń jeszcze nie doszło? Czy rzeczywistość z 11 września 2001 r. – kiedy organizacja terrorystyczna planowała atak przez dwa lata, w tym poprzez uczestnictwo w szkoleniach dla pilotów, a w końcu przy użyciu prostych nożyc do przeprowadzenia zmasowanego ataku terrorystycznego – może powtórzyć się w cyberprzestrzeni? To scenariusz, w którym organizacja terrorystyczna wysyła grupę terrorystów jako studentów na odpowiednie kierunki informatyki, uzbraja ich w dostępne dla każdego środki technologiczne i wykorzystuje je oraz nabyte przez nich zdolności do przeprowadzenia zmasowanego ataku terrorystycznego w cyberprzestrzeni realistyczny czy science-fiction? Aby odpowiedzieć na to pytanie, musimy przeanalizować kilka studiów przypadków cyberataków organizacji terrorystycznych, a następnie rozważyć, jakie zdolności może nabyć podmiot niepaństwowy i czy zdolności te mogą stanowić realne zagrożenie dla bezpieczeństwa narodowego. W tym rozdziale dokonano oceny, czy ataki organizacji terrorystycznych w cyberprzestrzeni, których skutki dotychczas były zwykle taktyczne, będą w stanie zwiększyć (a może już zwiększyły) ich zdolność do posługiwania się cyberbronią o znaczeniu strategicznym – bronią, która może zadać obrażenia na dużą skalę lub trwałe szkody tego rodzaju, które powodują upadek krytycznych systemów i „rzucają kraje na kolana". W niniejszym rozdziale skupiono się na działalności organizacji niepaństwowych mających programy i cele polityczne, nawet jeśli są one obsługiwane lub wspierane przez państwa. Rozróżnia się tę działalność od działalności prowadzonej bezpośrednio przez państwa, co wykracza poza zakres tego rozdziału, a także działalność organizacji, których cele mają głównie charakter przestępczy. Na potrzeby niniejszego rozdziału akt terrorystyczny dokonany przez organizację niepaństwową w cyberprzestrzeni będzie definiowany jako akt w cyberprzestrzeni mający na celu umyślne lub masowe wyrządzenie szkody ludności cywilnej (inne definicje cyberterroryzm). Aby ocenić działalność organizacji terrorystycznych w cyberprzestrzeni, w pierwszym etapie należy zidentyfikować motywy wykorzystania cyberprzestrzeni w ramach walki politycznej prowadzonej przez organizacje terrorystyczne. Zidentyfikowano dwa główne motywy. Pierwszym z nich jest wykorzystanie cyberprzestrzeni wspierające działalność terrorystyczną, głównie pozyskiwanie pieniędzy i rekrutów lub pranie

pieniędzy w celu sfinansowania działalności. Drugim jest wykorzystanie w cyberprzestrzeni narzędzi zapewniających faktyczny atak na cele wyznaczane przez organizacje terrorystyczne, a także wykorzystanie tego do innych środków przemocy. W tym kontekście będziemy analizować współpracę organizacji niepaństwowych z państwami, w których działają, wspierając ich działalność terrorystyczną. Drugi etap tego badania wymagał zbadania operacji terrorystycznych w cyberprzestrzeni, to znaczy operacji, których celem jest wyrządzenie umyślnej lub masowej szkody ludności cywilnej w drodze działań w cyberprzestrzeni organizacji niepaństwowych mających programy i cele polityczne, nawet jeśli są one prowadzone lub wspierane przez stany. Trzeci etap to ocena i zrozumienie możliwości, jakie organizacje terrorystyczne mogą uzyskać i dzięki którym wygenerować skuteczny i znaczący atak terrorystyczny.

STUDIUM PRZYPADKÓW – DZIAŁANIA W CYBERPRZESTRZENI PRZYPISANE ORGANIZACJOM TERRORYSTYCZNYM

Jednym z pierwszych udokumentowanych ataków organizacji terrorystycznej na państwowe systemy komputerowe był przeprowadzony przez bojowników partyzanckich Tamilskich Tygrysów na Sri Lance w 1998 r. Ambasady Sri Lanki na całym świecie tygodniami były zalewane 800 wiadomościami e-mail dziennie zawierającymi wiadomość: „ Jesteśmy Czarnymi Tygrysami Internetu i zamierzamy zakłócić wasze systemy komunikacji.” Niektórzy twierdzą, że to przesłanie wpłynęło na tych, którzy je otrzymali, siejąc niepokój i strach w ambasadach . Kilka lat później, 3 marca 2003 roku, japońska kultowa osoba Aum Shinrikyo („Najwyższa Prawda”) przeprowadziła złożony cyberatak, polegający na uzyskaniu poufnych informacji o obiektach nuklearnych w Rosji, Ukrainie, Japonii i innych krajach w ramach próby atakować systemy bezpieczeństwa informacji tych obiektów. Informacje zostały skonfiskowane, a próba ataku nie powiodła się, zanim organizacja zdążyła podjąć działania. Do ataku za pośrednictwem emisariusza doszło w styczniu 2009 roku w Izraelu. W tym przypadku hakerzy zaatakowali izraelską strukturę internetową w odpowiedzi na operację „Płynny ołów” w Strefie Gazy. Zaatakowanych zostało ponad pięć milionów komputerów. Zakłada się, że w Izraelu atak nastąpił z krajów, które wcześniej były częścią Związku Radzieckiego, i został zamówiony i sfinansowany przez Hezbollah i Hamas . W styczniu 2012 r. grupa propalestyńskich hakerów nazywających siebie „Koszmarem” spowodowała krótkotrwałą awarię giełdy papierów wartościowych w Tel Awiwie i stron internetowych El Al Airlines oraz zakłóciła działanie witryn internetowych Pierwszego Międzynarodowego Banku Izraela. Komentując to, rzecznik Hamasu w Strefie Gazy powiedział: „Przenikanie izraelskich stron internetowych otwiera nową sferę opozycji i nową wojnę elektroniczną przeciwko izraelskiej okupacji” . Wojna domowa w Syrii doprowadziła do intensywnych działań ofensywnych organizacji znanej jako Syryjska Armia Elektroniczna (SEA) – grupy internetowej złożonej z hakerów wspierających reżim Assada (studium przypadku SEA – patrz rozdział 9). Atakują przy użyciu technik odmowy usług i informacji lub włamują się na strony internetowe i zmieniają ich zawartość. Grupie udało się przeprowadzić różne szkodliwe operacje, przede wszystkim przeciwko stronom internetowym opozycji syryjskiej, ale także przeciwko zachodnim stronom internetowym. Ostatnia akcja SEA była skierowana głównie przeciwko mediom, serwisom kulturalnym i informacyjnym w zachodnich sieciach. Grupie udało się włamać do ponad 120 witryn, w tym do „Financial Times”, „The Telegraph”, „Washington Post” i „Al Arabia” (Love, 2013). Jeden z najbardziej znaczących i skutecznych ataków miał miejsce w kwietniu 2013 r., kiedy Syryjska Armia Elektroniczna włamała się na konto Associated Press na Twitterze i umieściła fałszywy „tweet” informujący, że Biały Dom został zbombardowany, a prezydent USA został ranny w ataku . Bezpośrednią konsekwencją tego ogłoszenia był gwałtowny spadek na amerykańskich rynkach finansowych i trwający kilka minut spadek indeksu Dow Jones Industrial Average . SEA jest także podejrzana o próbę penetracji systemów dowodzenia i kontroli systemów wodnych. Na przykład 8 maja 2013 r. irańska agencja informacyjna opublikowała fotografię systemu nawadniającego w kibucu Sa’ar. SEA włamała się także do witryn rozrywkowych, które obsługują

Twittera poza swoim celem, np. E! Online i The Onion, przy czym wielu przypuszcza, że jest to SEA rozkoszująca się rozgłosem i próbująca nadawać tam platformy poza swoim spektrum. W styczniu 2014 r. SEA zhakowała i zniszczyła 16 stron internetowych rządu Arabii Saudyjskiej, zamieszczając wiadomości potępiające terroryzm w Arabii Saudyjskiej, powodując wyłączenie wszystkich 16 stron internetowych . Podczas operacji Filar Obrony w Strefie Gazy w 2012 r. i w kolejnych miesiącach konflikt izraelsko-palestyński zainspirował grupę hakerów nazywającą się OpIsrael do przeprowadzania ataków na izraelskie strony internetowe we współpracy z Anonymous. Między innymi strony internetowe Kancelarii Prezesa Rady Ministrów, Ministerstwa Obrony Narodowej, Ministerstwa Edukacji, Ministerstwa Ochrony Środowiska, Israel Military Industries, Izraelskiego Centralnego Biura Statystycznego, Izraelskiego Stowarzyszenia Raka, Prezesa Urzędu Izraela (oficjalnego site) i dziesiątki małych izraelskich stron internetowych zostały dotknięte. Grupa oświadczyła, że przyczyną ataku było naruszenie przez Izrael palestyńskich praw człowieka i prawa międzynarodowego . W kwietniu 2013 r. grupa palestyńskich hakerów o nazwie Izz ad-Din al-Qassam Cyber Fighters, utożsamiana z wojskową sekcją Hamasu, przyznała się do ataku na stronę internetową American Express. Strona internetowa firmy doznała intensywnego ataku DDoS, który trwał dwie godziny i zakłócał korzystanie z usług firmy przez jej klientów. W przeciwieństwie do typowych ataków DDoS, takich jak te przeprowadzane przez Anonymous, które opierały się na sieci komputerów, które zostały spenetrowane i połączone w kontrolowany przez atakującego botnet, atak Izz ad-Din al-Qassam wykorzystywał skrypty działające na spenetrowanych serwerach sieciowych , czyli możliwość wykorzystania większej przepustowości do przeprowadzenia ataku. Wydarzenie to wpisuje się w ogólny trend zmierzający do wzmacniania zdolności cybernetycznych Hamasu, w tym poprzez udoskonalanie jego systemu gromadzenia danych wywiadowczych przeciwko IDF i groźbie wrogiego przejęcia urządzeń komórkowych personelu wojskowego, wykorzystywanych do odkrywania tajemnic. W przeciwieństwie do werbowania agentów terrorystycznych w świecie fizycznym, w cyberprzestrzeni możliwe jest znaczne zwiększenie puli uczestników działania, nawet jeśli często dadzą się oni oszukać, aby zachowywali się jak partnerzy przez organizacje terrorystyczne pod pozorem ataku na ustanowienie. Zjawisko to ilustrują ataki hakerów na cele izraelskie, które miały miejsce 7 kwietnia 2013 r., kiedy to niektórzy z napastników otrzymali wskazówki dotyczące metod i celów ataku z zakamuflowanych stron internetowych. Wykorzystywanie nastrojów antysystemowych i ogólnych nastrojów młodych ludzi wobec Zachodu lub Izraela umożliwia znaczne poszerzenie puli agentów i tworzy znaczną masę ułatwiającą operacje cyberterrorystyczne. Stwierdzono to na przykład podczas Operacji FilarDepartamentu Obrony udokumentowano ponad sto milionów cyberataków na izraelskie strony internetowe i spekulowano, że kampanią kierował Iran i jego satelity.

ANALIZA MOŻLIWOŚCI

Z reguły należy rozróżnić trzy podstawowe kategorie ataków: atak na bramę organizacji, głównie jej strony internetowe, poprzez ataki bezpośrednie, odmowę usługi lub uszkodzenie stron internetowych; atak na systemy informacyjne organizacji; i wreszcie najbardziej wyrafinowana (i złożona) kategoria — ataki na podstawowe systemy operacyjne organizacji, na przykład przemysłowe systemy sterowania. Cyberterroryzm wymierzony w kraj i jego obywateli może mieć różny poziom zaawansowania, przy czym każdy poziom wymaga zdolności zarówno pod względem technologii, jak i inwestycji dokonanej przez atakującego. Wyrządzone szkody są wprost proporcjonalne do poziomu inwestycji. Atak na bramę organizacji: Najbardziej podstawowym poziomem ataku jest atak na bramę organizacji, czyli jej witrynę internetową, która ze swej natury jest udostępniona publicznie. Najprostszy poziom cyberterroryzmu obejmuje ataki uniemożliwiające obsługę i zakłócające codzienne życie, ale nie powodujące znacznych, nieodwracalnych ani trwałych szkód. Ataki te, zwane „rozproszoną odmową usługi" (DDoS), zasadniczo powodują nasycenie określonego komputera lub usługi internetowej żądaniami komunikacyjnymi, przekraczając granice jego zdolności do odpowiadania i w ten sposób

paraliżując usługę. Odpowiednimi celami takiego ataku są m.in. banki, dostawcy usług komórkowych, operatorzy telewizji kablowej i satelitarnej oraz serwisy giełdowe (handel i wiadomości). Inną metodą ataku na bramę organizacji są ataki na serwery systemu nazw domen (DNS) — serwery używane do kierowania ruchu internetowego. Taki atak skieruje osoby poszukujące dostępu do określonej witryny lub usługi do innej witryny, do której atakujący będą starali się skierować ruch. Podobny, ale prostszy atak można przeprowadzić na poziomie pojedynczego komputera zamiast na poziomie ogólnego serwera DNS, co oznacza, że komunikacja z pojedynczego komputera będzie kierowana do witryny atakującego, a nie do rzeczywistej witryny, którą chce użytkownik surfować. Szkody spowodowane takimi atakami mogą obejmować kradzież informacji; odmowa obsługi klientów, powodująca szkody biznesowe w zaatakowanej usłudze; i szkody dla reputacji usługi. Osoba atakująca może przekierować ruch na stronę zawierającą propagandę i komunikaty, które chce zaprezentować społeczeństwu. Popularną i stosunkowo prostą metodą zniszczenia reputacji ofiary na wejściu do organizacji jest zniesławienie jej strony internetowej. Zniesławianie obejmuje umieszczanie złośliwych wiadomości na stronie głównej, umieszczanie propagandy, którą napastnicy chcą rozpowszechniać wśród szerokiego grona odbiorców, oraz niszczenie wizerunku organizacji (i biznesu) poprzez stwarzanie wrażenia, że jest ona niechroniona i podatna na potencjalne ataki. Atak na systemy informacyjne organizacji: Poziom pośredni w skali szkód w cyberprzestrzeni obejmuje ataki na systemy informacyjne i komputerowe organizacji, takie jak serwery, systemy komputerowe, bazy danych, sieci komunikacyjne i maszyny przetwarzające dane. Zaawansowanie technologiczne wymagane na tym poziomie jest większe niż wymagane w przypadku ataku na bramę organizacji. Poziom ten wymaga uzyskania dostępu do komputerów organizacji za pośrednictwem pracowników organizacji lub w inny sposób. Szkody potencjalnie spowodowane w środowisku wirtualnym obejmują uszkodzenia ważnych usług, takich jak banki, usługi komórkowe i poczta elektroniczna. Wyraźna granica oddziela opisane tutaj ataki od zagrożenia fizycznym terroryzmem cybernetycznym: zazwyczaj nie oczekuje się, że ataki te spowodują szkody fizyczne, ale poleganie na usługach wirtualnych i dostęp do nich może jednak wygenerować znaczne szkody. Jednym z takich przykładów jest atak z wykorzystaniem wirusa komputerowego Shamoon, który w sierpniu 2012 r. zainfekował komputery Aramco, saudyjskiego koncernu naftowego. W wyniku tego incydentu do systemu komputerowego Aramco wprowadzono złośliwy kod, w wyniku czego 30 000 komputerów zostało wyłączonych z działania. wynik. Mimo że atak nie wpłynął na podstawowe systemy operacyjne firmy, udało mu się unieruchomić dziesiątki tysięcy komputerów w sieci organizacyjnej, powodując jednocześnie znaczne szkody poprzez usunięcie informacji z komputerów organizacji i spowolnienie jej działania na dłuższy czas. Atak na podstawowe systemy operacyjne organizacji: Najwyższym poziomem na skali ryzyka ataku jest atak na podstawowe systemy operacyjne i operacyjne organizacji. Przykładami mogą być ataki na krytyczną infrastrukturę fizyczną, taką jak wodociągi, instalacje elektryczne, gazowe, paliwowe, systemy kontroli transportu publicznego lub systemy płatności bankowych, które uniemożliwiają świadczenie podstawowych usług przez określony czas lub, w poważniejszych przypadkach, nawet powodują fizyczne uszkodzenie szkody poprzez atak na systemy dowodzenia i kontroli zaatakowanej organizacji. W tym momencie wirtualny atak może spowodować szkody fizyczne, a jego skutki mogą być destrukcyjne. Po ujawnieniu Stuxneta wzrosła świadomość potrzeby ochrony przemysłowych systemów sterowania, ale nadal pozostaje wiele do zrobienia, zanim skuteczna ochrona zostanie faktycznie wdrożona. Grupy terrorystyczne mogą wykorzystać tę lukę, np. gromadząc grupę ekspertów w dziedzinie komputerów i automatyzacji procesów w celu stworzenia wirusa zdolnego wyrządzić szkody tym systemom.

MOŻLIWOŚCI TECHNOLOGICZNE, WYTYCZNE INTELIGENCJI I ZDOLNOŚĆ OPERACYJNA

Rozwój zdolności do ataku, czy to przez państwa, czy przez organizacje terrorystyczne, wymaga coraz silniejszego połączenia zdolności do działania w cyberprzestrzeni w trzech głównych obszarach:

możliwości technologicznych, wytycznych wywiadowczych w zakresie wyznaczania celów (generowania celów) oraz zdolności operacyjnych.

MOŻLIWOŚCI TECHNOLOGICZNE

Zdecentralizowany charakter Internetu ułatwia handel bronią cybernetyczną. W rzeczywistości wielu hakerów i handlarzy wykorzystuje te zalety i oferuje narzędzia cybernetyczne oraz usługi w zakresie ataków w cyberprzestrzeni każdemu, kto ich szuka. W ten sposób wyłonił się zróżnicowany i bardzo wyrafinowany rynek handlu produktami cybernetycznymi do różnych celów, z zakresem cen wahającym się od kilku dolarów za prosty jednorazowy atak typu „odmowa usługi" do tysięcy dolarów za wykorzystanie nieznanych luk w zabezpieczeniach i możliwości umożliwiające atakującemu przedostanie się do najlepiej chronionego systemu komputerowego. Narzędzia cybernetycznego półświatka mogą okazać się bardzo pomocne w atakach DDoS i kradzieży dużych ilości wrażliwych informacji z niewłaściwie chronionych firm (np. informacji o kartach kredytowych z niezabezpieczonych baz danych), co niemal na pewno wzbudzi niepokój opinii publicznej. Terroryści mają jednak jeszcze przed sobą długą drogę, zanim będą w stanie spowodować szkody w systemach kontroli, co jest znacznie trudniejsze niż kradzież kart kredytowych i w czym nie pomagają narzędzia cyberprzestępczości. Jeśli chodzi o opisany powyżej poziom pośredni dotyczący ataków na systemy informacyjne organizacji, wydaje się, że półświatek dysponuje narzędziami zdolnymi wspomóc cyberterroryzm. Konieczne jest pewne dostosowanie tych narzędzi, na przykład przekształcenie kradzieży informacji w ich usunięcie, ale nie jest to aż tak długi proces, a twórcy wirusów prawie na pewno zgodzą się przeprowadzić go dla organizacji terrorystycznych, jeśli będą wystarczająco zapłacony.

MOŻLIWOŚCI OPARTE NA INTELIGENCJI

Jednym z kluczowych elementów w procesie planowania cyberataku jest wybór celu lub grupy celów, których uszkodzenie wywoła efekt zamierzony przez organizację terrorystyczną. W tym celu jednostka terrorystyczna musi sporządzić listę podmiotów stanowiących potencjalne cele ataku. Technologia dostarczająca narzędzia ułatwiające realizację tego zadania jest już dostępna bezpłatnie. Konieczne jest także zmapowanie konfiguracji komputerów zaatakowanej organizacji oraz zrozumienie, które komputery są podłączone do Internetu, jakie systemy operacyjne i programy zabezpieczające są na nich zainstalowane, jakie uprawnienia posiada każdy komputer oraz za pośrednictwem jakich komputerów organizacja dowodzi można sterować systemem. Organizacje posiadające krytyczne systemy operacyjne zwykle korzystają z dwóch sieci komputerowych: jednej zewnętrznej, która jest podłączona do Internetu, i jednej wewnętrznej, która jest fizycznie odizolowana od Internetu i połączona z przemysłowymi systemami sterowania organizacji. Spis internetowy nie uwzględnia informacji o izolowanych sieciach wewnętrznych, ponieważ nie są one dostępne za pośrednictwem Internetu. Jakikolwiek atak na te sieci wymaga inteligencji, zasobów i dużego wysiłku i wątpliwe jest, aby jakiekolwiek organizacje terrorystyczne były w stanie przeprowadzić takie ataki.

MOŻLIWOŚĆ OPERACYJNA

Po zebraniu informacji wywiadowczych i stworzeniu lub zdobyciu narzędzi technologicznych do ataku, dla planistów terroryzmu cybernetycznego następuje kolejny etap operacyjny — przeprowadzenie faktycznego ataku za pomocą wektora ataku. Pojęcie to odnosi się do łańcucha działań przeprowadzanych przez atakującego, w którym każde działanie stanowi jeden krok na drodze do ostatecznego celu i który zwykle obejmuje pełną lub częściową kontrolę nad systemem komputerowym lub systemem sterowania przemysłowego. Nie można pominąć żadnego etapu wektora ataku, a aby przejść do danego kroku, należy sprawdzić, czy wszystkie poprzednie etapy zostały pomyślnie ukończone. Pierwszym etapem wektora ataku jest zwykle umożliwienie dostępu do

celu. Bardzo popularną i skuteczną metodą robienia tego w cyberprzestrzeni jest spoofing, czyli fałszerstwo. Metodę tę można wykorzystać na różne sposoby, a ich wspólnym mianownikiem jest sfałszowanie tożsamości nadawcy wiadomości, tak aby odbiorca zaufał treści i bez wahania otworzył odnośnik w wiadomości. Fałszowanie wiadomości e-mail jest metodą ataku istniejącą od wielu lat. W związku z tym opracowano przeciwko niemu środki obronne, ale napastnicy również zgromadzili doświadczenie. Przytaczać można teraz incydenty zupełnie niewinnie wyglądających wiadomości e-mail dostosowanych do ich odbiorców, zawierających informacje odnoszące się do nich osobiście lub dokumenty bezpośrednio związane z branżą, w której działają. W tych przypadkach adresy nadawców zostały sfałszowane tak, aby wskazywały na adres kolegi z pracy. Gdy tylko odbiorcy otworzyli wiadomość e-mail, nieświadomie infekowali swoje komputery wirusem. Metoda fałszerstwa może być przydatna, gdy celem jest komputer podłączony do Internetu i można do niego wysyłać wiadomości. W niektórych przypadkach tak jednak nie jest. Sieci o wysokim poziomie ochrony są zwykle fizycznie odizolowane od świata zewnętrznego, w związku z czym nie ma pomiędzy nimi fizycznego połączenia (nawet bezprzewodowego) z siecią o niższym poziomie bezpieczeństwa. W tej sytuacji atakujący będzie musiał zastosować inny lub dodatkowy środek w wektorze ataku – zainfekować sieć docelową wirusem przy użyciu urządzeń działających zarówno w sieci niechronionej, jak iw sieci chronionej. Jednym z takich przykładów jest pamięć flash USB („Disk on Key" lub „memory stick"), służąca do wygodnego, mobilnego przechowywania plików. Jeśli się powiedzie, atakujący uzyskuje dostęp do sprzętu technologicznego ofiary (komputer, PalmPilot, smartfon), a pierwszy etap wektora ataku – zapewnienie dostępu do celu – zostaje zakończony. W niektórych scenariuszach ten krok jest najważniejszy i znaczący dla atakującego. Przykładowo, jeśli celem terrorysty jest sabotaż sieci i wymazanie z niej informacji, wówczas głównym wyzwaniem jest uzyskanie dostępu do celu, czyli dostępu do sieci operacyjnej firmy. Akty kasowania i sabotażu są łatwiejsze, jeśli zaimplantowany w sieci wirus działa na odpowiednio wysokim poziomie autoryzacji. Jednakże w bardziej złożonych scenariuszach, w których terrorysta chce wyrządzić znaczne szkody i osiągnąć większe zastraszenie, konieczne są znaczne inwestycje w etapy wektora ataku, jak opisano poniżej. Na rynku ofensywnych produktów cybernetycznych terroryści znajdą dostępne możliwości dla nieodizolowanego celu. Na tym samym rynku znajdą również produkty do ataku i prawdopodobnie znajdą również produkty do przeprowadzania operacji w sieci docelowej (podobnie jak interfejs zarządzania koniem trojańskim SpyEye). Pomimo tej dostępności nie zidentyfikowano jeszcze narzędzi dostępnych w Internecie, które ułatwiałyby atak na systemy operacyjne organizacji. Dostęp do tych narzędzi jest w zasadzie możliwy (Rid, 2013), jednak zadanie to wymaga dużych zasobów kadrowych (szpiedzy, fizycy i inżynierowie), inwestycji finansowych (opracowanie narzędzia ataku i przetestowanie go na prawdziwym sprzęcie w warunkach laboratoryjnych) i dużo czasu na wykrycie luk i skonstruowanie skutecznego wektora ataku.

WNIOSEK

Niski próg wejścia w przypadku niektórych ataków oraz dostęp do narzędzi ataku cybernetycznego nie skłoniły organizacji terrorystycznych do przejścia na ataki o dużym i ciągłym potencjale szkód. Do tej pory cyberataki organizacji terrorystycznych były skierowane głównie na bramę organizacji docelowej. Głównymi narzędziami ataku były ataki typu „odmowa usługi" oraz ataki na skalę od amatorskiej do średniej, przede wszystkim ze względu na ograniczone możliwości i środki organizacji terrorystycznych w cyberprzestrzeni oraz jak dotąd brakowało im niezależnej infrastruktury naukowej i technologicznej niezbędnej do opracować narzędzia cybernetyczne zdolne do wyrządzenia znacznych szkód. Biorąc pod uwagę, że organizacje terrorystyczne nie mają możliwości gromadzenia wysokiej jakości danych wywiadowczych na potrzeby operacji, prawdopodobieństwo, że przeprowadzą one znaczący cyberatak, wydaje się niskie. Aby organizacja terrorystyczna mogła działać niezależnie i przeprowadzić znaczący atak w cyberprzestrzeni, będzie potrzebować szeregu zdolności, w tym możliwości gromadzenia precyzyjnych informacji o celu, jego sieciach komputerowych i systemach; zakup lub

rozwój odpowiedniego narzędzia cybernetycznego; znalezienie tropu do penetracji organizacji; kamuflowanie narzędzia ataku podczas przejmowania systemu; oraz przeprowadzenie ataku w nieoczekiwanym czasie i miejscu i osiągnięcie znaczących rezultatów. Wydaje się, że niezależne działanie organizacji terrorystycznej bez wsparcia państwa nie jest oczywiste. Tego samego wniosku nie można jednak wyciągnąć w przypadku organizacji wspieranych, a nawet prowadzonych przez państwa posiadające znaczące zdolności. Istnieje także możliwość ataków organizacji terrorystycznych poprzez outsourcing. Grupa hakerów o nazwie Icefog koncentruje się na ukierunkowanych atakach na łańcuch dostaw organizacji (przy użyciu metody „uderz i uciekaj"), głównie w branżach wojskowych na całym świecie. Jest to przykład outsourcingu cyberataków (Kaspersky, 2013). Kolejnym osiągnięciem jest dystrybucja złośliwych kodów z wykorzystaniem laboratoriów kryminalnych sieci DarkNet, co zwiększyło dostęp do istniejących kodów na potrzeby ataków. Organizacje przestępcze już wykorzystują istniejące kody do ataków na systemy finansowe, powielając je i przekształcając w kody mutacyjne. Z jednej strony wachlarz możliwości i środków, którymi dysponują organizacje terrorystyczne w cyberprzestrzeni, jest ograniczony ze względu na jego silną korelację z dostępnością technologiczną, która zwykle leży w zasięgu krajów o zaawansowanych możliwościach technologicznych i firm o znaczących możliwościach technologicznych. Z drugiej strony dostęp do wolnego rynku ułatwia handel bronią cybernetyczną i informacjami istotnymi dla ataku. Czynnikiem pomocnym w gromadzeniu tych zdolności są kraje, które wspierają terroryzm i starają się korzystać z pełnomocników, aby ukryć swoją tożsamość jako inicjatora ataku na konkretny cel. Ponadto organizacja terrorystyczna musi szkolić ekspertów i gromadzić wiedzę na temat sposobów gromadzenia informacji, metod ataku i sposobów kamuflowania broni ofensywnej, aby ominąć systemy obronne na celu. Badanie to pokazuje, że dotychczas organizacjom terrorystycznym brakowało niezależnej infrastruktury naukowej i technologicznej niezbędnej do opracowania narzędzi cybernetycznych zdolnych do wyrządzania znacznych szkód. Brakuje im również możliwości gromadzenia wysokiej jakości danych wywiadowczych na potrzeby operacji. Zdolność organizacji terrorystycznych do prowadzenia szkodliwej działalności w cyberprzestrzeni zostanie zatem rozważona w świetle tych ograniczeń. Możliwość przeprowadzenia ataku obejmuje penetrację systemów operacyjnych i spowodowanie ich uszkodzeń jest dość złożona. Konieczność wysokiego poziomu zdolności wywiadowczych i penetracyjnych, która istnieje jedynie w ograniczonej liczbie krajów, oznacza, że każdy atak będzie koniecznie przeprowadzony przez państwo. Z tego powodu jak dotąd nie zaobserwowano żadnego udanego ataku podmiotu niepaństwowego na podstawowe systemy operacyjne jakiejkolwiek organizacji. Choć nie zidentyfikowano żadnego takiego ataku, można dostrzec tendencję w kierunku poprawy możliwości technologicznych najemników działających w cyberprzestrzeni na potrzeby przestępczości i oszustw. Prawdopodobnie zatem w zamian za odpowiednią rekompensatę przestępcze ugrupowania technologiczne zgodzą się na stworzenie narzędzi realizujących ataki na podstawowe systemy operacyjne infrastruktury krytycznej i spółki komercyjne. Strony te będą mogły także oddać swój towar do dyspozycji organizacji terrorystycznych. Istnieje realna możliwość, że w najbliższej przyszłości organizacje terrorystyczne będą kupować usługi ataków od najemnych hakerów i używać kodów mutacyjnych w oparciu o odmianę istniejących kodów do ataków na cele. Możliwość ta nie może być ignorowana przy tworzeniu odniesienia do zagrożeń w cyberprzestrzeni w przypadku ataków na bramę organizacji lub nawet na jej systemy informacyjne. Jest zatem bardzo prawdopodobne, że w nadchodzących latach organizacje terrorystyczne poczynią postępy w zakresie swoich zdolności do ataku cybernetycznego, w oparciu o zdobycie bardziej zaawansowanych zdolności i przełożenie tych zdolności na ataki na systemy informacyjne organizacji (nie tylko na bramę organizacji).

Media społecznościowe i Big Data

WSTĘP

Media społecznościowe stanowią coraz większą i zasadniczą część środowiska internetowego generowanego przez Web 2.0, w którym użytkownicy są autorami treści i nie otrzymują biernie informacji, ale je tworzą, przekształcają i udostępniają. W niektórych przypadkach interakcja między użytkownikami oparta na mediach społecznościowych stworzyła społeczności, wirtualne światy (np. Second Life, World of Warcraft) lub projekty crowdsourcingowe (Wikipedia). Chociaż istnieją znaczne różnice w charakterze tych wyników, dwa aspekty są zawsze obecne i istotne w świetle tego wkładu: duża ilość informacji, treści generowane przez użytkowników. Platformy mediów społecznościowych agregują ogromne ilości danych generowanych przez użytkowników, które w wielu przypadkach są identyfikowane lub możliwe do zidentyfikowania . Przyczynia się to do stworzenia specyficznego krajobrazu technologicznego, w którym zdolność predykcyjna wyróżnia Big Data . Ma istotny wpływ nie tylko na przewagę konkurencyjną w świecie biznesu (identyfikacja z wyprzedzeniem pojawiających się trendów, business intelligence itp.), ale także na wdrażanie systemów nadzoru społecznego przez państwa i grupy władzy. Z tej perspektywy na kolejnych stronach rozważone zostaną zjawiska koncentracji informacji cyfrowej i związane z nią asymetrie, które oddają w ręce nielicznych podmiotów ogromną ilość danych, ułatwiając próby inwigilacji społecznej przez rządy i firmy prywatne. Celem tego rozdziału jest zaproponowanie niektórych możliwych rozwiązań prawnych i politycznych, zarówno w celu zwiększenia bardziej demokratycznego dostępu do informacji, jak i ochrony wolności indywidualnej i zbiorowej.

BIG DATA: ASYMETRYCZNY ROZKŁAD KONTROLI NAD INFORMACJAMI I MOŻLIWE ŚRODKI ZARADCZE

Big Data nie jest czymś nowym, ale znajduje się obecnie w końcowej fazie długiej ewolucji możliwości analizy danych przy wykorzystaniu zasobów komputera. Big Data reprezentuje konwergencję różnych istniejących technologii, które pozwalają na budowę ogromnych centrów danych, tworzenie szybkich autostrad elektronicznych oraz zapewnienie wszechobecnego i na żądanie sieciowego dostępu do zasobów obliczeniowych (cloud computing). Technologie te oferują zasadniczo nieograniczone miejsce na dane, umożliwiają przesyłanie ogromnych ilości danych z jednego miejsca do drugiego, a także pozwalają na rozproszenie tych samych danych w różnych miejscach i ich ponowną agregację w ciągu kilku sekund. Wszystkie te zasoby pozwalają na gromadzenie dużej ilości informacji z różnych źródeł, a petabajty danych generowanych przez media społecznościowe stanowią idealny kontekst, w którym można wykorzystać analitykę Big Data. Cały zbiór danych może być na bieżąco monitorowany za pomocą narzędzi analitycznych, aby identyfikować pojawiające się trendy w przepływach danych i uzyskiwać wyniki w czasie rzeczywistym lub prawie rzeczywistym w sposób rewolucyjny i różniący się od tradycyjnej metody próbkowania . Dostępność tych nowych technologii i dużych zbiorów danych zapewnia przewagę konkurencyjną posiadaczom tych technologii w zakresie zdolności przewidywania nowych trendów gospodarczych, społecznych i politycznych. W kontekście mediów społecznościowych asymetrie te są widoczne w przypadku platform komercyjnych (np. Twitter, Google+ itp.), w których usługodawcy odgrywają istotną rolę w zakresie kontroli informacji. I odwrotnie, gdy media społecznościowe opierają się na otwartych, zdecentralizowanych i partycypacyjnych architekturach, asymetrie te zostają przezwyciężone; z tego powodu w kolejnych akapitach rozważymy rolę, jaką pełnią otwarte architektury i otwarte dane w celu osiągnięcia szerszego dostępu do informacji i niższej koncentracji kontroli nad informacją. Aby kontrolować i ograniczać asymetrie informacyjne związane z Big Data i ich konsekwencje w aspekcie korzyści ekonomicznych i kontroli społecznej, konieczne wydaje się przyjęcie różnych środków zaradczych, gdyż złożoność zjawiska wymaga odmiennego podejścia. Przede wszystkim ważne jest osiągnięcie lepszej alokacji kontroli nad informacją. W tym celu konieczne jest przyjęcie odpowiednich środków kontroli osób posiadających tę władzę, aby ograniczyć ewentualne nadużycia i bezprawne korzyści. Jednocześnie należy zwiększyć dostęp do informacji oraz liczbę podmiotów zdolnych do tworzenia i zarządzania dużymi ilościami danych, rozkładając władzę

informacyjną w rękach kilku organów. Konieczność kontrolowania tych wielkich skupisk danych wiąże się także z ich znaczeniem politycznym i strategicznym i powinna skutkować wprowadzeniem obowiązkowego powiadamiania o utworzeniu dużej i ważnej bazy danych – tak jak to miało miejsce na początku ery komputerowej, kiedy istniał podobna koncentracja władzy w rękach a kilka tematów ze względu na wysoki koszt pierwszych komputerów mainframe – oraz utworzenie specjalnych niezależnych organów międzynarodowych. Władze te będą w stanie zapanować nad inwazyjną postawą władzy rządowej wobec dużych baz danych i władzy właściciela Big Data, ale mogą też odegrać ważną rolę w określeniu konkretnych standardów bezpieczeństwa danych. Będzie to długa i kręta podróż, ponieważ opiera się na współpracy międzynarodowej; niemniej jednak ważne jest, aby rozpocząć je jak najszybciej, korzystając z istniejących organów międzynarodowych i wielostronnego dialogu między krajami. Jednocześnie wszelkie rozwiązania należy odpowiednio stopniować, unikając angażowania wszelkiego rodzaju farm danych budowanych gdzieś na świecie, a biorąc pod uwagę jedynie farmy danych o absolutnie niezwykłym wymiarze lub dużym znaczeniu ze względu na gromadzone dane (np. policyjne lub wojskowe bazy danych). Dostęp do danych i udostępnianie danych to kolejne dwa główne aspekty, które należy wziąć pod uwagę, aby ograniczyć władzę właścicieli Big Data i dać społeczeństwu możliwość dostępu do wiedzy. Z tej perspektywy kluczową rolę odgrywają otwarte dane i wspomniana wyżej polityka przejrzystości społeczeństwa informacyjnego (czyli notyfikacji), która pozwala dowiedzieć się, kto ma dużą władzę informacyjną i zwrócić się do tych podmiotów o udostępnienie swoich archiwów. Udostępnianie obywatelom publicznych baz danych i potencjalnie prywatnych archiwów oraz udostępnianie im surowych danych nie tylko ogranicza władzę właścicieli informacji w zakresie wyłącznego dostępu do danych, ale także ogranicza ich przewagę w zakresie umiejętności analizy technicznej i kulturowej. Wreszcie konieczne jest zajęcie się krytycznymi kwestiami dotyczącymi geopolitycznego podziału władzy informacyjnej, co stanowi wyłaniający się problem dla Europy. Mimo że duże europejskie firmy są w stanie gromadzić i analizować duże ilości danych, główne komercyjne media społecznościowe mają swoją siedzibę w USA i ten element stawia ten kraj na lepszej pozycji do kontrolowania światowych przepływów informacji generowanych przez użytkowników tego rodzaju mediów. usługi. Z geopolitycznego punktu widzenia sytuacja ta stanowi słabość UE, polegającą na utracie kontroli nad danymi jej obywateli w związku z koniecznością powierzenia zarządzania informacjami strategicznymi podmiotom zagranicznym. Aby zmniejszyć to ryzyko, wzywa się przemysł europejski do przyjęcia ważniejszej roli w sektorze ICT, a jednocześnie UE. wzmacnia ochronę danych osobowych.

BIG DATA I NADZÓR SPOŁECZNY: WSPÓŁPRACA PUBLICZNA I PRYWATNA W KONTROLI SPOŁECZNEJ

Zagrożenia związane z koncentracją kontroli nad informacjami w kontekście mediów społecznościowych i w ogóle nie ograniczają się do demokratycznego dostępu i dystrybucji informacji i wiedzy, ale także do potencjalnych systemów nadzoru społecznego, które można zrealizować przy użyciu tych informacji. Z tej perspektywy niedawna sprawa NSA stanowi bardziej oczywistą ilustrację potencjalnych konsekwencji monitorowania interakcji online, choć jest to to najnowszy z serii programów przyjętych przez agencje rządowe w różnych krajach w celu prowadzenia masowej inwigilacji społecznej. W zachodnich krajach demokratycznych współczesny nadzór społeczny nie jest już realizowany wyłącznie przez aparat wywiadowczy, który samodzielnie gromadzi ogromną ilość informacji poprzez wszechobecne systemy monitorowania. Nadzór społeczny jest wynikiem interakcji między sektorem prywatnym i publicznym, opartym na modelu współpracy możliwym dzięki nakazom obowiązkowego ujawniania informacji wydanym przez sądy lub organy administracyjne i rozszerzonym na nieokreśloną pulę dobrowolnej lub proaktywnej współpracy dużych przedsiębiorstw . W ten sposób rządy uzyskują informacje przy pośredniej „współpracy" użytkowników, którzy prawdopodobnie nie przekazaliby tych samych informacji podmiotom publicznym, gdyby zostały o to poproszone. Dostawcy usług gromadzą na przykład dane osobowe na podstawie umów prywatnych (polityki prywatności) za

zgodą użytkownika i dla swoich konkretnych celów , ale rządy wykorzystują tę praktykę, wydając obowiązkowe nakazy uzyskania ujawnienia tych danych Informacja. Ten podwójny mechanizm ukrywa przed obywatelami ryzyko i wymiar kontroli społecznej, którą można realizować poprzez monitorowanie sieci społecznościowych lub innych usług oraz wykorzystanie technologii analityki Big Data. Kolejnym istotnym aspektem kontroli wynikającej z Big Data jest jej ilość. Analizy skupiające się na profilowaniu pozwalają przewidzieć postawy i decyzje pojedynczego użytkownika, a nawet dopasować podobne profile. Natomiast Big Data nie służy do skupiania się na jednostkach, ale do analizy dużych grup i populacji (np. nastrojów politycznych całego kraju). Chociaż w wielu przypadkach działania wywiadowcze mają niewiele wspólnego z ogólnymi przepisami o ochronie danych – są bowiem dozwolone na mocy szczegółowych przepisów prawnych wprowadzających wyjątki od zasad ogólnych dotyczące ochrony danych i prywatności mogą odegrać istotną rolę w zakresie ograniczenia ilości danych gromadzonych przez podmioty prywatne, a w konsekwencji pośrednio wpłynąć na informacje dostępne na potrzeby publicznego nadzoru społecznego. Interakcję pomiędzy publicznym i prywatnym w kontroli społecznej można podzielić na dwie kategorie, obie istotne z punktu widzenia ochrony danych. Pierwsza dotyczy gromadzenia danych przedsiębiorstw prywatnych przez władze rządowe i sądowe (patrz sekcja „Zestaw zatwierdzonych przepisów prawnych dotyczących e-nadzoru"), natomiast druga dotyczy wykorzystywania przez władze rządowe i sądowe instrumentów i technologii udostępnianych przez prywatne firmy do celów organizacyjnych i dochodzeniowych (patrz sekcja „Wykorzystanie narzędzi i zasobów sektora prywatnego").

ZESTAW ZATWIERDZONYCH PRZEPISÓW DOTYCZĄCYCH ESONTROLU

W przypadku pierwszej kategorii, a zwłaszcza gdy wniosek składają agencje rządowe, kwestia ewentualnego naruszenia praw podstawowych staje się bardziej delikatna. System przechwytywania Echelon i program całkowitej świadomości informacyjnej (TIA) to konkretne przykłady, które nie są odosobnionymi incydentami, ale niewątpliwie sprawą NSA wyraźnie pokazało, jak inwazyjny może być nadzór w dobie globalnego przepływu danych i Big Data. Aby lepiej zrozumieć tę sprawę, dość ważny jest przegląd znacznej części ustawodawstwa dotyczącego nadzoru elektronicznego, które szczególnie po 11 września zostało zatwierdzone w Stanach Zjednoczonych i, do pewnego stopnia, w wielu krajach Kraje europejskie. Najważniejszym aktem prawnym jest ustawa o nadzorze wywiadu zagranicznego (FISA) z 1978 r., która określa procedury gromadzenia informacji wywiadu zagranicznego poprzez elektroniczny nadzór komunikacji dla celów bezpieczeństwa wewnętrznego. Artykuł 702 ustawy FISA zmienionej w 2008 r. (FAA) rozszerzył jej zakres poza przechwytywanie komunikacji, aby uwzględnić również wszelkie dane w chmurze publicznej. Co więcej, w tej sekcji wyraźnie wskazano, że istnieją dwa różne systemy przetwarzania i ochrony danych w przypadku obywateli i rezydentów USA (USPER) z jednej strony oraz obywateli i rezydentów spoza USA (nie-USPER) z drugiej. Mówiąc dokładniej, Czwarta Poprawka ma zastosowanie wyłącznie do obywateli USA, ponieważ brak jest jakichkolwiek rozpoznawalnych praw do prywatności w przypadku „osób spoza USA". osób" w ramach FISA (Bowden, 2013). Dzięki ustawie FISA i nowelizacji z 2008 r. władze USA mają możliwość dostępu do danych osobowych UE i ich przetwarzania. obywateli na dużą skalę, między innymi poprzez beznakazowe podsłuchiwanie przez Agencję Bezpieczeństwa Narodowego (NSA) kablowego ruchu internetowego (UPSTREAM) i bezpośredni dostęp do danych osobowych przechowywanych na serwerach prywatnych firm z siedzibą w USA, takich jak Microsoft, Yahoo , Google, Apple, Facebook lub Skype (PRISM), poprzez programy do wyszukiwania między bazami danych, takie jak X-KEYSCORE. Władze USA mają również prawo wymusić ujawnienie kluczy kryptograficznych, w tym kluczy SSL używanych do zabezpieczania przesyłania danych przez główne wyszukiwarki, sieci społecznościowe, portale poczty internetowej i ogólnie usługi w chmurze (program BULLRUN) (Corradino, 1989; Bowdena, 2013). Niedawno działająca przy Prezydencie Stanów Zjednoczonych Grupa Przeglądowa ds. Technologii Wywiadowczych i Komunikacyjnych opublikowała raport zatytułowany „Wolność i bezpieczeństwo w

zmieniającym się świecie". Kompleksowy raport przedstawia 46 zaleceń mających na celu ochronę bezpieczeństwa narodowego przy jednoczesnym poszanowaniu naszego wieloletniego zaangażowania na rzecz prywatności i swobód obywatelskich, ze szczególnym odniesieniem do obywateli spoza USA. Nawet jeśli ustawa FISA jest najczęściej stosowanym i znanym narzędziem legislacyjnym do prowadzenia działań wywiadowczych, istnieją inne istotne akty prawne dotyczące nadzoru elektronicznego. Wystarczy wziąć pod uwagę ustawę Communications Assistance For Law Enforcement Act (CALEA) z 1994 r., która upoważnia organy ścigania i agencje wywiadowcze do prowadzenia nadzoru elektronicznego, wymagając, aby operatorzy telekomunikacyjni i producenci sprzętu telekomunikacyjnego modyfikowali i projektowali swój sprzęt, obiekty i usług, aby mieć pewność, że mają wbudowany monitoring. Ponadto w następstwie Patriot Act z 2001 r. zaproponowano mnóstwo projektów ustaw. Najnowsze ustawy (jeszcze nieobowiązujące) to ustawa Cyber Intelligence Sharing and Protection Act (CISPA) z 2013 r., która umożliwiłaby wymianę informacji o ruchu internetowym pomiędzy rządem USA a niektórymi firmami technologicznymi i produkcyjnymi oraz ustawę o ochronie dzieci przed internetowymi pornografami z 2011 r., która rozszerza obowiązki dotyczące przechowywania danych na amerykańskich dostawców usług internetowych . Prawdę mówiąc, programy inwigilacji obejmują nie tylko Stany Zjednoczone. W Europie Program Rozwoju Możliwości Komunikacyjnych wywołał ogromne kontrowersje, biorąc pod uwagę jego zamiar stworzenia wszechobecnego programu masowego nadzoru w Wielkiej Brytanii w odniesieniu do rozmów telefonicznych, wiadomości tekstowych i e-maili, a także rozszerzenia do rejestrowania komunikacji w mediach społecznościowych. Niedawno, w czerwcu 2013 r., w ramach tzw. programu TEMPORA wykazano, że brytyjska agencja wywiadowcza Government Communications Headquare (GCHQ) współpracowała z NSA w zakresie działań inwigilacyjnych i szpiegowskich . Po tych doniesieniach, we wrześniu 2013 r., ukazały się raporty skupiające się na w sprawie działalności szwedzkiego Radia Obrony Narodowej (FRA). Podobne projekty przechwytywania danych telekomunikacyjnych na dużą skalę zostały przeprowadzone zarówno przez Francuską Generalną Dyrekcję Bezpieczeństwa Zewnętrznego (DGSE), jak i niemiecką Federalną Służbę Wywiadowczą (BDE). Nawet jeśli wydaje się, że E.U. i programy nadzoru w USA są podobne, istnieje jedna istotna różnica: w UE, zgodnie z prawem o ochronie danych, osoby fizyczne zawsze mają kontrolę nad swoimi danymi osobowymi, podczas gdy w USA osoba fizyczna ma bardziej ograniczoną kontrolę, gdy użytkownik zaakceptuje warunki i stan usługi.

WYMUSZONA WSPÓŁPRACA „NA TELEFON" PODMIOTÓW PRYWATNYCH

Oprócz działań monitorujących agencji rządowych zdarzają się przypadki, w których dostawcy usług internetowych współpracują spontanicznie lub na proste żądanie organów ścigania. Gwałtowny wzrost Big Data od 2001 r. stworzył naprawdę wyjątkową okazję. Kluczową rolę w tym zakresie odegrały Media Społecznościowe. Wystarczy zastanowić się nad faktem, że Facebook, Twitter, Google+ i Instagram, wszystkie zlokalizowane w Dolinie Krzemowej, szczycą się około 2 miliardami użytkowników na całym świecie, a wielu z nich to obywatele Unii Europejskiej. Założyciel Facebooka mógł mieć na celu „wzmocnienie pozycji jednostki", ale nie ma wątpliwości, że usługi sieci społecznościowych (SNS) wzmocniły również władzę organów ścigania.

Gromadzenie danych na potrzeby przewidywania i zapobiegania przestępczości

Aby pozostać w temacie pozyskiwania informacji przez organy ścigania, istnieją dwa interesujące przypadki gromadzenia Big Data w celach zapobiegania przestępczości: Pierwszy to oprogramowanie „PredPol", używane początkowo przez policję w Los Angeles, a obecnie przez inną policję sił zbrojnych w Stanach Zjednoczonych (Palm Beach, Memphis, Chicago, Minneapolis i Dallas). Działania policji predykcyjnej to zasadniczo sprawdzanie danych, miejsc i technik dotyczących niedawnych przestępstw z różnych źródeł, analizowanie ich, a następnie wykorzystywanie wyników do przewidywania

przyszłych przestępstw, zapobiegania im i skuteczniejszego reagowania na nie. Nawet jeśli software house tworzony przez PredPol deklaruje, że nie prowadzi działań profilowania, istotne staje się dokładne zapoznanie się z technologią stosowaną do anonimizacji danych osobowych pozyskiwanych przez bazę organów ścigania. Ten rodzaj oprogramowania z pewnością będzie miał duży wpływ w Stanach Zjednoczonych na koncepcję ochrony praw zgodnie z Czwartą Poprawką, a dokładniej na pojęcia takie jak „prawdopodobna przyczyna" i „uzasadnione podejrzenie", które w przyszłości mogą się pojawić zależą od algorytmu, a nie od wyboru człowieka . Drugim przykładem jest oprogramowanie X1 Social Discovery. Oprogramowanie to mapuje daną lokalizację, na przykład określoną przecznicę w mieście lub nawet cały konkretny obszar metropolitalny, i przeszukuje cały publiczny kanał Twittera w celu zidentyfikowania wszelkich tweetów zlokalizowanych w przeszłości. trzy dni (czasami dłużej) na tym konkretnym obszarze. Aplikacja ta może dostarczać szczególnie przydatnych danych do celów kontroli społecznej. Można sobie wyobrazić możliwość posiadania przydatnych elementów (np. adresu IP) umożliwiających identyfikację podmiotów znajdujących się na danym obszarze podczas poważnego wypadku samochodowego lub ataku terrorystycznego.

Prawowitość

Ze ściśle prawnego punktu widzenia te narzędzia kontroli społecznej mogą być stosowane poprzez zbieranie informacji bezpośrednio od obywateli, zgodnie z następującą zasadą publiczną: „Jeżeli ktoś dokonuje czynu w miejscu publicznym, przestrzeganie i rejestrowanie tego czynu zwykle nie budzi oczekiwań prywatności". (Gillespiego, 2009)

W Unii Europejskiej, choć tego rodzaju gromadzenie danych jest częste, mogłoby to kontrastować z orzecznictwem Europejskiego Trybunału Praw Człowieka, który w sprawie Rotaru przeciwko Rumunii orzekł, że „informacje publiczne mogą wchodzić w zakres życia prywatnego, jeżeli jest systematycznie gromadzone i przechowywane w aktach znajdujących się w posiadaniu władz." Jak zauważa O'Floinn: „Informacje nieprywatne mogą stać się informacjami prywatnymi w zależności od ich przechowywania i wykorzystania. Gromadzenie informacji prawdopodobnie doprowadzi do uzyskania prywatnych informacji o tej osobie" . W Stanach Zjednoczonych temat ten został poruszony w toczącej się obecnie przed Sądem Najwyższym sprawie People vs. Harris. W dniu 26 stycznia 2012 r. Biuro Prokuratora Okręgowego Hrabstwa Nowy Jork wysłało wezwanie do sądu firmy Twitter, Inc. w celu uzyskania danych z Twittera dotyczących użytkowników podejrzanych o udział w ruchu „Occupy Wall Street". Twitter odmówił udostępnienia funkcjonariuszom organów ścigania żądanych informacji i wniósł o uchylenie wezwania. Sąd Karny w Nowym Jorku podtrzymał wniosek Prokuratury Okręgowej hrabstwa Nowy Jork, odrzucając argumenty Twittera, stwierdzając, że tweety są z definicji publiczne i że nie jest wymagany nakaz, aby zmusić Twittera do ujawnić je. Biuro Prokuratora Okręgowego argumentowało, że zastosowanie ma doktryna „ujawniania informacji osobom trzecim" przedstawiona po raz pierwszy w sprawie United States przeciwko Millerowi.

WYKORZYSTANIE NARZĘDZI I ZASOBÓW SEKTORA PRYWATNEGO

Druga zależność dotyczy wykorzystania przez państwo narzędzi i zasobów spółki prywatnej na potrzeby organizacyjne i dochodzeniowe. Biorąc pod uwagę rozległe oceany Big Data, władze amerykańskie zdecydowały się zwrócić do sektora prywatnego nie tylko w celu zarządzania oprogramowaniem, ale także w odniesieniu do samego zarządzania danymi. Jednym z przykładów jest platforma Hadoop należąca do CTO, która jest w stanie zapamiętywać i przechowywać dane dotyczące wielu organów ścigania w Stanach Zjednoczonych. Podobnie powstał system chmury prywatnej, który przekazuje najnowsze informacje wywiadowcze w czasie zbliżonym do rzeczywistego żołnierzom amerykańskim stacjonującym w Afganistanie . Innym przykładem jest technologia rozpoznawania twarzy opracowana przez Walta Disneya na potrzeby jego parku i sprzedana siłom zbrojnym USA. Biorąc pod uwagę

oszczędność kosztów i ogromną moc obliczeniową scentralizowanej chmury nieuniknione jest, że organy ścigania, siły zbrojne i agencje rządowe będą stopniowo polegać na tego rodzaju usługach. Powyższa zmiana będzie wiązała się z możliwymi do wyciągnięcia kwestiami prawnymi w zakresie jurysdykcji, bezpieczeństwa i prywatności w zakresie zarządzania danymi. Odpowiednie kwestie prawne można rozwiązać poprzez prywatną chmurę na terenie stanu z wyłączną kontrolą kluczy klienta. Warto jednak wziąć pod uwagę, że w ten sposób podmioty prywatne uzyskają dostęp do niezwykle ważnego i stale rozwijającego się zasobu informacyjnego. Dzięki potencjałowi systemów chmurowych będą mogły zatem rozwijać coraz bardziej wyrafinowane narzędzia do eksploracji danych. Scenariusz ten, który jest już faktem w Stanach Zjednoczonych, może stać się rzeczywistością także dzięki impulsowi Europejskiej Agendy Cyfrowej i promowaniu w niej inicjatyw Partnerstwa Publiczno-Prywatnego w chmurze (Komisja Wspólnot Europejskich, 2009; zob. także Europejski Partnerstwo w chmurze (ECP), 2013). Dlatego ważne jest, aby europejskie usługi w chmurze opierały się na wysokich standardach ochrony danych, bezpieczeństwa, interoperacyjności i przejrzystości w zakresie poziomów usług i dostępu rządu do informacji, co niedawno uznała Komisja Europejska .

ROLA UE REFORMA OCHRONY DANYCH W OGRANICZANIU RYZYKA NADZORU SPOŁECZNEGO

Opisane powyżej ramy pokazują, że współczesna kontrola społeczna jest wynikiem interakcji pomiędzy sektorem prywatnym i publicznym. Ten model współpracy opiera się nie tylko na nakazach obowiązkowego ujawniania informacji wydawanych przez sądy lub organy administracyjne, ale także rozszerzył się na bardziej nieokreśloną szarą strefę dobrowolnej i proaktywnej współpracy dużych przedsiębiorstw. Trudno jest uzyskać szczegółowe informacje na temat tego drugiego modelu dobrowolnej współpracy; jednak przewaga firm amerykańskich w sektorze ICT, zwłaszcza w zakresie Internetu i usług w chmurze, zwiększa wpływ administracji USA na krajowe firmy i ułatwia zawieranie konkretnych tajnych porozumień o współpracy w kontroli społecznej. Na tym tle wyłania się polityczna i strategiczna wartość europejskich przepisów dotyczących ochrony danych. Zasady te mogą pełnić rolę bariery ochronnej mającej na celu uniemożliwienie i ograniczenie dostępu do informacji o obywatelach Europy. W tym sensie U.U. Wniosek dotyczący ogólnego rozporządzenia o ochronie danych (Komisja Europejska, 2012) rozszerza jego zakres terytorialny (art. 3 ust. 2, 2013) poprzez „przetwarzanie danych osobowych osób, których dane dotyczą, w Unii przez administratora lub podmiot przetwarzający niemający siedziby w Unii, gdy czynności przetwarzania związane są z:

a) oferowanie towarów lub usług takim podmiotom danych w Unii, niezależnie od tego, czy wymagana jest płatność od podmiotu danych; Lub

b) monitorowanie takich osób, których dane dotyczą".

Należy zauważyć, że różni komentatorzy uważają, że ryzyko prywatności związane z analizą Big Data jest niskie, wskazując na dużą ilość danych przetwarzanych przez analitykę oraz brak możliwości identyfikacji większości tych danych. Wniosek ten jest błędny. Anonimowość poprzez pozbawienie tożsamości jest celem trudnym do osiągnięcia, jak wykazano w szeregu badań . Siła analityki Big Data w wyciąganiu nieprzewidywalnych wniosków z informacji podważa wiele strategii opartych na deidentyfikacji . W wielu przypadkach możliwy jest proces odwrotny w celu identyfikacji osób; możliwa jest także ich identyfikacja na podstawie pierwotnie anonimowych danych. W tym przypadku bliższe prawdy jest stwierdzenie, że każde dane stanowią informację osobową, niż twierdzenie, że możliwe jest zarządzanie danymi w sposób nieidentyfikujący. Choć projekt nowego rozporządzenia nie uwzględnia danych przetwarzanych przez organom publicznym do celów zapobiegania, prowadzenia dochodzeń, wykrywania, ścigania przestępstw lub wykonywania kar karnych21, jego wpływ na kontrolę społeczną jest znaczący, ponieważ w wielu przypadkach bazy danych przedsiębiorstw prywatnych są przedmiotem dochodzeń organów publicznych. Z tego względu ograniczenie ilości

danych gromadzonych przez podmioty prywatne oraz zwiększenie samostanowienia osób, których dane dotyczą, w zakresie ich danych osobowych ograniczają możliwość kolejnych inicjatyw kontroli społecznej przez agencje rządowe. Jednakże złożoność procesów przetwarzania danych i siła współczesnej analityki, a także występowanie efektów uzależnienia technologicznego i rynkowego drastycznie zmniejszają świadomość osób, których dane dotyczą, ich zdolność do oceny różnych konsekwencji swoich wyborów oraz wyraz prawdziwego swobodnego oraz świadoma zgoda . Ten brak świadomości ułatwia tworzenie szerszych baz danych, do których organy mają dostęp w przypadkach przewidzianych przez prawo, i nie można go uniknąć poprzez przekazywanie odpowiednich informacji osobom, których dane dotyczą, lub polityki prywatności, ze względu na fakt, że te powiadomienia są czytane jedynie przez bardzo ograniczoną liczbę użytkowników, którzy w wielu przypadkach nie są w stanie zrozumieć części terminów prawnych stosowanych zwykle w tych ogłoszeniach . Aspekty te są jeszcze bardziej istotne w kontekście Big Data, co powoduje, że tradycyjny model ochrony danych znajduje się w kryzysie . Tradycyjny model opiera się na ogólnym zakazie plus „powiadomienie i zgoda" oraz na spójności gromadzenia danych z celami określonymi w momencie zbierania informacji. Jednak obecnie znaczna część wartości danych osobowych nie jest oczywista w przypadku zwykłego powiadomienia i wyrażenia zgody, a „przekształcające" wykorzystanie dużych zbiorów danych często uniemożliwia wyjaśnienie opisu wszystkich możliwych sposobów ich wykorzystania w momencie ich początkowego gromadzenia. Aby wzmocnić ochronę informacji indywidualnych, propozycja UE uwzględnia te ograniczenia i przenosi punkt ciężkości ochrony danych z indywidualnego wyboru na architekturę zorientowaną na prywatność . Podejście to, które ogranicza ilość danych gromadzonych poprzez bariery „strukturalne" i wprowadza prewencyjną ocenę ochrony danych , wywołuje także bezpośredni wpływ na kontrolę społeczną poprzez zmniejszenie ilości dostępnych informacji. W odniesieniu do zebranych informacji Komisja Europejska Propozycja wzmacnia samostanowienie użytkowników poprzez wymóg przenoszenia danych, co daje użytkownikowi prawo do uzyskania od administratora kopii danych podlegających przetwarzaniu „w formacie elektronicznym i ustrukturyzowanym, który jest powszechnie używany i umożliwia dalsze wykorzystanie przez osobę, której dane dotyczą". Przenośność zmniejszy ryzyko uzależnienia technologicznego ze względu na standardy technologiczne i formaty danych przyjęte przez dostawców usług, które ograniczają migrację z jednej usługi do drugiej. Jednak w wielu przypadkach, głównie w kontekście mediów społecznościowych, ograniczona liczba firm świadczących usługi zmniejsza ryzyko, że użytkownicy nie zostaną wyśledzeni w wyniku przeniesienia ich konta z jednej platformy na drugą, a tym samym minimalizuje pozytywne skutki przenoszenia danych. Wreszcie Propozycja wzmacnia prawo do żądania usunięcia danych przetwarzanych bez zgody osoby, której dane dotyczą, wbrew jej sprzeciwowi, bez zapewnienia jej odpowiednich informacji lub poza ramami prawnymi. Skuteczna realizacja tego prawa może zmniejszyć ogólną ilość danych przechowywanych przez usługodawców, a także może ograniczyć ilość informacji znajdujących się w archiwach bez uzasadnionej przyczyny przetwarzania informacji. W ten sposób ograniczana jest także możliwość przeglądania przez władze historii poszczególnych profili. Wszystkie omówione powyżej aspekty sprzyjają ograniczeniu informacji dostępnych wszystkim podmiotom zainteresowanym kontrolą społeczną, a co za tym idzie, wpływają także na żądania ujawnienia składane przez agencje rządowe i sądy przedsiębiorstwom prywatnym. Niemniej jednak te uprawnienia do przeszukania i zajęcia oraz ich wykonywanie stanowią podstawowy rdzeń kontroli społecznej.

OCHRONA UE STANDARD OCHRONY DANYCH W ZGLOBALIZOWANYM ŚWIECIE

Aby przeanalizować ten aspekt w scenariuszu przyszłych europejskich ram ochrony danych, należy wziąć pod uwagę obie propozycje Komisji Europejskiej:

- Wniosek dotyczący nowego ogólnego rozporządzenia o ochronie danych (PRODO) oraz

- mniej dyskutowany wniosek dotyczący dyrektywy w sektorze egzekwowania prawa (PDPI).

Chociaż druga propozycja dotyczy bardziej szczegółowo kontroli rządowej i sądowej, pierwsza uwzględnia ten aspekt z punktu widzenia przepływów danych. Nowy wniosek dotyczący nowego ogólnego rozporządzenia o ochronie danych, a także obowiązująca obecnie dyrektywa 96/46/WE dopuszcza transgraniczny przepływ danych z Europy do innych krajów tylko wtedy, gdy państwo trzecie zapewnia odpowiedni poziom ochrony danych . Oceniając adekwatność ochrony danych w danym kraju, Komisja powinna wziąć pod uwagę także ustawodawstwo obowiązujące w krajach trzecich „w tym dotyczące bezpieczeństwa publicznego, obronności, bezpieczeństwa narodowego i prawa karnego". W związku z tym obecność inwazyjnych organów publicznych prowadzących dochodzenia oraz brak odpowiednich gwarancji dla osoby, której dane dotyczą, nabierają znaczenia przy podejmowaniu decyzji o ograniczeniu transgranicznego przepływu danych między spółkami zależnymi a holdingami lub między spółkami. Po raz kolejny ograniczenie to nie ma wpływu na władze publiczne, ale ogranicza zbiór informacji będących w posiadaniu przedsiębiorstw prywatnych i dostępnych do ich kontroli. Pomijając sprawę NSA, która jest nadal w toku, sprawa SWIFT dostarcza wyjaśnienia dotyczącego związku między transgranicznymi przepływami danych, zagraniczną jurysdykcją i możliwymi skutkami dla obywateli i kontroli społecznej; ta sama krytyka ma zastosowanie i została wyrażona przez komentatorów w odniesieniu do amerykańskiej ustawy Patriot Act. Te dwie sprawy różnią się, ponieważ w sprawie NSA spoza UE. władze zwróciły się o dostęp do informacji znajdujących się w posiadaniu spółki z siedzibą w UE, podczas gdy w sprawie SWIFT wnioski kierowano do spółek amerykańskich w celu uzyskania dostępu do informacji, które otrzymały z UE. spółki zależne. W sprawie SWIFT (Grupa Robocza Art. 29 ds. Ochrony Danych) Grupa Robocza Art. 29 ds. Ochrony Danych wyjaśniła, że prawo zagraniczne nie stanowi podstawy prawnej ujawniania danych osobowych podmiotom spoza UE. właściwe organy, ponieważ jedynie instrumenty międzynarodowe zapewniają odpowiednie ramy prawne umożliwiające współpracę międzynarodową (Grupa Robocza ds. Ochrony Danych, art. 29, 2006b; zob. także Grupa Robocza ds. Ochrony Danych, art. 29, 2006a). Ponadto wyjątek przewidziany w art. 26 ust. 1 lit. b) Dyrektywa 95/46/WE27 nie ma zastosowania, jeżeli przeniesienie nie jest konieczne lub wymagane prawnie ze względu na ważne względy interesu publicznego UE. Państwo członkowskie (Grupa Robocza Art. 29 ds. Ochrony Danych, 2006b). Natomiast (co wyszło w sprawie PATRIOT Act, a także w odniesieniu do szerszego, złożonego i dynamicznego systemu uprawnień, którymi dysponuje rząd USA w sferze dochodzeń karnych i bezpieczeństwa narodowego, władze USA mogą uzyskać dostęp do danych przechowywanych przez UE. spółki zależne spółek amerykańskich. Należy jednak wskazać, że istnieje potencjalne naruszenie ochrony danych osobowych obywateli europejskich i dzieje się to nie tylko w odniesieniu do prawa amerykańskiego, ale także w powiązaniu z innymi regulacjami zagranicznymi, gdyż czego dowodem jest niedawny projekt indyjskiej ustawy o ochronie prywatności i chińskich przepisów dotyczących ochrony danych. W celu ograniczenia takich włamań projekt ustawy UE. Wniosek dotyczący ogólnego rozporządzenia o ochronie danych ograniczył ujawnianie organom zagranicznym i to przewidywał

„żaden wyrok sądu lub trybunału ani żadna decyzja organu administracyjnego państwa trzeciego nakładająca na administratora lub podmiot przetwarzający obowiązek ujawnienia danych osobowych nie będzie uznawana ani wykonalna w żaden sposób, bez uszczerbku dla traktatu o wzajemnej pomocy lub umowy międzynarodowej w obowiązujące między wnioskującym państwem trzecim a Unią lub państwem członkowskim"

Projekt zobowiązał także administratorów i podmioty przetwarzające do powiadamiania krajowych organów nadzorczych o wszelkich tego typu żądaniach oraz do uzyskania uprzedniej zgody organu nadzorczego na przekazanie . Przepisy te zostały usunięte z ostatecznej wersji wniosku Komisji z dnia 25 stycznia 2012 r., ale obecnie zostały ponownie wprowadzone przez Parlament Europejski w

odpowiedzi na sprawę NSA. Oprócz wniosku dotyczącego ogólnego rozporządzenia o ochronie danych, wyżej wymieniony wniosek Dyrektywa w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy (PDPI) ustanawia pewną ochronę przed możliwym naruszeniem prywatności obywateli UE. Celem tej dyrektywy jest zapewnienie, że „w społeczeństwie globalnym charakteryzującym się szybkimi zmianami technologicznymi, w którym wymiana informacji nie zna granic", podstawowe prawo do ochrony danych będzie konsekwentnie chronione.35 Jedną z głównych kwestii w UE jest: poziomem jest brak harmonizacji przepisów o ochronie danych w państwach członkowskich, a nawet bardziej „w kontekście wszystkich przepisów UE". polityki, w tym egzekwowania prawa i zapobiegania przestępczości, a także w naszych stosunkach międzynarodowych". Chociaż dyrektywa może nie mieć takiego samego wpływu na harmonizację przepisów krajowych obowiązujących obecnie w różnych państwach członkowskich , w rzeczywistości stanowi ona pierwszy element prawodawstwa, aby miało ono bezpośredni skutek w porównaniu z poprzednimi próbami podejmowanymi w drodze zalecenia Rady Europy nr R (87)36 i decyzji ramowej 2008/977/WSiSW.

Podstawowe zasady niniejszej dyrektywy, wspólne z poprzednimi dyrektywami, o których mowa, są dwojakie:

(1) Po pierwsze, istnieje potrzeba uczciwego, zgodnego z prawem i odpowiedniego przetwarzania danych w trakcie dochodzeń karnych lub w celu zapobiegania przestępstwom, zgodnie z którym wszelkie dane muszą być gromadzone w określonych, wyraźnych i zgodnych z prawem celach oraz muszą zostać usunięte lub poprawione bez opóźnienia (art. 4, PDPI i art. 4b, 2013).

(2) Następnie istnieje obowiązek dokonania wyraźnego rozróżnienia pomiędzy różnymi kategoriami potencjalnych osób, których dane dotyczą w postępowaniu karnym (osoby, w stosunku do których istnieją poważne podstawy, aby sądzić, że popełniły lub zamierzają popełnić przestępstwo) , osoby skazane, ofiary przestępstwa, osoby trzecie uczestniczące w przestępstwie).

Dla każdej z tych kategorii należy poświęcić inny odpowiedni poziom uwagi ochronie danych, szczególnie w przypadku osób, które nie należą do żadnej z kategorii, o których mowa powyżej. Te dwie zasady mają ogromne znaczenie, chociaż ich zastosowanie na poziomie praktycznym nie będzie w niektórych Państwach Członkowskich ani łatwe, ani natychmiastowe. Łatwo to wykazać na podstawie trudności napotykanych przy opracowywaniu praktycznych zasad rozróżniających w aktach sądowych kilka kategorii potencjalnych osób, których dane dotyczą, lub przy próbie określenia zasady, na podstawie której dany dokument sądowy ma zostać usunięty. Oprócz tych dwóch ogólnych zasad, przepisy Dyrektywy są interesujące i potwierdzają ujednolicone zasady ochrony danych. Wystarczy wspomnieć tutaj zakaz stosowania środków opartych wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych, które w istotny sposób wpływają lub wywołują niekorzystne skutki prawne dla osoby, której dane dotyczą, a także wdrażanie mechanizmów ochrony danych już w fazie projektowania i domyślnych zapewniających ochronę danych praw podmiotu i przetwarzania wyłącznie tych danych osobowych. Ponadto wniosek dotyczący dyrektywy w sektorze egzekwowania prawa pociąga za sobą obowiązek wyznaczenia inspektora ochrony danych we wszystkich organach egzekwowania prawa w celu monitorowania wdrażania i stosowania polityk w zakresie ochrony danych osobowych. Zasady te stanowią istotne ograniczenie możliwości eksploracji danych osobowych i wrażliwych gromadzonych przez organy ścigania. Jeśli prawdą jest, że większość tych przepisów znalazła się także w Zaleceniu nr R (87) Rady Europy oraz w Decyzji Ramowej 2008/977/WSiSW, to prawdą jest również, że napędzanie mechanizmów ochrony danych już w fazie projektowania i domyślnych i środki mogłyby zachęcać do anonimizacji danych i pomóc w uniknięciu masowego stosowania zautomatyzowanego przetwarzania danych osobowych.

Media społecznościowe i ich rola dla organów ścigania: przegląd i wnioski

WSTĘP

Media społecznościowe stały się głównym aspektem aktywności w Internecie, a tym samym istotną częścią działań związanych z cyberprzestępczością i cyberterroryzmem. W miarę jak LEA (organy egzekwowania prawa) skupiają się na zagrożeniach związanych z cyberprzestępczością i cyberterroryzmem, rośnie także wymóg rozważenia potencjalnego zastosowania mediów społecznościowych jako istotnego aspektu każdej strategii cyberobrony. Aby pogłębić wiedzę na temat działalności związanej z cyberprzestrzenią, należy docenić rolę mediów społecznościowych w społeczeństwie, aby umożliwić opracowanie strategii zwalczania nie tylko cyberprzestępczości i cyberterroryzmu, ale także przestępstw ułatwianych poprzez korzystanie z mediów społecznościowych. Obejmują one jego potencjalne wykorzystanie w zwalczaniu szerokiej gamy zagrożeń przestępczych, takich jak te określone w scenariuszach w sekcji „Scenariusze wykorzystania LEA w mediach społecznościowych", a ostatecznie w rozwijaniu przewagi konkurencyjnej nad szeroką gamą nielegalnej działalności przestępczej. Chociaż media społecznościowe są często kojarzone z dużymi usługami sieciowymi, takimi jak Facebook i Twitter, termin media społecznościowe odnosi się do większej rodziny platform usługowych. Usługi te można podzielić na sześć grup :

1. Wspólne projekty (np. Wikipedia)

2. Blogi, w tym mikroblogi (np. Twitter)

3. Społeczności treści (np. YouTube)

4. Serwisy społecznościowe (np. Facebook, LinkedIn)

5. Wirtualne światy gier (np. World of Warcraft)

6. Wirtualne światy społecznościowe (np. Second Life)

Różnica między mediami społecznościowymi a mediami „tradycyjnymi" polega na tym, że użytkownicy mogą tworzyć i wymieniać treści, które sami stworzyli . Zmiana ta spowodowała, że użytkownicy odeszli od biernego odbioru treści na rzecz aktywnego uczestnictwa w tworzeniu treści online. W tym procesie media społecznościowe zaczęły służyć wielu różnym celom. Ji i in. (2010) wyróżniają pięć głównych funkcji:

1. Komunikacja: rozmowy ze znajomymi i przekazywanie indywidualnych opinii za pośrednictwem sieci

2. Połączenie: utrzymanie relacji utworzonych offline

3. Udostępnianie treści: udostępnianie lub dystrybucja treści, takich jak informacje, muzyka, filmy itp.

4. Wyszukiwanie eksperckie: wyszukiwanie osób posiadających profesjonalną wiedzę i doświadczenie, do których użytkownicy chcą uzyskać dostęp

5. Tożsamość: publikowanie własnych cech, emocji, nastrojów itp. w celu wyrażenia tożsamości użytkowników w Internecie

Funkcje te niekoniecznie są powiązane z konkretnymi platformami mediów społecznościowych. W rzeczywistości często jedna platforma mediów społecznościowych może pełnić wiele funkcji. LinkedIn, profesjonalny serwis społecznościowy, obsługuje wszystkie pięć elementów: budowanie kontaktów ze znajomymi offline, takimi jak współpracownicy, udostępnianie treści, takich jak dokumenty i linki, wyszukiwanie ekspertów merytorycznych, a także reprezentowanie własnej tożsamości zawodowej użytkownika. Można go również używać do celów komunikacyjnych, od wysyłania i odbierania

osobistych wiadomości e-mail po reklamowanie usług biznesowych. Dla wielu obywateli media społecznościowe stały się integralną częścią życia codziennego. Obecnie szacunki wskazują, że około 30% światowej populacji korzysta z serwisów społecznościowych i choć sieci o ugruntowanej pozycji, takie jak Facebook, mogą odnotowywać stagnację w liczbie użytkowników lub przynajmniej zmiany demograficzne użytkowników, ogólna tendencja wzrostu wykorzystania mediów społecznościowych pozostaje nieprzerwana. Według stanu na rok 2013 73% dorosłych w USA ma członkostwo w co najmniej jednym serwisie społecznościowym, a około 42% korzysta z wielu serwisów. W ciągu dziesięciu lat istnienia Facebook rozwinął się z małej sieci studentów do globalnej platformy, z której korzysta 1,19 miliarda użytkowników. Co więcej, konkurencyjne platformy, takie jak Google + i Twitter, mogą pochwalić się po około 500 milionami użytkowników, a LinkedIn ma 238 milionów użytkowników. I pomimo faktu, że najpopularniejsze usługi mediów społecznościowych są nadal zlokalizowane w USA, najbardziej zaangażowani użytkownicy pod względem średniej liczby godzin spędzonych w miesiącu na korzystaniu z sieci społecznościowych pochodzą z Izraela, Argentyny, Rosji, Turcji i Chile. Biorąc pod uwagę ich niemal wszechobecność, media społecznościowe stały się dla organów ścigania istotnym narzędziem w budowaniu przewagi konkurencyjnej przeciwko zagrożeniom związanym z przestępczością zorganizowaną. W tym celu media społecznościowe służą trzem głównym celom.

1. Przekazywanie informacji społeczeństwu w kwestiach bezpieczeństwa w celu usprawnienia zadań prewencyjnych Policji,

2. Poprawę efektywności operacyjnej poprzez poszerzenie udziału społeczeństwa, oraz

3. Poprawa zaufania społecznego do policji poprzez podniesienie dostępności i przejrzystości.

Oprócz tego media społecznościowe umożliwiają także pozyskiwanie informacji wywiadowczych

Różnorodność celów, jakim służą media społecznościowe, powoduje, że można rozróżnić aspekt performatywny od relacyjnego aspektu ich wykorzystania przez organy ścigania. Aspekt performatywny odnosi się do wykorzystania mediów społecznościowych jako instrumentu wspierania działań, czy to poprzez dystrybucję, czy pozyskiwanie informacji. Poszczególne przykłady pokazujące zastosowanie usług takich jak Twitter i Facebook w zapobieganiu przestępczości i skazywaniu można wykorzystać do zademonstrowania ich potencjalnego zastosowania. Na przykład w październiku 2008 r. notatka o stanie na Facebooku pomogła w rozwiązaniu sprawy o morderstwo pierwszego stopnia w kanadyjskim mieście Edmonton, natomiast belgijska policja ma pozytywne doświadczenia w korzystaniu z Facebooka w celu zapobiegania brutalnym atakom między znanymi wrogimi grupami. Według najnowszego badania przeprowadzonego przez Międzynarodowe Stowarzyszenie Szefów Policji (IACP) wartość mediów społecznościowych dla policji polega na ich wysokim potencjale w zakresie rozpowszechniania informacji w sytuacjach nadzwyczajnych i klęskach żywiołowych, dochodzeń w sprawie przestępstw oraz public relations i inicjatyw społecznych (IACP, 2013). Według tego samego badania 95,9% amerykańskiej policji korzysta obecnie z mediów społecznościowych w swoich dochodzeniach, a 80,4% z nich twierdzi, że media społecznościowe pomogły w rozwiązaniu przestępstwa. Oprócz funkcji performatywnej, procesy takie jak docieranie do społeczności i public relations ilustrują relacyjny aspekt korzystania z mediów społecznościowych. Użycie relacyjne odnosi się do budowania i utrzymywania relacji z członkami społeczeństwa, ze szczególnym uwzględnieniem zwiększania zaufania i legitymizacji organów ścigania. Osiąga się to poprzez pozytywne zaangażowanie opinii publicznej w serwisach społecznościowych. W tym rozdziale skupiamy się przede wszystkim na performatywnym aspekcie mediów społecznościowych dla organów ścigania, a dokładniej na gromadzeniu informacji wywiadowczych w odniesieniu do ich wyraźnego zastosowania w tym kontekście. Media społecznościowe wkraczają obecnie w codzienne życie wielu ludzi, w tym osób

łamiących prawo i prowadzących inne niegodziwe działania. To właśnie łatwość, z jaką komunikację ułatwiają serwisy społecznościowe, czyni je tak atrakcyjnymi. Ze względu na często otwarty charakter działania te są regularnie prowadzone na widoku. Jednak sama ilość informacji przesyłanych za pośrednictwem mediów społecznościowych utrudnia wykrycie tych działań. Serwisy informacyjne często czerpią informacje z mediów społecznościowych w raportach po wydarzeniu, które mogły stanowić wczesną wskazówkę o zbliżającym się przestępstwie. Jednak identyfikacja tych słupków przed wydarzeniem przypomina szukanie igły w stogu siana. Dlatego tego rodzaju wskaźniki zagrożenia często są ignorowane, co może prowadzić do scenariuszy samotnych wilków i strzelanin w szkołach (podam dwa przykłady). Organy ścigania odbierają te sygnały wskaźnikowe dopiero w następstwie zdarzenia. Korzystanie przez LEA z mediów społecznościowych opiera się na udziale obywateli, składających się zarówno z obserwatorów publicznych, jak i samych sprawców. Udział ten może przybrać formę aktualizacji statusu, informacji geograficznych lub zdjęć i filmów zawierających informacje potencjalnie obciążające. Ponadto pozornie niewinne informacje mogą okazać się kluczowym ogniwem w łańcuchu łączącym różne wpisy w mediach społecznościowych i innych źródłach informacji wywiadowczych. Ta tak zwana inteligencja typu open source może następnie zwiększyć świadomość sytuacyjną i/lub stworzyć inteligencję, która będzie przydatna do podejmowania działań. Aby ten proces zadziałał, ważna jest świadomość „typowych" cech i zachowań użytkowników, a także rodzaju informacji, które użytkownicy mediów społecznościowych publikują w Internecie. W tym rozdziale dokonamy przeglądu aktualnej wiedzy na temat użytkowników mediów społecznościowych, powodów ich zaangażowania w media społecznościowe oraz czynników wpływających na zachowania użytkowników, w tym na wiarygodność informacji o użytkownikach. Ponadto dokonujemy przeglądu szeregu potencjalnych przypadków wykorzystania mediów społecznościowych w kontekście egzekwowania prawa w celach dochodzeniowych. Należą do nich zdarzenia takie jak scenariusze samotnego wilka, sytuacje z zakładnikami i handel ludźmi. Następnie omawiamy zaangażowanie społeczne jako kluczową kwestię umożliwiającą uzyskanie szeroko zakrojonego i stałego wsparcia dla crowdsourcingu i innych zastosowań mediów społecznościowych w zwalczaniu przestępczości internetowej oraz przestępczości ułatwianej poprzez korzystanie z mediów społecznościowych.

CECHY UŻYTKOWNIKÓW MEDIÓW SPOŁECZNOŚCIOWYCH I RÓŻNICE W WYKORZYSTANIU DEMOGRAFIKI W SIECIACH

Wykorzystując usługi mediów społecznościowych jako potencjalne źródło informacji wywiadowczych, ważne jest zrozumienie składu różnych odpowiednich grup użytkowników. Poniżej znajdują się wnioski z najnowszego badania Pew, które podkreślają cechy użytkowników w najpowszechniejszych przykładach usług mediów społecznościowych:

• LinkedIn jest szczególnie popularny wśród absolwentów szkół wyższych i użytkowników z gospodarstw domowych o wyższych dochodach.

• Twittera odwiedzają głównie młodsi dorośli, mieszkańcy miast i osoby rasy innej niż biała.

• Instagram odwiedzają głównie młodsi dorośli, mieszkańcy miast i osoby niebiałe; także użytkownicy mieszkający w miastach, a nie na obszarach wiejskich.

• Pinterest przyciąga około cztery razy więcej kobiet niż mężczyzn i ma nieco większą liczbę użytkowników z wyższym wykształceniem i wyższymi dochodami wśród użytkowników.

• Z Facebooka częściej korzystają kobiety niż mężczyźni, ale jego rozkład jest prawie równy według grup etnicznych (biały-nie-Latynos, Latynos, czarnoskóry-nie-Latynos), poziomu wykształcenia, skali wynagrodzeń oraz środowiska miejskiego, podmiejskiego i wiejskiego.

Dysproporcje te pokazują, że usługi mediów społecznościowych różnią się pod względem przyciąganych przez nie osób, zwłaszcza pod względem wieku, płci i poziomu wykształcenia ich użytkowników. Ma to konsekwencje dla stylu, częstotliwości postów i rodzaju treści, których można się spodziewać w różnych usługach. Ma to również konsekwencje dla sposobu, w jaki użytkownicy zbliżają się do różnych sieci. Co ciekawe, użytkownicy zazwyczaj pozostają przy usługach, które znają. Ta „lepkość" nie tylko tworzy stosunkowo stabilne grupy użytkowników, ale także stwarza wyzwania dla wprowadzenia nowych aplikacji (np. wyspecjalizowanych aplikacji do komunikacji kryzysowej).

UZASADNIENIE KORZYSTANIA Z MEDIÓW SPOŁECZNOŚCIOWYCH

Chociaż kiedyś ludzie korzystali z Internetu, szukając anonimowości , obecnie jednym z głównych celów aktywności online jest utrzymywanie kontaktów towarzyskich. Jednak głównym powodem korzystania z mediów społecznościowych w tym sensie nie jest tworzenie nowych relacji z nieznajomymi, ale podtrzymywanie istniejących relacji. Szacuje się, że 85–98% uczestników korzysta z mediów społecznościowych w celu utrzymywania i wzmacniania istniejących sieci offline składających się z przyjaciół, rodziny lub osób o podobnych zainteresowaniach . Użytkownicy technologii mobilnych mają zatem tendencję do pozostawania w zwartych sieciach, tzw. grupach monadycznych. Grupy te są zazwyczaj zamknięte na wpływy zewnętrzne i trudno się z nimi skontaktować online, chyba że ktoś jest częścią ich społeczności offline. Poszczególne osoby różnią się znacznie pod względem podejścia do korzystania z mediów społecznościowych. Ogólnie można wyróżnić pięć różnych typów użytkowników :

1. Użytkownicy sporadyczni: Ta grupa jest najbliższa osobom niebędącym użytkownikami, ponieważ łączą się rzadko. Głównym powodem korzystania z SNS (serwisu społecznościowego) jest sprawdzenie, czy ktoś się z nimi kontaktował.

2. Lurkerzy: Głównymi powodami korzystania z SNS w tej grupie jest bierna konsumpcja treści udostępnionych online przez innych, na przykład w celu przeglądania zdjęć, znajdowania informacji o znajomych, sprawdzania, czy ktoś się z nimi skontaktował lub po prostu dla „zabicia czasu".

3. Socjaliści są zainteresowani wykorzystaniem SNS przede wszystkim do spotkań towarzyskich z przyjaciółmi, rodziną i ludźmi o podobnych poglądach.

4. Dyskutanci aktywnie wnoszą wkład w treść, pisząc i przesyłając własne wypowiedzi, zwłaszcza poprzez udział w dyskusjach i debatach.

5. Zaawansowani użytkownicy są najaktywniejszą grupą na SNS i wykazują najszerszą i najbardziej zróżnicowaną gamę zachowań.

Zróżnicowanie tych grup użytkowników jest istotne, ponieważ różnią się one pod względem prawdopodobieństwa, z jakim mogą angażować się w działania zalecane przez organy ścigania, takie jak prośby o pomoc w dochodzeniach, oraz powodów i sposobów, w jakie mogą być angażowani w Internecie (tj. socjalizatorzy mogą potrzebować innego podejścia niż przyciąganie na przykład debatantów lub lurkerów). To rozróżnienie może być szczególnie istotne, ponieważ twórcy treści, tj. bardziej aktywne grupy użytkowników, zwykle pochodzą ze stosunkowo uprzywilejowanych środowisk pod względem wykształcenia i sytuacji społeczno-demograficznej (Brake, 2014). Oznacza to nie tylko, że treści w mediach społecznościowych mogą być stronnicze skierowane do tych grup, ale także że do grup znajdujących się w niekorzystnej sytuacji może być trudniej dotrzeć i aktywować je.

WPŁYW NA ZACHOWANIA W MEDIACH SPOŁECZNOŚCIOWYCH

Na zachowania online i postrzeganie tego, co można publikować w Internecie, a co nie, wpływa szereg czynników, w tym przede wszystkim cechy użytkownika, takie jak płeć, osobowość i kultura narodowa, podejście do usługi lub osób kontaktujących się z nią w Internecie, a także konfiguracja technologiczna sieci społecznościowych. same usługi medialne. Charakterystyka użytkownika. Wczesne badania dotyczące korzystania z Internetu sugerowały, że osoby introwertyczne korzystały z Internetu częściej niż ich bardziej towarzyscy odpowiednicy. Już tak nie jest, ponieważ media społecznościowe przyciągają obecnie osoby charakteryzujące się wysokim poziomem ekstrawersji i otwartości na nowe doświadczenia. Szczególnie wśród młodszych użytkowników istnieje silny związek między ekstrawersją a intensywnym korzystaniem z mediów społecznościowych . Ponadto częstsze korzystanie z mediów społecznościowych wiąże się również z większym stopniem niestabilności emocjonalnej, chociaż dotyczy to tylko mężczyzn . (Nie)stabilność emocjonalna również odgrywa rolę w liczbie i długości czasu spędzanego w serwisach społecznościowych. Osoby mniej stabilne emocjonalnie częściej spędzają na stronach internetowych dłużej, natomiast użytkownicy bardziej stabilni emocjonalnie i bardziej introwertyczni częściej odwiedzają strony. Niestabilność emocjonalna dodatkowo wpływa na rodzaj zamieszczanych informacji. Użytkownicy o niższym poziomie stabilności emocjonalnej częściej zamieszczają na swoim profilu treści problematyczne, takie jak nadużywanie substancji czy treści o charakterze seksualnym, podobnie jak kompulsywni użytkownicy Internetu . Płeć wpływa na korzystanie z mediów społecznościowych, ponieważ kobiety mają tendencję do korzystania z serwisów społecznościowych przez dłuższy czas oraz publikują więcej zdjęć i komentarzy na swój temat niż mężczyźni. Z drugiej strony mężczyźni częściej niż kobiety korzystają z serwisów . Kultura narodowa wpływa na oczekiwania użytkowników, a także zachowania użytkowników. Porównując na przykład użytkowników z USA, Korei i Chin, Ji i inni odkryli, że osoby z Korei i Chin korzystają z portali społecznościowych jako narzędzia do wyszukiwania ekspertów w celu uzyskania porad dotyczących ważnych decyzji i wsparcia emocjonalnego. Użytkownicy z USA są zainteresowani raczej tworzeniem relacji, w których ważną rolę odgrywa dzielenie się treściami. W przypadku użytkowników z Korei i Chin nie znaleziono związku między udostępnianiem treści a relacjami. Porównanie studentów amerykańskich ze studentami niemieckimi sugeruje ponadto, że studenci amerykańscy częściej publikują na swoich stronach na Facebooku problematyczne zachowania, takie jak nadużywanie substancji psychoaktywnych lub treści o charakterze seksualnym (Karl i in., 2010). Status mniejszości wpływa również na zachowania, ponieważ członkowie grup mniejszościowych częściej korzystają z mediów społecznościowych w celach zawodowych niż prywatnych, podczas gdy członkowie grupy większościowej są bardziej zainteresowani społecznym potencjałem mediów społecznościowych (tj. czatami i osobistymi relacjami z rodziną i znajomymi). przyjaciółmi) . Mniej chętnie korzystają z usług mediów społecznościowych oferowanych przez policję. Stanowi to wyraźne wskazanie, że zachowania w Internecie kształtują demografia, a także kontekst krajowy oraz obowiązujące w nim normy i standardy kulturowe. Różnice te są istotne, gdy organy ścigania próbują nawiązać kontakt z odmiennymi grupami użytkowników, a także dla lepszego zrozumienia rozbieżności w informacjach internetowych przekazywanych przez użytkowników. Postawy wobec usług lub ludzi. Ogólnie rzecz biorąc, zaufanie poprzedza wymianę informacji. Im bardziej ludzie ufają drugiej osobie, tym chętniej są skłonni spełnić nawet natrętne prośby o informacje, przynajmniej jeśli czują, że interakcja pozostanie prywatna . Jeśli partner komunikacji jest zaufany, informacje wrażliwe są przekazywane nawet w sytuacji, gdy prywatność jest niska. Zaufanie w Internecie może sięgać tak daleko, że nawet udawanie przyjaciela może wystarczyć, aby skłonić użytkowników do ujawnienia danych osobowych . Centralna rola zaufania jest również istotna w przypadku kontaktów organów ścigania z osobami fizycznymi w mediach społecznościowych, ponieważ chęć użytkownika do nawiązania kontaktu jest powiązana z jego zaufaniem do organizacji, z którą nawiązuje kontakt. Konfiguracja techniczna. Funkcje witryny, takie jak możliwość ustawiania komunikatów o statusie, wysyłania prywatnej korespondencji lub publicznego przekazywania opinii na temat treści innych użytkowników, silnie wpływają na

zachowanie ludzi, a także rodzaj informacji, które decydują się ujawniać w Internecie. Ponadto Hampton i inni ustalili, że na zachowania użytkowników wpływają nie tylko cechy fizyczne sieci społecznościowych, ale także otoczenie społeczne, w którym użytkownicy prowadzą interakcje, przy czym użytkownicy często korzystają z sieci online w celu utrzymania istniejących sieci podczas korzystania z sieci społecznościowych w środowisku społecznościowym . Co więcej, zaawansowani użytkownicy (tj. wysoce doświadczeni technofile) oceniają jakość treści wyżej, gdy mają one dostosowywalny interfejs, podczas gdy mniej zaawansowani użytkownicy wolą raczej treści spersonalizowane.

UJAWNIANIE I WIARYGODNOŚĆ INFORMACJI

Wiele dyskusji toczy się wokół kwestii, czy informacje podawane w Internecie są godne zaufania. Czy użytkownicy zgłaszają, kim naprawdę są, czy też świadomie fałszują i fałszują informacje? Na przykład nastolatki często celowo podają w swoich profilach fałszywe informacje . Często zdarza się również, że użytkownicy świadomie uwzględniają lub pomijają dane osobowe, takie jak wiek lub status związku, aby uzyskać interesującą, „pełną" osobowość. Ogólnie rzecz biorąc, kobiety są bardziej świadome ryzyka i ryzyka, jeśli chodzi o ujawnianie informacji w Internecie, niż mężczyźni . Jednak obawy dotyczące prywatności często nie prowadzą do zachowań bardziej zorientowanych na prywatność (tzw. paradoks prywatności). Aspekty takie jak znaczenie społeczne sieci w zakresie wpływania na ogólną gotowość użytkownika do ujawniania danych osobowych wydają się być bardziej dominujące przy podejmowaniu decyzji, czy dane osobowe są publikowane publicznie, czy nie: im większe znaczenie sieci dla utrzymywania relacji społecznych, tym silniejszy ogólna gotowość danej osoby do ujawnienia prywatnych informacji wynosi . Poszczególne osoby mają również tendencję do ujawniania większej ilości informacji we wpisach na blogach, gdy można je łatwiej zidentyfikować wizualnie (tj. udostępniają swoje zdjęcie); natomiast osoby o większym poziomie obaw związanych z prywatnością zwykle korzystają z mniejszej liczby aplikacji społecznościowych. Użytkownicy obawiający się o swoją prywatność mogą wybrać trzy podejścia w celu ograniczenia możliwych zagrożeń: unikanie (np. wybieranie innych niż Internet sposobów komunikowania się, kupowania produktów itp.), rezygnacja (np. rezygnacja z gromadzenia informacji przez osoby trzecie)) oraz proaktywną samoobronę (np. korzystanie z technologii zwiększających prywatność, usuwanie plików cookie itp.). Wydaje się, że na wybór metody wpływają czynniki kulturowe. Na przykład w Sydney i Nowym Jorku użytkownicy raczej nie wybrali strategii unikania, podczas gdy użytkownicy w Bangalore i Seulu częściej unikali Internetu niż stosowali technologie zwiększające prywatność . Postawy wobec prywatności wydają się różnić wzdłuż podziału Północ-Południe i Południowy-Wschód, przynajmniej w Europie: Użytkownicy w krajach Europy Północnej uważali prywatność za kwestię osobistej odpowiedzialności, podczas gdy użytkownicy z Południa postrzegali to raczej jako kwestię zaufania. Użytkownicy w krajach Europy Południowej uważali ponadto, że ujawnienie informacji jest osobistym wyborem, podczas gdy użytkownicy w krajach wschodnich postrzegali to raczej jako wybór wymuszony. Ujawnianie i fałszowanie informacji prywatnych są zatem powiązane z demografią i zaufaniem, ale są także kwestią szerszego środowiska, w którym działa użytkownik.

ZNACZENIE DLA LEA

Pozyskując dane wywiadowcze, organy ścigania mogą chcieć wykorzystać te informacje w swoich modelach i założeniach. Jeżeli różne grupy demograficzne różnią się pod względem powodów i sposobów korzystania z mediów społecznościowych, organy ścigania muszą wziąć pod uwagę te rozbieżności podczas śledzenia i gromadzenia informacji od grup interesów. Co więcej, ponieważ relacje offline często poprzedzają relacje online, można wyciągnąć wnioski na temat kręgu znajomych danej osoby. Zrozumienie normalnego wzorca interakcji konkretnego użytkownika z mediami społecznościowymi może również okazać się wskaźnikiem krytycznych zmian w postawach. Na

przykład stopniowe zmiany w języku mogą wskazywać na radykalizację, a pojedynczy niespodziewany post z groźbami może wymagać większej uwagi niż w przypadku ciągłego publikowania takich komentarzy przez daną osobę, ale wyraźnie nie są one poważne. W tym kontekście ważne jest, aby wiedzieć, że na takie zachowania wpływają również różnice osobowości i kulturowe, co sprawia, że stosowanie jednego standardu „normalnych" i „problematycznych" zachowań w Internecie jest wątpliwe. Organy ścigania muszą mieć możliwość dopasowywania profili online do prawdziwych osób. W tym kontekście znajomość postaw wobec fałszowania danych osobowych w różnych grupach użytkowników jest niezbędna do oceny prawdopodobieństwa, a także możliwych motywacji w celu odróżnienia zachowań „normalnych" od potencjalnie „problematycznych".

SCENARIUSZE WYKORZYSTANIA LEA DLA MEDIÓW SPOŁECZNOŚCIOWYCH

Ciągły wzrost popularności i różnorodności zachowań użytkowników mediów społecznościowych, jak omówiono w sekcji „Cechy użytkowników i sposób korzystania z mediów społecznościowych", doprowadził do szeregu wydarzeń i potencjalnych scenariuszy, na których organy ścigania mogą wykorzystać potencjał dostępnych informacji w celu poprawy ich zdolności dochodzeniowych. W tej sekcji przedstawiamy szereg istotnych i aktualnych przypadków użycia potencjalnych zastosowań mediów społecznościowych w konkretnych scenariuszach skupiających się na egzekwowaniu prawa. W poprzedniej sekcji widzieliśmy, jak korzystanie z mediów społecznościowych różni się w zależności od grupy demograficznej i kulturowej, a także widzieliśmy przyczyny i rodzaje korzystania z mediów społecznościowych. Oczekiwania i zachowania różnią się także w zależności od kultury, płci, cech osobowości i stanów emocjonalnych, a stopień zaufania użytkowników do informacji znalezionych w Internecie i to, co decydują się ujawnić na swój temat – wszystko to wpływa na sposób, w jaki organy ścigania muszą ustrukturyzować swoje procesy gromadzenia danych wywiadowczych i przyjęte przez nie założenia. myśleć o znalezionych danych. W tym artykule stosujemy tę wiedzę w praktycznych przykładach tego, jak i dlaczego organy ścigania miałyby nawiązywać kontakt z mediami społecznościowymi oraz czego mogą się spodziewać, jeśli chodzi o zwiększenie zdolności i skuteczności dochodzeniowej. Przedstawiono pięć scenariuszy, w których wykorzystanie i zrozumienie mediów społecznościowych może przynieść korzyści organom ścigania. Należą do nich sytuacja ataku samotnego wilka, sytuacja zakładników, wykrywanie przestępczości zorganizowanej, zastosowanie crowdsourcingu i handel ludźmi. W ostatnich latach wzrosła liczba aresztowań policyjnych w odpowiedzi na groźby zamieszczane w Internecie w związku ze strzelaninami, zamachami bombowymi i inną działalnością przestępczą. W przypadkach takich jak szkoła Skyline High School w Sammamish w stanie Waszyngton w 2012 r., Pitman High School w New Jersey w dniu 6 stycznia 2014 r. oraz sprawa Terri Pitman w sprawie Council Pitt, Iowa w 2013 r.; matki, która na Facebooku groziła, że zastrzeli swoich synów znęcających się nad kolegami z klasy, lokalna policja została powiadomiona o wpisach w mediach społecznościowych, w których grożono strzelaniną w odpowiednich lokalizacjach, poprzez wskazówki od obserwatorów internetowych. We wszystkich trzech zidentyfikowanych przypadkach policji udało się ewakuować i przeszukać pomieszczenia, zanim pojawiło się jakiekolwiek zagrożenie. Jednakże we wszystkich przytoczonych przypadkach policja polegała na raportach niezależnych obserwatorów, takich jak koledzy z klasy, rodzice i inni widzowie, aby uzyskać świadomość zaistniałej sytuacji. Krótkie wyszukiwanie w Internecie ujawnia szereg incydentów, nie tylko związanych z groźbami strzelanin w szkołach, w których zamachy bombowe, strzelaniny i sprawcy innej działalności przestępczej zostali oskarżeni o zamiar popełnienia przestępstwa na podstawie postów opublikowanych w mediach społecznościowych ,serwisy medialne, takie jak Twitter, Facebook i Tumblr. Porównując współczesne scenariusze, takie jak te zidentyfikowane wcześniej, ze scenariuszami sprzed zaledwie dziesięciu do piętnastu lat, takimi jak strzelanina w szkole w Columbine w Jefferson w Kolorado, staje się jasne, że pojawienie się i wszechobecne wykorzystanie technologii, w tym komunikacji mobilnej i mediów społecznościowych, spowodowało zmiana kulturowa, tworząc

nowe środowisko, które wymaga ewolucji mechanizmów policyjnych niezbędnych do skutecznego reagowania na tego typu zagrożenia. Aby uzyskać dostęp do tych informacji i je wykryć, organy ścigania muszą inteligentnie monitorować media społecznościowe. Analizę sieci społecznościowych można wykorzystać do identyfikacji siatek przestępczych i dopasowywania profili na platformach mediów społecznościowych i zamkniętych rejestrach policyjnych, dodatkowo wspomaganych przez technologie takie jak rozpoznawanie twarzy, w celu stworzenia pełnego, zintegrowanego obrazu podmiotów przestępczych, ich profili internetowych i sieci, jak również pokazany przez model w scenariuszach użycia LEA dla mediów społecznościowych. A także treści tekstowe publikowane w mediach społecznościowych; zdjęcia i filmy, takie jak te zarejestrowane w serwisach takich jak Instagram, Flickr i Twitter, również stanowią potencjalnie przydatne źródło informacji. Do obrazów regularnie dołączone są metadane tekstowe, takie jak „hashtagi" i opisy treści, a także komentarze i opinie innych użytkowników platformy opisujące daną treść medialną. Ręczne przeszukiwanie tych obrazów, jeden po drugim, jest niemożliwe ze względu na ogromną ilość treści znajdujących się na platformach. Ponieważ tagowanie i geotagowanie są powszechne, eksplorację danych i przetwarzanie analityczne można wykorzystać do przyspieszenia i zautomatyzowania wydobywania informacji. Techniki eksploracji tekstu mogą również wyodrębniać dalsze metadane, takie jak nazwiska, miejsca lub działania związane z działalnością przestępczą. Techniki eksploracji i analizy danych można stosować na różne sposoby w celu poprawy jakości informacji dostępnych w dochodzeniach policyjnych. Technologie takie jak wykorzystanie sztucznych sieci neuronowych do wyodrębniania podmiotów z policyjnych raportów narracyjnych, zastosowanie podejścia algorytmicznego opartego na obliczaniu odległości euklidesowych w celu identyfikacji oszustw związanych z tożsamością przez przestępców, śledzenie tożsamości przestępców na podstawie opublikowanych wiadomości w Internecie przy użyciu algorytmów uczących się, takich jak maszyny wektorów nośnych, oraz wykorzystanie analizy sieci społecznościowych do odkrywania wzorców strukturalnych z sieci przestępczych mogą pomóc w poprawie jakości i różnorodności informacji wprowadzanych do operacji wywiadowczych organów ścigania.

MEDIA SPOŁECZNOŚCIOWE W SCENARIUSZACH „SAMOTNEGO WOLFA" DO WCZESNEJ OCENY I IDENTYFIKACJI ZAGROŻEŃ

Obecnie wywiad policyjny opiera się na doniesieniach opinii publicznej lub odbiorców gróźb, aby podjąć odpowiednie działania w odpowiedzi na zamieszczone w Internecie wpisy wskazujące na możliwe zachowania przestępcze. Ze względu na poleganie na raportach publicznych istnieje ryzyko, że zagrożenia te zostaną zignorowane lub zagłuszone szumem niewymiernej ilości informacji publikowanych każdego dnia w mediach społecznościowych. Często w przypadkach takich jak te zidentyfikowane sprawcy nie działają w imieniu szerszej organizacji przestępczej ani nie realizują zaplanowanego działania. Zamiast tego są to zazwyczaj instynktowne ataki, które są nieplanowane i irracjonalne, będące odpowiedzią na zdarzenia wywołujące emocje, dokonywane przez jednostki żądne zemsty, często mające historię niestabilności społecznej i problemów psychologicznych. W przypadkach takich jak ta organy ścigania nie są w stanie skorzystać z solidnych źródeł wywiadowczych, aby zidentyfikować bieżące lub przyszłe zagrożenie ze strony danej osoby, ponieważ jednorazowe, nieplanowane zdarzenia, takie jak zidentyfikowane wcześniej scenariusze strzelanin w szkole samotnych wilków, rzadko mają podstawowy ślad dowodowy mogą zostać wykryte przez istniejące operacje wywiadowcze LEA. Niedawne przeglądy amerykańskiej infrastruktury wywiadowczej doprowadziły do rozwoju i utworzenia „centrów fuzji", których celem jest koordynacja działań wywiadowczych i służenie organom egzekwowania prawa (LEA) w całych stanach w zakresie pozyskiwania, analizowania i rozpowszechniania informacji wywiadowczych (Departament Sprawiedliwości Stanów Zjednoczonych, 2005).). W tych centrach fuzyjnych istnieje potencjał zastosowania i integracji analityki mediów społecznościowych w przeszukiwaniu i analizie mediów

społecznościowych jako repozytorium danych wywiadowczych typu open source w odpowiedzi na pojawiające się, nieplanowane scenariusze „samotnego wilka", takie jak te omówione w rozdziale 10. W takich sytuacjach istnieją dwa potencjalne strumienie informacji, które mają potencjalną wartość dla organów ścigania. Po pierwsze, istnieje identyfikacja wpisów sprawcy zawierających wyraźne sygnały zamiaru wyrządzenia krzywdy, a po drugie, sentyment wyrażany przez interesariuszy sytuacyjnych w odniesieniu do zagrożeń i działań jednostki. Dzięki zastosowaniu technologii, takich jak przetwarzanie języka naturalnego (NLP) i techniki analizy nastrojów, możliwe jest zidentyfikowanie konkretnych wpisów, które (a) zawierają zamiary przestępcze oraz (b) zawierają odniesienia do konkretnych koncepcji, takich jak lokalizacje docelowe i metody, które należy zastosować. używane przez daną osobę (osoby). Techniki wyodrębniania nazwanych jednostek i koncepcji zapewniają użytkownikowi (w tym przypadku analitykowi w ośrodku syntezy) wyraźne odniesienie do lokalizacji i charakteru stwarzanego zagrożenia, oprócz nazwiska i lokalizacji osoby tworzącej zagrożenie. Na podstawie tych informacji można następnie przeanalizować zagrożenie i porównać je, korzystając z solidnych źródeł wywiadowczych „zamkniętego źródła", takich jak karta zdrowia i karalność osoby stwarzającej zagrożenie oraz bliskość tej osoby do miejsca, w którym występuje zagrożenie. przeciwko. To wzajemne powiązanie informacji wywiadowczych tworzy następnie solidny portfel wiedzy, który można następnie wykorzystać do oceny powagi i zasadności stwarzanego zagrożenia, co z kolei można przefiltrować do funkcjonariuszy operacyjnych w przypadkach, gdy konieczne są dalsze działania na miejscu zdarzenia. wymagany. Kluczową obawą związaną z wykorzystywaniem w ten sposób danych uzyskanych z mediów społecznościowych jest to, że oddzielenie rzeczywistych zagrożeń od wybuchów emocji i żartów niezadowolonych osób uważa się za niezwykle trudne. W tym miejscu istotne jest zrozumienie różnych typów zachowań użytkowników w mediach społecznościowych. Porównywanie wskaźników zagrożeń z mediów społecznościowych z solidnymi źródłami informacji wywiadowczych o zamkniętym źródle jest niezwykle cenne, ponieważ pomaga w odróżnieniu prawdopodobnych i prawdopodobnych zagrożeń od „hałasu" mediów społecznościowych. Dla większej wiarygodności wskazanie zagrożenia może również wywołać dodatkową analizę obecności danej osoby w mediach społecznościowych, ponieważ osoby te często używają tych samych pseudonimów i nazw użytkowników w różnych usługach, starając się zidentyfikować wszelkie inne potencjalne wskaźniki, którymi dana osoba może być zdolna i mieć zamiary popełnienia przestępstwa, którym grozili na różnych platformach mediów społecznościowych. Na przykład proces ten może obejmować identyfikację, że dana osoba posiada zdjęcia, na których pozuje z bronią, co dodatkowo potwierdza tezę, że dana osoba jest zdolna do zrealizowania zagrożenia, przed którym się uniknęła.

PODEJŚCIE OPARTE NA MEDIACH SPOŁECZNOŚCIOWYCH W SCENARIUSZU ZAKŁADNIKÓW

Sytuacje z udziałem zakładników definiuje się jako zdarzenia, w wyniku których aktor(y) (tj. biorca(-cy) zakładników) przetrzymują w niewoli jedną lub więcej osób wbrew swojej woli. Motywy tych ataków mogą być różnorodne i wahać się od motywów ekspresyjnych, takich jak wyrażanie opinii lub poglądów religijnych, po motywy instrumentalne, takie jak zysk finansowy w postaci żądania okupu (Alexander i Klein, 2009). Istnieje wiele możliwości komunikacji i wykorzystania mediów społecznościowych podczas sytuacji, w których są zakładnicy, z ofiarami, osobami biorącymi zakładników, organami ścigania, mediami i przypadkowymi świadkami, z których każdy może komentować i monitorować sytuację przed, w trakcie i po samym wydarzeniu . Ponadto biorący zakładników mogą monitorować sytuację zewnętrzną i sprawdzać tożsamość zakładników, korzystając z profili w mediach społecznościowych i wyszukiwarek internetowych, na przykład podczas ataków w Bombaju (Oh i in., 2011); mogą także wybierać zakładników za pośrednictwem mediów społecznościowych, monitorując przemieszczanie się lub rzeczy osobiste. W rzadkich przypadkach sami zakładnicy mogą również być w stanie potajemnie kontaktować się z rodziną, przyjaciółmi lub organami ścigania. Komentarze i aktualizacje w czasie rzeczywistym mogą także publikować organizacje informacyjne i osoby

postronne. Organy ścigania mogą także wykorzystywać media społecznościowe do przekazywania oficjalnych informacji, jeśli tylko mogą. uzyskać także podstawowe informacje na temat politycznych, religijnych i osobistych stanowisk osób biorących zakładników, opublikowane w Internecie, aby ułatwić negocjacje poprzez zrozumienie ich motywów. Na przykład dwa scenariusze, w których organy ścigania mogłyby korzystać z mediów społecznościowych, dotyczą zapobiegania rozprzestrzenianiu się wrażliwych szczegółów operacyjnych aby zrozumieć motywy stojące za daną sytuacją z zakładnikami. Chociaż opinia publiczna często może być pomocna, dostarczając organom ścigania kluczowych informacji, media społecznościowe stanowią również miejsce, w którym ludzie często zamieszczają posty bez zastanowienia, nieświadomi potencjalnych konsekwencji swoich działań. Publikowanie w Internecie aktualnych taktyk lub szczegółów operacyjnych, np. tych, które miały miejsce podczas ataków bombowych w Bombaju, stwarza ryzyko dla powodzenia każdej operacji. Znalezienie sposobów na ograniczenie rozprzestrzeniania się tych informacji, gdy są one poza bezpośrednią kontrolą organów ścigania, jest niezwykle ważne – policja nie może otoczyć Twittera kordonem – aby pomóc w pomyślnym rozwiązaniu takich sytuacji. Chociaż organy ścigania nie mogą zmuszać ludzi do usuwania informacji, przeszukując tweety w czasie rzeczywistym, identyfikując osoby zawierające istotne informacje i kontaktując się z osobami, które opublikowały potencjalnie wrażliwe informacje operacyjne, z prośbą o ich usunięcie, ryzyko wycieku informacji można ograniczyć. Można wykorzystać przetwarzanie języka naturalnego do identyfikacji słów kluczowych i hashtagów powiązanych z wydarzeniem, a także wdrożyć systemy ułatwiające zapewnienie zautomatyzowanej, wiarygodnej odpowiedzi w celu ograniczenia rozprzestrzeniania się szkodliwej retoryki i wspierania wirtualnej społeczności umiarkowanych, godnych zaufania porad i pozytywne wzmocnienie. Kluczowym celem jest także zapewnienie komunikacji przed wzięciem zakładników. W przeciwnym razie działałoby to jak czerwona flaga informująca o ważnych informacjach. Drugi scenariusz opiera się na zrozumieniu motywów biorących zakładników i sposobach rozwiązania sytuacji. Bez zrozumienia tła sytuacji z zakładnikami trudno jest podjąć niezbędne kroki, aby rozwiązać ją pokojowo bez dalszych incydentów lub potencjalnego dalszego pogorszenia sytuacji. Szybkie gromadzenie wszystkich potencjalnych dowodów i łączenie punktów na podstawie danych wywiadowczych uzyskanych z wpisów i profili w mediach społecznościowych, aby negocjatorzy uzbrojenia posiadali wiedzę niezbędną do skuteczniejszego wykonywania swojej pracy. Organy ścigania muszą szybko wydobywać istotne i odrzucać nieistotne informacje na temat biorących zakładników, ich interakcji społecznych oraz sympatii politycznych lub religijnych, aby szybko stworzyć profil użytkownika, uzupełniający istniejące informacje znajdujące się już w aktach policji. Informacje te mogą pochodzić z sieci społecznościowych, forów, blogów, osobistych witryn internetowych i wpisów wideo, takich jak te w serwisie YouTube. Chociaż może to nie odzwierciedlać ich pełnego profilu, może dostarczyć istotnych wskazówek na temat ich osobowości i motywów, które negocjatorzy mogą wykorzystać i wykorzystać na swoją korzyść (Mandak, 2012). Przedstawiono dwa potencjalne przypadki wykorzystania mediów społecznościowych w sytuacji przetrzymywania zakładników: kontrola rozpowszechniania informacji w tych scenariuszach oraz wykorzystanie mediów społecznościowych do sprawdzania przeszłości osób biorących zakładników. Korzystając z profili w mediach społecznościowych, organy ścigania mogą zidentyfikować dane demograficzne, z którymi identyfikują się biorący zakładników, ich motywacje w oparciu o udostępnianie treści lub zidentyfikować ich relacje poprzez interakcje w Internecie i wykorzystać tę wiedzę, aby poinformować decydentów o tym, jak najlepiej działać i kontynuować negocjacje.

ANALIZA DANYCH W MEDIACH SPOŁECZNOŚCIOWYCH DOTYCZĄCYCH PRZESTĘPCZOŚCI ZORGANIZOWANEJ

Aresztowanie Bernardo Provenzano, wyższego rangą członka mafii sycylijskiej, w 2006 r., po 43 latach ukrywania się, ujawniło kwestię, w jaki sposób osoba przestępcza taka jak ta mogła unikać władz, a

jednocześnie nadal kierować imperium przestępcze. Provenzano był w ciągłym ruchu, komunikując się za pomocą pizzini, drobnych notatek pisanych na maszynie, dostarczanych mu ręcznie przez zaufanych asystentów . Po aresztowaniu Provenzano posiadał pięć egzemplarzy Biblii, z których jeden był pełen tajemniczych notatek. Arturo Castellanos, przywódca meksykańskiej mafii przebywający w jednym z najsurowszych więzień w Ameryce, Pelican Bay State w Północnej Kalifornii, wysłał list do Florencia 13, wielopokoleniowego gangu ulicznego w południowym Los Angeles. Castellanos w swoim liście podkreślił szereg zasad, czyli reglas, dotyczących tego, jak jego zdaniem mafią należy kierować na poziomie ulicy. W szczególności zasady te określały, w jaki sposób powinny być zarządzane gangi uliczne i ich podgrupy, w jaki sposób należy realizować sprzedaż narkotyków, prostytucję i inną nielegalną działalność oraz w jaki sposób należy rozstrzygać spory. W obu przypadkach wyraźnie pokazano, że komunikacja odgrywa główną rolę w sposobie, w jaki zorganizowane podmioty przestępcze wykonują swoją nielegalną działalność w celu zachowania anonimowości. Można bezpiecznie założyć, że przywódcy przestępczości zorganizowanej korzystają z mediów społecznościowych, takich jak Twitter czy Facebook, aby w ten sam sposób komunikować się ze swoimi grupami. Komunikacja ta może być ponownie prowadzona w sposób zagadkowy, wykorzystując konta w mediach społecznościowych zawierające fałszywe dane osobowe i zdjęcia, używając określonych terminów w celu przekazania wiadomości. Złożoność organizacji przestępczości zorganizowanej jeszcze bardziej utrudnia monitorowanie komunikacji między jej członkami. Sieć społecznościową można postrzegać jako strukturę węzłów (często reprezentujących ludzi), połączonych ze sobą pewnym rodzajem relacji . Algorytmy eksploracji tekstu można wykorzystać do wyodrębnienia podejrzanych słów kluczowych z kont w mediach społecznościowych. Można następnie monitorować działanie tych kont i zbierać wszystkie ich posty. Na podstawie zebranych postów można opracować kontekst formalny. Aby wyodrębnić najważniejsze koncepcje z tych postów i zwizualizować je w postaci siatki pojęciowej, można zastosować oprogramowanie do formalnej analizy koncepcji (FCA). Badanie kraty pojęciowej pozwoli zidentyfikować słowa kluczowe, które pojawiają się najczęściej w zebranych postach. Na podstawie tych słów kluczowych można zebrać do analizy konta, które z nich korzystały, w celu sformułowania bardziej szczegółowych wniosków. Formalna analiza koncepcji to tylko jeden przykład technologii, którą można zastosować do agregowania i podsumowywania danych. Formalna analiza koncepcji może być bardzo przydatna w analizie komunikacji opartej na mediach społecznościowych pomiędzy członkami mafii. Zebrane dane mogą wyjaśnić sposób, w jaki przestępcy zorganizowani komunikują się ze sobą oraz hierarchię, jaką przestrzegają. Ponadto może wyjaśnić rolę każdego członka organizacji przestępczej, sposób organizacji działalności przestępczej oraz sposoby przewidywania przyszłej działalności przestępczej organizowanej przez organizacje mafijne i zapobiegania jej. Ponadto zastosowanie analizy koncepcji formalnych w mediach społecznościowych może skutkować łatwiejszą penetracją organizacji o charakterze mafijnym przez policję, co umożliwi likwidację takich grup

CROWDSOURCING Z PLATFORMĄ ZBIOROWEJ INTELIGENCJI

Dane pochodzące z crowdsourcingu mają ogromne znaczenie w sytuacjach kryzysowych. Crowdsourcing umożliwia szybki i skuteczny przepływ informacji między specjalistami ds. zarządzania kryzysowego a społeczeństwem. Istnieje wiele narzędzi, takich jak Pathfinder i Many Eyes, które są wykorzystywane do analizy informacji pochodzących od społeczności. platformy takie jak Ushahidi i mapy kryzysowe Google są już wykorzystywane do pozyskiwania informacji w sytuacjach reagowania na klęski żywiołowe. Crowdsafe , aplikacja mobilna, która umożliwia użytkownikom wprowadzanie danych dotyczących przestępczości w celu zidentyfikowania hotspotów, pomaga również użytkownikom wyznaczyć trasy do domu, które ich omijają. Oprócz korzystania z crowdsourcingu w celu koordynowania działań niesienia pomocy, organy ścigania mogą również chcieć pozyskiwać informacje z crowdsourcingu w trakcie zdarzenia kryzysowego i po nim, aby zapewnić zarówno

świadomość sytuacyjną, jak i poskładać w całość prawdziwy charakter wydarzeń, np. ręczne przeglądanie tych danych jest prawie niemożliwe. Włączanie organów ścigania w pętlę pozyskiwania tłumów jest również konieczne, ale jak pokazały zamachy bombowe w Bostonie w 2013 r.; Same dane publiczne pochodzące z crowdsourcingu niekoniecznie prowadzą do właściwych wniosków z dochodzeń . Podobnie jak w przypadku crowdsourcingu, inteligencja zbiorowa jest wynikiem zbiorowych i wspólnych wysiłków wielu osób mających wspólny cel. Platforma inteligencji zbiorowej łączy dane z wielu różnych źródeł (np. repozytoriów wywiadu typu open source). Dane otrzymane w drodze odwołań w ramach crowdsourcingu za pośrednictwem mediów społecznościowych oraz dane zamknięte, które nie są udostępniane opinii publicznej, są następnie łączone z specjalistyczną wiedzą funkcjonariuszy LEA, ekspertów dziedzinowych i analityków w celu opracowania działań, wyników lub elementów składowych wiedzy. Wyniki tych analiz mogą wrócić do domeny publicznej w celu udoskonalenia i reorganizacji działań interesariuszy scenariusza w oparciu o informacje dostarczone przez organy ścigania. Platforma tego typu byłaby przydatna nie tylko w sytuacji zarządzania kryzysowego, ale także do śledzenia zdarzeń, takich jak przestępczość zorganizowana związana z handlem bronią, handlem narkotykami i gangami piorącymi pieniądze . W ramach platformy zbiorowej inteligencji można wykorzystać i zintegrować wiele technologii. Formalna analiza koncepcji jest jednym z takich przykładów i może być wykorzystywana do analizy danych generowanych przez media społecznościowe, które są potencjalnie powiązane ze zdarzeniami przestępczymi. W FCA obiekt można zwykle umieścić na określonym poziomie hierarchii tylko wtedy, gdy zawiera wszystkie atrybuty obecne na tym poziomie. W szczególności podczas analizy danych tekstowych problematyczny jest szeroki zakres wyrażeń, których można użyć do wyjaśnienia dokładnie tej samej sytuacji. Dwa potencjalne sposoby rozwiązania tego problemu to wykorzystanie leksykalnej bazy danych, takiej jak Wordnet , do mapowania synonimów dla każdego z atrybutów, a drugi polega na wprowadzeniu odporności na błędy dla FCA. Oznacza to akceptowanie obiektów na określonym poziomie hierarchii, nawet jeśli nie odpowiadają one wszystkim atrybutom, ale odpowiadają pewnej liczbie z nich powyżej określonego progu. Zapobiega to przedostawaniu się sytuacji, w których doszło do nieudanego zdarzenia, przedostając się przez metaforyczną sieć FCA. Oznacza to, że platformę inteligencji zbiorowej można udoskonalać w miarę dodawania większej ilości informacji, a w celu dalszego ulepszania i udoskonalania wyników można zastosować dalsze techniki analityczne, takie jak uczenie maszynowe, grupowanie i dodatkowa klasyfikacja. Dynamika sytuacji kryzysowej powoduje, że wydarzenia mogą się szybko zmieniać. Przykładowe technologie takie jak FCA mogą oznaczać ciągłe przewartościowanie liczby obiektów występujących na różnych pozycjach w hierarchii i wprowadzenie nowych terminów. Wzrost liczby obiektów znajdujących się niżej w hierarchii wskazuje na zmianę sytuacji lub widoczność, na którą organy ścigania również mogą być zmuszone zareagować. Dodanie nowego terminu może wskazywać na nowe zdarzenie, na przykład słowo „bandyta" może pojawiać się z określoną nazwą miejsca, ale pięć minut później system zaczyna wykrywać drugą nazwę miejsca, a obiekty są rozdzielane pomiędzy dwie . Może to wskazywać, że jest więcej niż jeden bandyta lub że są w ruchu. Tego typu informacje zwykle przyjmują formę nieustrukturyzowanych tekstów, niezweryfikowanych lub częściowych raportów oraz wiedzy ludzkiej, która niekoniecznie jest zawarta w ścieżce papierowej. Jednak zebranie wszystkich tych informacji z różnych źródeł i połączenie kropki między nimi są niezbędne do śledzenia przestępczości zorganizowanej. Platforma inteligencji zbiorowej jest wymagana do importowania, agregowania, filtrowania, analizowania, wizualizowania, a także prezentowania tych informacji w zwięzły sposób. Aplikacja agregująca wiadomości Summly była pionierem pomysłu łączenia wiadomości i mediów społecznościowych, mając jednocześnie świadomość, że większość użytkowników nie chce długich raportów, ale krótkich fragmentów podsumowań. To samo rozumowanie można zastosować do opracowania sytuacji kryzysowych w celu dostarczenia raportów służbom ratowniczym, społeczeństwu i osobom w centrach kontroli. W szczególności crowdsourcing wymaga zaangażowania społeczeństwa i przekazywania informacji.

Prawdopodobnie w dyskusji wezmą udział głównie debatanci i zaawansowani użytkownicy portali społecznościowych, dlatego organy ścigania powinny zdawać sobie sprawę z wszelkich uprzedzeń demograficznych, które mogą mieć wpływ na otrzymywane przez nich informacje. Organy ścigania muszą również rozważyć, w jaki sposób chcą otrzymywać informacje, ponieważ użytkownicy wolą korzystać ze znanych im usług. Użytkownicy mogą również mieć obawy dotyczące prywatności w związku z ujawnianiem informacji oznaczonych znacznikami geograficznymi lub przyciąganiem niechcianej uwagi.

ZASTOSOWANIE MEDIÓW SPOŁECZNOŚCIOWYCH W SCENARIUSZACH HANDLU LUDŹMI

Handel ludźmi jest zróżnicowanym i złożonym problemem międzynarodowym. Ze względu na jego zglobalizowany, transgraniczny i zróżnicowany charakter, każda reakcja na handel ludźmi musi mieć podobny zakres. Handel ludźmi obejmuje wszelkie wysiłki zmierzające do nielegalnego transportu ludzi przez granice przy użyciu siły lub z wykorzystaniem gróźb, takich jak uprowadzenie, oszustwo, podstęp i przymus, przy czym organizacje przestępcze stale identyfikują i wykorzystują nowe trasy, środki transportu i preteksty do nielegalnego handel ludźmi (UNODC, 2004). Handel ludźmi jest nie tylko problemem globalnym, ale także narastającym – brytyjska agencja NCA (Krajowa Agencja ds. Przestępczości) odnotowała 9% wzrost liczby wyroków skazujących związanych z handlem ludźmi w Wielkiej Brytanii w 2012 r. o 9% rok do roku (UKHTC, 2013). Aby ulepszyć podstawy architektoniczne strategii obrony przed handlem ludźmi, wymagane jest skoordynowane, wielodyscyplinarne podejście łączące wymogi w celu maksymalizacji identyfikacji działalności przestępczej oraz pociągnięcia do odpowiedzialności osób i nielegalnych organizacji za nią odpowiedzialnych (UNODC , 2012). Media społecznościowe stanowią potencjalne źródło przewagi konkurencyjnej organów ścigania nad organizacjami przestępczymi popełniającymi przestępstwa takie jak handel ludźmi i często są uważane za niewykorzystane repozytorium informacji wywiadowczych typu open source, które tradycyjnie są niedoceniane w umysłów i praktyk funkcjonariuszy policji w wyniku zakorzenionych kulturowo uprzedzeń, które są głęboko zakorzenione w kulturze i mechanizmach organizacyjnych współczesnej policji . Głęboko zakorzeniony opór, taki jak ten, wymaga, aby wszelkie nowe podejścia były poparte mechanizmami organizacyjnymi umożliwiającymi zarządzanie wiedzą, co ułatwiłoby integrację wszelkich nowych podejść opartych na danych wywiadowczych do zwalczania zagrożeń związanych z przestępczością zorganizowaną, taką jak handel ludźmi. W odpowiedzi na ten wymóg media społecznościowe są tylko jednym z zasobów, które można wykorzystać w odpowiedzi na stale rosnące zagrożenie handlem ludźmi poprzez wykorzystanie eksploracji tekstu, ekstrakcji, kategoryzacji i analizy informacji. Chociaż jest mało prawdopodobne, że agenci zajmujący się handlem ludźmi sami będą szczegółowo opisywać charakter swojej działalności w tekstach i obrazach publikowanych w mediach społecznościowych, obserwatorzy otoczenia (tj. ogół społeczeństwa) potencjalnie będą zamieszczać posty odnoszące się do zachowań, które są podejrzane lub nietypowe. W niedawnej sprawie dotyczącej handlu ludźmi w południowo-wschodniej Anglii węgierski gang handlarzy został skazany za przewiezienie ponad 50 nastoletnich dziewcząt do Wielkiej Brytanii w celu prowadzenia nielegalnej siatki prostytucyjnej. Zdarzenia takie jak ten stanowią potencjalny przypadek użycia do zilustrowania zastosowania analityki mediów społecznościowych i wydobywania informacji w zwalczaniu zagrożenia, jakim jest handel ludźmi. W zidentyfikowanym przypadku pewna liczba ofiar handlu ludźmi została przemycona do akademików na Uniwersytecie Sussex w celach prostytucji (Campbell, 2014). W przypadku takich wydarzeń jak to jest prawdopodobne, że inni mieszkańcy korytarzy i studenci lokalnych uniwersytetów umieściliby ciekawe posty w mediach społecznościowych, takich jak Twitter i Facebook, w związku z niezwykłym charakterem nagłego pojawienia się wielu kobiet z Europy Wschodniej na terenie obiektu i rzadko można je zobaczyć lub usłyszeć. Chociaż z postów obserwatorów mogło nie wynikać, że dane osoby były w rzeczywistości ofiarami handlu ludźmi i działały w kręgu przymusowej prostytucji, techniki analityczne, takie jak przetwarzanie języka

naturalnego (NLP) i wyodrębnianie nazwanych podmiotów, umożliwione dzięki technologiom przeszukiwania sieci, można używać w połączeniu z bazą wiedzy zawierającą specjalistyczną wiedzę ekspertów ds. handlu ludźmi, która mogłaby wyodrębnić informacje tekstowe z mediów społecznościowych wskazujące wiele raportów o nietypowych zachowaniach z tego samego miejsca, które następnie zostałyby podzielone na kategorie w celu wskazania, że w rzeczywistości może to być związane z potencjalną nielegalną działalnością, taką jak handel ludźmi. Filtrując i łącząc źródła informacji, analitycy organów ścigania mogą zacząć gromadzić wystarczającą ilość informacji, aby stworzyć reprezentację obserwowanego środowiska, poprzez agregację informacji w oparciu o dane o lokalizacji oznaczone tagiem geograficznym, które są osadzone w treściach mediów społecznościowych. Aspekt repozytorium dowolnego proponowanego systemu zostałby wypełniony wiedzą dziedzinową składającą się z prawdopodobnych wskaźników działalności związanej z handlem ludźmi, zarówno jeśli chodzi o ofiary, właściwości wykorzystywane przez osoby zaangażowane, jak i cechy samych sprawców, a wszystko to byłoby powiązane z regułami językowymi zaprojektowanymi aby wybrać terminy slangowe i posty z mediów społecznościowych, które odwołują się do aktywności pokrywającej się z tą zapisaną w bazie wiedzy . W przeszłości policja i organy ścigania polegały na bezpośrednim zgłaszaniu podejrzanych działań przez obserwatorów, jednak w nowym środowisku, które powstało w wyniku ery informacji, te same informacje są rozproszone w mediach społecznościowych poprzez wpisy pasywnych, intuicyjnych obserwatorów , umożliwiające wczesną identyfikację nielegalnych działań na podstawie agregacji słabych wskaźników wyrażonych za pośrednictwem platform mediów społecznościowych, takich jak Twitter i Facebook.

ZAANGAŻOWANIE PUBLICZNE W MEDIACH SPOŁECZNOŚCIOWYCH

Wysiłki na rzecz pozyskiwania środków od społeczności, na przykład w celu wsparcia dochodzeń w sprawie przestępstw lub podczas kryzysów, zależą od chęci obywateli do wspierania organów ścigania i nawiązywania z nimi kontaktu w mediach społecznościowych. Może to nie być logiczny krok dla wszystkich obywateli, jak pokazują różnice w potencjalnych cechach użytkownika opisane w sekcji „Funkcje Użytkownicy i wykorzystanie mediów społecznościowych.” Usługi takie jak Amber Alert (program Departamentu Sprawiedliwości Stanów Zjednoczonych mający na celu zwiększenie świadomości społecznej na temat osób zaginionych) wymagają stabilnej społeczności, która jest stale dostępna. Ale w jaki sposób organy ścigania mogą przyciągnąć obywateli i związać ich z obecnością w mediach społecznościowych? Organizacja pozarządowa z Kosowa InternewsKosova wraz z Balkan Investigative Reporting Network (BIRN) stworzyły platformę internetową (www.kallxo.com) dla obywateli Kosowa, umożliwiającą zgłaszanie przypadków korupcji za pośrednictwem mediów społecznościowych, SMS-ów i Internetu. Rok po uruchomieniu platformy zgłoszono 900 przypadków, a około 30 gmin w Kosowie umieściło ramkę iFrame platformy na swoich stronach internetowych (Program Narodów Zjednoczonych ds. Rozwoju, 2014). W Wielkiej Brytanii udostępniono usługę publiczną (http://www.police.uk), która wyświetla statystyki przestępczości dla każdego adresu w kraju, umożliwiając obywatelom Wielkiej Brytanii przeglądanie statystyk przestępczości na ich obszarze lokalnym. Niedawne badanie dotyczące policyjnych usług mediów społecznościowych przeprowadzone z udziałem obywateli Republiki Czeskiej, Rumunii, Byłej Jugosłowiańskiej Republiki Macedonii i Wielkiej Brytanii wykazało, że zaufanie do policji jest jednym z głównych czynników decydujących o tym, czy ludzie chcą korzystać z takich usług, czy nie . W tym przypadku organy ścigania są traktowane tak samo jak użytkownicy indywidualni . Co więcej, brak wiedzy i umiejętności związanych z wykorzystaniem technologii informatycznych jest czynnikiem ograniczającym wykorzystanie mediów społecznościowych do zgłaszania przestępstw przez znaczną część populacji . Ponadto ludzie chcą mieć pewność, że ich anonimowość jest zabezpieczona, gdy zgłaszają przestępstwo, co nie zawsze jest możliwe lub jasne, gdy rozważa się korzystanie z mediów społecznościowych. Organy ścigania starają się nakłonić ludzi do zgłaszania informacji o przestępstwie

za pomocą nagród finansowych, jednak nawet w przypadku mediów społecznościowych wiele osób boi się podawać takie informacje. Mimo że zaufanie często buduje się w trybie offline, organy ścigania mogą popracować nad prezentacją usług mediów społecznościowych i własnym zachowaniem wobec obywateli, którzy z nich korzystają. Akceptacja wirtualnego świadczenia usług publicznych jest powiązana z następującymi czterema aspektami: oczekiwaniami dotyczącymi działania witryny, obecnością społeczną (tj. „poczuciem bycia ze sobą"), wpływami społecznymi przez odpowiednie inne osoby, które uważają, że korzystanie z tych witryn jest pozytywne, oraz lęk przed komputerem. Przy rozważaniu akceptacji ważne są zwłaszcza aspekty emocjonalne, a przede wszystkim obecność społeczna. Sugeruje to, że media umożliwiające natychmiastową i osobistą komunikację, bardzo przypominającą spotkania twarzą w twarz, są chętniej akceptowane przez obywateli niż platformy umożliwiające jedynie sporadyczną wymianę tekstową. Na przykład w przypadku technologii wirtualnego zgłaszania przestępstw pewne opory wynikają z braku prawdziwego kontaktu z ludźmi. To, czy dana osoba jest skłonna skorzystać z technologii, czy nie, zależy od jej reakcji poznawczych, pozytywnych i afektywnych. Reakcje poznawcze są powiązane z osobistymi przekonaniami, reakcje twórcze są związane z chęcią jednostki do zaangażowania, a reakcje afektywne są powiązane z emocjami jednostki . Po utworzeniu platformy mediów społecznościowych ważną kwestią staje się przywiązanie użytkowników do platformy w celu wspierania aktywnej, stałej społeczności. Reagowanie i odpowiadanie na posty użytkowników to jeden z najskuteczniejszych sposobów zaangażowania użytkowników w usługę, gdyż zwiększa wartość uczestnictwa w oczach samych użytkowników . Dlatego otrzymanie odpowiedzi na pierwszy post zwiększa prawdopodobieństwo, że dana osoba opublikuje go ponownie. Ponadto istotne jest, aby informacje podawane w sieciach były postrzegane jako zgodne z prawdą; w przeciwnym razie zaufanie do usługi i postrzegana wartość usługi spadną. Ważną rolę odgrywa także to, kto przekazuje informacje. Niestety, wydaje się, że płeć nadal odgrywa rolę w postrzeganiu wiarygodnych informacji. Na przykład blogi autorów płci męskiej są często uważane za bardziej wiarygodne niż blogi autorów płci żeńskiej . Co więcej, wiarygodność informacji jest również wyższa, jeśli źródło jest oficjalne, a nie nieoficjalne, ale tylko wtedy, gdy komunikat pochodzi od mężczyzny.

OD MEDIÓW SPOŁECZNOŚCIOWYCH DO INTELIGENCJI LEA

Ponieważ media społecznościowe są obecnie wszechobecne, można je zastosować w dowolnych scenariuszach LEA. Obecnie dostępna jest różnorodna i szeroka gama platform mediów społecznościowych; a liczba i różnorodność tych platform stale rośnie. Organy ścigania mogą wykorzystywać media społecznościowe na trzy główne sposoby:

1. Przeszukiwanie i monitorowanie źródeł mediów społecznościowych poprzez śledzenie publicznych komentarzy oraz przeglądanie profili i postów kryminalnych

2. Organy ścigania prowadzą bezpośrednią komunikację i interakcję ze społeczeństwem za pośrednictwem własnych kont w mediach społecznościowych

3. Skoordynowane przez LEA informacje pochodzące z crowdsourcingu

Po zebraniu tych danych organy ścigania muszą wyodrębnić, oczyścić, przefiltrować i agregować dane nieustrukturyzowane w formatach nadających się do odczytu maszynowego. Rodzaje pobieranych danych mogą obejmować:

• Nieustrukturyzowany tekst z tweetów i innych wpisów

• Wideo i obrazy

• Informacje geograficzne

• Informacje o sieciach społecznościowych

• Dane osobowe, w tym wiek, lokalizacja, rodzina, upodobania, antypatie itp.

Po zebraniu wszystkich tych danych należy je przetworzyć i przeanalizować, aby organy ścigania mogły je w sensowny sposób wykorzystać. Przykładami takich technik są:

• Rozpoznawanie twarzy i dopasowywanie zdjęć do obrazów przechowywanych w aktach

• Dopasowywanie profili platform mediów społecznościowych i raportów policyjnych

• Przetwarzanie języka naturalnego w celu zrozumienia tekstu nieustrukturyzowanego

• Analiza nastrojów w celu monitorowania opinii publicznej

• Geo-tagowanie i rozdzielczość lokalizacji w celu śledzenia ruchów i kluczowych miejsc

• Analiza sieci społecznościowych w celu mapowania przyjaciół, znajomych i interakcji

Te rozbieżne analizy można następnie filtrować, przetwarzać i konsolidować w przydatne, wiarygodne informacje, a następnie oceniać je osoby posiadające wiedzę specjalistyczną w danej dziedzinie. Wyniki tych procesów można następnie zastosować w szeregu scenariuszy, takich jak przestępczość zorganizowana, samotny wilk, handel ludźmi, sytuacje związane z zakładnikami oraz zdarzenia kryzysowe i terrorystyczne, jak opisano wcześniej w tym rozdziale. To jednak nie koniec pętli. W trakcie całego procesu, w miarę gromadzenia większej ilości danych wywiadowczych, są one wykorzystywane ponownie w poszukiwaniach w celu udoskonalenia i uczynienia narzędzi dokładniejszymi i bardziej ukierunkowanymi, umożliwiając uwzględnienie nowych informacji w celu wzmocnienia potencjalnych wyników dla organów ścigania i zwiększenia wiarygodności ich danych wywiadowczych.

UWAGI KOŃCOWE

W miarę jak zagrożenia i praktyki przestępcze ewoluują wraz z otaczającym je środowiskiem, zasoby wywiadowcze oferowane przez media społecznościowe stają się ważnym atutem w arsenale dochodzeniowym organów ścigania. Media społecznościowe oferują niezrównane repozytorium przemyślanych operacji policyjnych; których analiza odgrywa znaczącą rolę w ocenie ważności, wiarygodności i dokładności informacji uzyskanych z repozytoriów danych wywiadowczych typu open source, takich jak media społecznościowe. Techniki takie jak eksploracja tekstu, NLP (przetwarzanie języka naturalnego) i analiza nastrojów zapewniają zróżnicowany zestaw narzędzi, które można zastosować, aby lepiej informować decydentów LEA i prowadzić do identyfikacji miejsca, w którym prawdopodobne jest wystąpienie przestępstwa, kto prawdopodobnie go popełni oraz charakteru samego zagrożenia. Jednak w tym kontekście potrzebne są nie tylko szczegóły techniczne dotyczące wyszukiwania i analizowania informacji z mediów społecznościowych, ale także dogłębna wiedza na temat osób korzystających z usług, ich motywacji i zachowań. Przedstawiliśmy krótki przegląd aktualnej wiedzy na temat korzystania z mediów społecznościowych, w tym charakterystyki użytkowników i czynników wpływających na zachowania użytkowników w Internecie. Następnie przedstawiliśmy przegląd scenariuszy użycia, aby pokazać, w jaki sposób media społecznościowe mogą wspierać organy ścigania w ich działaniach. Scenariusze te ustanawiają przypadki użycia mediów społecznościowych w zapobieganiu, przewidywaniu i rozwiązywaniu szerokiego zakresu zagrożeń przestępczych, pokazując w ten sposób potencjalną zdolność mediów społecznościowych do wykorzystania przez organy ścigania.

Wzrost ubezpieczenia od odpowiedzialności cybernetycznej

KRÓTKA HISTORIA UBEZPIECZEŃ

Chociaż „zagrożenia cybernetyczne” mogą być nowym zjawiskiem, potrzeba ochrony przedsiębiorstw przed zagrożeniami i stratami poniesionymi w przypadku poważnej katastrofy jest prawie tak stara jak sama cywilizacja. Ludzie na przestrzeni dziejów stosowali techniki zarządzania ryzykiem, aby zmniejszyć prawdopodobieństwo straty lub zmniejszyć skutki w przypadku skrystalizowania się i wystąpienia zagrożenia. Już w II wieku chińscy kupcy podróżujący przez niebezpieczne rzeki rozprowadzali swoje towary na wielu statkach, aby zminimalizować straty w przypadku utraty jednego lub więcej w wzburzonych wodach, a to Rzymianie i Grecy wprowadzili koncepcję ubezpieczenia na życie i zdrowie, gdzie krewni poległych w bitwie lub na morzu odnieśliby korzyść w postaci otrzymania płatności na pokrycie pogrzebu i przyszłych kosztów utrzymania. Ubezpieczenie na wypadek strat towarzyszy nam od wieków, od wczesnych Babilończyków po Rzymian i Greków. Niedawno, w XVII wieku, kawiarnia Edwarda Lloyda w Londynie wyruszyła w nową podróż, ponieważ szybko stała się znana jako miejsce, w którym można uzyskać ubezpieczenie morskie. W świecie coraz bardziej zależnym od żeglugi i produktów z całego świata potrzeba ochrony przedsiębiorstw prowadzących handel tymi niebezpiecznymi drogami wodnymi była dla wszystkich oczywista. Firma Lloyds of London ugruntowała swoją pozycję światowego gracza w ubezpieczeniach morskich, kiedy młody mężczyzna nazwiskiem Cuthbert Heath dołączył do Lloyds w 1877 r. Cuthbert Heath, ubezpieczyciel w Lloyds, wkrótce opracowywał polisy dotyczące ubezpieczeń i reasekuracji niezwiązanych z morzem, w tym ubezpieczeń od ognia ubezpieczenia, ubezpieczenia od włamań, w tym polisy na rynek amerykański. To wyprowadziło firmę Lloyds ze szlaków żeglugowych i otworzyło nowe i wschodzące rynki, a także ustanowiło szablon, którego Lloyds przestrzega do dziś, szczycąc się objęciem nowych i złożonych obszarów ryzyka.

UBEZPIECZENIE PRZERWY W DZIAŁALNOŚCI

Dzisiejszy świat jest zupełnie inny niż w 1877 r., ale Lloyds stworzył ramy dla współczesnego ubezpieczenia od przerwania działalności gospodarczej (BI Insurance), na którym nadal polega wiele przedsiębiorstw. W zależności od zakresu ubezpieczenia, BI Insurance zapewnia ochronę przed utratą zarobków lub zysków firmy w mało prawdopodobnym przypadku, gdy zostanie ona zamknięta na pewien okres z dowolnej liczby powodów, w tym (ale nie wyłącznie); pożar, powódź, trzęsienie ziemi lub akty terroryzmu. Zazwyczaj dostępne są trzy rodzaje ubezpieczenia BI:

• Ubezpieczenie „Przerwa w działalności” rekompensuje ubezpieczonemu utracone dochody w okresie renowacji lub w czasie niezbędnym do naprawy lub przywrócenia fizycznego uszkodzenia ubezpieczonego mienia;

• „Przedłużona przerwa w działalności” (EBI) zapewnia typową ochronę

ograniczone czasowo, w przypadku dochodów utraconych po naprawie majątku, ale zanim dochody te powrócą do poziomu sprzed szkody; I

• „Warunkowa przerwa w działalności” (CBI) zapewnia ubezpieczenie na wypadek utraty dochodów ubezpieczonego w wyniku szkód fizycznych nie w jego własnym mieniu, ale w mieniu osób trzecich (tj. szkoda nie miała wpływu na majątek ubezpieczonego, ale dotknęła kogoś innego) na których polegają i w związku z tym wpływa na ich zysk).

Ubezpieczenie BI w dowolnej formie uznawane jest za bardzo wartościowy i niezbędny rodzaj ubezpieczenia, który dla wielu przedsiębiorców jest podstawowym ubezpieczeniem niezbędnym do prowadzenia działalności. Chociaż ubezpieczenie BI Insurance i jego warianty obejmują utratę zysków, zwrot kosztów i kompensację szkód w majątku fizycznym, takim jak własność, rzadko, jeśli w ogóle, pokrywają koszt aktywów niefizycznych. Oznacza to, że BI Insurance może zwrócić powodowi stratę komputera, ale jest mało prawdopodobne, aby zrekompensował mu dane, które się na nim znajdują,

mimo że dane przechowywane w tym urządzeniu mogą być wielokrotnie warte wartości samego urządzenia. Lukę tę, zdaniem niektórych, wypełnia dodatkowa forma ubezpieczenia znana jako ubezpieczenie od odpowiedzialności zawodowej (PI Insurance), która może pomóc chronić firmę w przypadku wniesienia przeciwko niej roszczeń przez klienta, który uważa, że doszło do jakiejś formy zaniedbania lub błędu (zamierzonego lub nieumyślny). W organizacjach świadczących usługi profesjonalne, takie jak instytucje finansowe lub osoby prawne, ta forma ubezpieczenia jest niezwykle ważna, ponieważ ryzyko sporów sądowych jest często niezwykle wysokie. Ta forma ubezpieczenia może pokryć również koszty kar lub grzywien wynikających z naruszenia danych i przybliża nas do nowej formy ubezpieczenia, która zaczęła zyskiwać na znaczeniu i szybko staje się kolejnym „must have" dla firm działających w epoka nowożytna; Odpowiedzialność za ubezpieczenie cybernetyczne.

CZYM JEST CYBERODPOWIEDZIALNOŚĆ?

Jak widzieliśmy, historycznie uważano za rozsądne zabezpieczanie majątku fizycznego przedsiębiorstwa poprzez ubezpieczenie (ubezpieczenie BI), a później roszczenia z tytułu szkód spowodowanych błędem lub zaniedbaniem (ubezpieczenie PI). Jednak w miarę jak świat staje się coraz bardziej wzajemnie powiązany, a nasza zależność od technologii wzrasta, zagrożenie nieuprawnionym dostępem lub utratą danych osobowych spowodowało potrzebę ochrony przed ryzykami, których wcześniej nie można było ubezpieczyć. Dlatego rynek ubezpieczeniowy zareagował, tworząc produkt „Cyber Liability Insurance" (CL Insurance). Ubezpieczenie CL ma na celu pokrycie ryzyka związanego z naruszeniami danych, które zgodnie z przepisami dotyczącymi prywatności i komunikacji elektronicznej (2011) obejmują „przypadkowe lub niezgodne z prawem zniszczenie, utratę, zmianę, nieuprawnione ujawnienie lub dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetworzone." Chociaż CL Insurance jest stosunkowo nowym produktem, produkty rozwijają się szybko, ponieważ zarówno firmy, jak i firmy ubezpieczeniowe dostrzegają rosnące ryzyko związane z działaniem w cyberprzestrzeni. Wzrost ten napędzany jest wieloma czynnikami, w tym szybkością i wzrostem wykorzystania Internetu oraz naszą zależnością od technologii. W 2013 roku firma sieciowa CISCO napisała artykuł zatytułowany „Internet wszystkiego dla miast", w którym omówiono „Łączenie ludzi, procesów, danych i rzeczy w celu poprawy „livability" miast i społeczności". W tym artykule opisano, w jaki sposób „Internet rzeczy" (IoT), wzajemnie połączone systemy, staną się „Internetem wszystkiego (IoE), siecią sieci, w której miliardy, a nawet biliony połączeń tworzą niespotykane dotąd możliwości, ale także nowe zagrożenia". Gdy wkraczamy w erę „Internetu wszystkiego", kilka rzeczy staje się oczywistych:

• Świat staje się bardziej wzajemnie powiązany;

• podstawowa infrastruktura staje się bardziej złożona;

• przeciętny użytkownik pragnie prostoty i „łatwości obsługi"

To znaczy że

• Nie musimy rozumieć, jak działa ta technologia, aby z niej korzystać

• Wymiana informacji między ludźmi i organizacjami staje się łatwiejsza

• Istnieje większe prawdopodobieństwo, że informacje zostaną zachowane na dłużej (przechowywanie na dysku jest tańsze niż kiedykolwiek)

• Informacje częściej znajdują się na wielu urządzeniach (nie są już przechowywane w bezpiecznych pomieszczeniach komputerowych)

• Informacje można przesłać do tysięcy osób jednym kliknięciem

• Możemy komunikować się (za pomocą mediów społecznościowych) z tysiącami ludzi

• Możemy pozostać anonimowi lub stworzyć nową tożsamość, za którą będziemy się ukrywać

• Możemy łączyć się z ludźmi o podobnych poglądach na całym świecie

W miarę wzrostu naszej zależności od technologii i informacji organizacje zaczynają dostrzegać, że ich narażenie na zagrożenia wzrasta, czego przyczyną są w dużej mierze głośne naruszenia związane z cyberbezpieczeństwem oraz wzmożona kontrola regulacyjna i wymogi prawne. Wraz ze wzrostem świadomości organizacje zdają sobie sprawę, że zagrożenia cybernetyczne nie dotyczą wyłącznie utraty lub nieuprawnionego ujawnienia danych osobowych lub informacji. Chociaż istnieje szeroki zakres zagrożeń cybernetycznych, w tym związanych z przerwami w działalności i odmową usługi, w rzeczywistości dostępne są tylko dwie formy ubezpieczenia CL (chociaż nie wykluczają się one wzajemnie, ponieważ jedno może mieć wpływ na drugie)

WIERNA ODPOWIEDZIALNOŚĆ CYBER

Ubezpieczenie własne odnosi się do polisy zapewniającej ochronę majątku będącego własnością ubezpieczonej organizacji, a w odniesieniu do zagrożeń cybernetycznych zazwyczaj obejmuje naruszenie danych dotyczących własnych informacji i usług firmy (np. włamanie i zniszczenie witryny internetowej lub odmowa usługi (DoS)) atak). Dodatkowa odpowiedzialność własna może obejmować przerwę w działalności spowodowaną awarią sieci lub systemu, utratę lub uszkodzenie zasobów cyfrowych, kradzież zasobów cyfrowych (w tym pieniędzy), wymuszenie cybernetyczne i utratę reputacji.

ODPOWIEDZIALNOŚĆ CYBER STRONY TRZECIEJ

Odpowiedzialność osób trzecich za cyberbezpieczeństwo odnosi się do polityki zapewniającej ochronę przed zagrożeniami cybernetycznymi, które narażają na ryzyko informacje klientów lub partnerów, których bezpieczeństwo organizacja ma obowiązek chronić. Na przykład włamanie na stronę internetową, w wyniku którego ujawniono dane karty kredytowej klienta, lub dostawca chmury IT, który doświadcza awarii skutkującej utratą informacji o kliencie. Ta forma ochrony zapewnia również odszkodowanie za straty poniesione w wyniku dochodzenia, koszty obrony i kary wynikające z naruszenia i może obejmować koszty związane z powiadamianiem i odszkodowaniem klientów dotkniętych naruszeniem. Obie formy odpowiedzialności mogą być równie szkodliwe, w przypadku gdy zobowiązania pierwszej strony wpływają na zdolność głównego przedsiębiorstwa do działania, podczas gdy zobowiązania stron trzecich mogą mieć wpływ na ich klientów i klientów, co może mieć wpływ na całą reputację i markę wszystkich zaangażowanych stron. Organizacje muszą zatem wziąć pod uwagę szereg zagrożeń cybernetycznych, zrozumieć swoje narażenie na nie, a następnie ocenić potencjał wykorzystania ubezpieczenia jako mechanizmu kontroli. W miarę jak stajemy się coraz bardziej połączeni i w coraz większym stopniu polegamy na cyberprzestrzeni w celu świadczenia usług, wzrasta wraz z tym potrzeba ochrony przed stratami.

ZAGROŻENIA CYBERRYCZNE – ROSNĄCE ZMARTWIENIA

Według rządowej strony internetowej www.gov.uk wartość rynku związanego z Internetem w Wielkiej Brytanii szacuje się obecnie na 82 miliardy funtów rocznie, podczas gdy brytyjskie firmy zarabiają 1 funta na każde 5 funtów wygenerowanych w Internecie. To pokazuje znaczenie Internetu zarówno dla firm, jak i osób prywatnych, ale badania sponsorowane są przez Departament Biznesu

Badanie Innovation & Skills in 2013 ujawniło, że w 2012 roku w Wielkiej Brytanii 93% dużych organizacji doświadczyło naruszenia bezpieczeństwa, a w przypadku małych firm – 87%. W raporcie oszacowano,

że koszty poniesione w wyniku naruszenia bezpieczeństwa wahają się odpowiednio od 450 tys. do 850 tys. funtów i od 35 tys. do 65 tys. funtów. Prawdopodobnie z powodu tych znacznych kosztów związanych z naruszeniami budżety na bezpieczeństwo wzrosły w 2013 r. o 16% (w porównaniu z 2012 r.). Potwierdza to dalsze dane Departamentu Innowacji i Umiejętności Biznesowych, z których wynika, że 81% kadry kierowniczej wyższego szczebla w dużych organizacjach jest coraz bardziej zaniepokojonych bezpieczeństwem i postrzega je jako wysoki lub bardzo wysoki priorytet. Łatwo zrozumieć rosnące zaniepokojenie osób pracujących w dużych (i małych) firmach, gdy liczba naruszeń bezpieczeństwa wydaje się wzrastać, a nagłówki gazet niemal codziennie wypełniają historie o naruszeniach bezpieczeństwa przedsiębiorstw. Sprawy obejmują znane nazwiska, takie jak „Yahoo!" (ujawniono 400 tys. haseł), „LinkedIn" (ujawniono 6,5 mln haseł) i „Adobe" (naruszono 38 mln rekordów [nieoficjalnie liczba ta jest znacznie wyższa i szacuje się, że przekracza 150 mln]). Zgłaszanych jest znacznie więcej historii, a niezliczona ilość pozostaje niezgłaszana, co ilustruje rosnącą potrzebę zrozumienia rosnących zagrożeń związanych z „cybernetykiem". Poniższe przykłady stanowią kolejny dowód na zróżnicowany charakter zagrożeń cybernetycznych:

• W dniu 29 sierpnia 2013 r. dwóm osobom postawiono zarzuty w związku z próbą szantażu firmy internetowej w Manchesterze za pomocą cyberataku. Dochodzenie w sprawie tego zdarzenia jest obecnie w toku, prowadzone przez policję Greater Manchester we współpracy z Agencją ds. Poważnej i Zorganizowanej Przestępczości. Ten incydent uwydatnia rosnące zagrożenie, jakie cyberwymuszenie stwarza dla brytyjskiego biznesu.

• Międzynarodowa firma ubezpieczeniowa musiała zapłacić wielomilionową sumę brytyjskim organom regulacyjnym, gdy udowodniono, że zgubiła taśmy z kopiami zapasowymi serwerów swojego systemu informatycznego, zawierające prywatne dane ponad 40 000 ubezpieczających.

• W 2011 r. brytyjska firma produkująca kosmetyki „Lush" została zhakowana za pośrednictwem zewnętrznego dostawcy poczty e-mail. Hakerom udało się uzyskać dostęp do szczegółów płatności 5000 klientów, którzy wcześniej robili zakupy na tej stronie internetowej. Firma Lush nie spełniła w pełni standardów branżowych dotyczących bezpieczeństwa płatności kartami i groziła jej potencjalna grzywna w wysokości 500 000 funtów nałożona przez Biuro Komisarza ds. Informacji.

Te incydenty i wiele innych im podobnych pokazują mnogość i różnorodność zagrożeń, przed którymi stoją dziś organizacje, nie tylko wynikających z bezpośrednich strat wynikających z samego wydarzenia, ale także z ryzyka związanego z wpływem na reputację (wymagającego zorganizowanej i często kosztownej reakcji PR) oraz ze zwiększonej kary pieniężne i roszczenia odszkodowawcze.

ZAGROŻENIE CYBER

Zagrożenie cybernetyczne dla organizacji ma różne kształty i rozmiary i w zależności od tego, kim one są, mogą być postrzegane jako główny cel, szkody uboczne lub po prostu „plac zabaw", na którym cyberniemowlę doskonali swoje „hakowanie" umiejętności. Zagrożenia te mogą obejmować: haktywizm, kradzież własności intelektualnej, cyberstalking, wymuszenia, rozpowszechnianie wirusów, kradzież tożsamości, wandalizm i oszustwa. Wiele firm może również nieświadomie wziąć udział w atakach na inne sieci komputerowe, gdy zostaną „zainfekowane" narzędziami, które umożliwiają osobie atakującej przejęcie kontroli nad ich komputerami oraz wykorzystanie ich według własnego uznania w ramach „rozproszonej odmowy usługi". Atak (DDOS) na inną organizację lub infrastrukturę krytyczną. Stanley Konter, dyrektor generalny Sabre Technologies w Savannah, stwierdził kiedyś: „Problem stał się bardziej powszechny w przypadku stale włączonego, szybkiego dostępu do Internetu. Atakujący zawsze szukają tego typu komputerów. Nawiązał do faktu, że komputery często pozostają włączone i podłączone do Internetu, nawet jeśli nie są używane, a osoby chcące wyrządzić nam krzywdę mogą wykorzystać to połączenie w obie strony. Zagrożenia te obejmują

zarówno sponsorowanych przez państwo terrorystów, którzy chcą zakłócać infrastrukturę krajową, jak i pojedyncze osoby i grupy osób, które robią to dla „lulz" (w slangu określenie „dla śmiechu"). Chociaż należy przyznać, że zagrożenie cybernetyczne może pochodzić ze źródła zewnętrznego, należy przypomnieć przedsiębiorstwom, że ryzyko incydentu cybernetycznego mającego miejsce wewnątrz ich własnej organizacji jest znacznie większe niż w przypadku źródła zewnętrznego. Wiele organizacji podejmuje już kroki w celu ochrony siebie i swojej firmy przed zagrożeniami cybernetycznymi za pomocą technologii zapory ogniowej, ochrony antywirusowej i systemów wykrywania włamań. Jednak wewnętrznie ich procesy nie ewoluowały, aby chronić siebie i przechowywane informacje w tym samym tempie. Opisane wcześniej incydenty pokazują, że posiadanie dobrych zabezpieczeń nie zapobiegnie „zagubieniu" plików kopii zapasowych zawierających masę informacji. Nie uniemożliwi to również pracownikom wyrzucania do kosza fizycznej dokumentacji zawierającej dane osobowe. Zagrożenie cybernetyczne nie jest zatem związane wyłącznie z informacjami dostępnymi w Internecie, a jest to kwestia, którą próbują rozwiązać ramy regulacyjne na całym świecie.

ZMIENIAJĄCY SIĘ KRAJOBRAZ REGULACYJNY

Większa kontrola ze strony organów regulacyjnych (na całym świecie) i groźby wyższych kar wyraźnie zwiększyły potrzebę odpowiedniej ochrony. W Europie w styczniu 2012 r. Komisja Europejska zaproponowała reformę unijnych przepisów o ochronie danych z 1995 r. w celu wzmocnienia praw do prywatności w Internecie. Uznano to za kluczowy wymóg, częściowo ze względu na to, że 27 państw członkowskich UE wdrożyło przepisy z 1995 r. w różny sposób, co doprowadziło do rozbieżności w egzekwowaniu przepisów. Zamiarem jest stworzenie jednolitego prawa, które obniży koszty administracyjne (ram prawnych) i jest postrzegane jako sposób na zwiększenie zaufania do usług online (patrz rozdziały 1 i 14). Ten rozdział nie ma na celu szczegółowego przeglądu nowego rozporządzenia, ale istnieją kluczowe elementy standardu, które warto zbadać, ponieważ bezpośrednio wpływają na rosnące zapotrzebowanie na ubezpieczenie CL.

POWIADOMIENIE ICO

Rozporządzenie, które miało wejść w życie w 2014 r. (ewentualnie w 2015 r.), upoważnia każdy organ nadzorczy do nałożenia sankcji administracyjnych zgodnie z rozporządzeniem i stanowi, że w ciągu 24 godzin i przedstawienia pełnego raportu w ciągu 3 dni od zdarzenia. Brzmienie art. 31 rozporządzenia stanowi: W przypadku naruszenia ochrony danych osobowych administrator bez zbędnej zwłoki, a w miarę możliwości nie później niż w terminie 24 godzin od powzięcia o tym informacji, zgłasza naruszenie ochrony danych osobowych organowi nadzorczemu autorytet. Do zawiadomienia organu nadzorczego należy dołączyć uzasadnione uzasadnienie, jeżeli nie zostało ono dokonane w terminie 24 godzin. Rozporządzenie określa, jakie informacje są wymagane, a także sposób, w jaki należy je przekazywać. Ponadto art. 79 („Sankcje administracyjne") określa sankcje administracyjne, jakie organ nadzorczy może nałożyć na organizacje, które naruszają przepisy, i stwierdza, że sankcja „powinna być w każdym indywidualnym przypadku skuteczna, proporcjonalna i odstraszająca" (art. 79 ust. 2). Artykuł 79 rozporządzenia stanowi dalej, że wysokość administracyjnej kary pieniężnej ustala się z uwzględnieniem charakteru, wagi i czasu trwania naruszenia, umyślnego lub niedbałego charakteru naruszenia, stopnia odpowiedzialności osoby fizycznej lub osoby prawnej i wcześniejszych naruszeń tej osoby, wdrożonych środków technicznych i organizacyjnych oraz procedur [zgodnie z art. 23] oraz stopnia współpracy z organem nadzorczym w celu usunięcia naruszenia. Powyższy fragment wyraźnie wskazuje, że organizacje muszą być w stanie zrozumieć swoje ryzyko i mieć jasne pojęcie o tym, w jaki sposób chronią się przed tym, że ryzyko to stanie się incydentem. W dalszej części rozporządzenia określono rodzaje sankcji, jakie może nałożyć organ nadzorczy, i to właśnie tych sankcji organizacje stają się coraz bardziej świadome i obawiają się, co skłania je do rozważenia skorzystania z jakiejś formy ubezpieczenia, które zmniejsza zwiększone ryzyko kar finansowych. Sankcje te obejmują grzywny w

wysokości od 250 000 do 1 000 000 euro lub od 0,5% do 2% rocznego światowego obrotu, w zależności od okoliczności naruszenia oraz poziomu ochrony i łagodzenia, jaki można wykazać. W miarę jak przepisy stają się coraz bardziej kompleksowe, przedsiębiorstwa muszą nie tylko rozważyć najodpowiedniejsze sposoby poprawy kontroli bezpieczeństwa (np. poprzez przyjęcie międzynarodowej normy bezpieczeństwa informacji ISO27001:2013), ale muszą także szukać sposobów na ograniczenie potencjalnych strat wynikających z karami nałożonymi przez lokalny organ nadzorczy poprzez korzystanie z odpowiedniego ubezpieczenia.

CO OBEJMUJE UBEZPIECZENIE OD CYBER ODPOWIEDZIALNOŚCI?

Na tym etapie należy stwierdzić, że ubezpieczenia CL nie należy postrzegać jako metody umożliwiającej organizacjom proste przeniesienie ryzyka na ubezpieczyciela i niepodjmowanie żadnych innych wysiłków w celu ochrony przed potencjalnymi zdarzeniami. Podobnie jak wiele produktów ubezpieczeniowych, produkty CL Insurance zawierają szereg wyjątków i wyłączeń mających na celu ochronę ubezpieczyciela przed ubezpieczaniem złych ryzyk. Ubezpieczenie Cyber Liability ma na celu ograniczenie strat wynikających z różnych incydentów związanych z cyberbezpieczeństwem, w tym tych wskazanych wcześniej. W związku z pojawieniem się nowych przepisów oraz coraz bardziej złożonym i wzajemnie powiązanym środowiskiem, w którym działają przedsiębiorstwa; łatwo zrozumieć, dlaczego ubezpieczenia cybernetyczne są tak pożądane przez firmy. Dobry produkt CL Insurance powinien chronić przed finansowymi skutkami wycieku danych, utraty danych lub naruszenia systemu informatycznego firmy i może obejmować dodatkową ochronę takich elementów jak Cyber Extortion czy koszty związane z zarządzaniem PR. Obecne produkty różnią się pod względem tego, co będą obejmować, a czego nie, ale zasadniczo obejmują utratę informacji z pojedynczego laptopa po włamanie do całej sieci lub magazynu w chmurze. Wpływ któregokolwiek z powyższych czynników może mieć poważny wpływ na system informatyczny firmy, jej reputację rynkową i, co najważniejsze, stabilność finansową. Skutki naruszenia danych mogą być dalekosiężne, ale ubezpieczenie od odpowiedzialności cywilnej w zakresie cyberbezpieczeństwa zasadniczo dzieli się na trzy odrębne obszary:

• Utrata lub uszkodzenie danych — dane, które zostały utracone, skradzione, uszkodzone lub uszkodzone w jakikolwiek sposób, w tym w wyniku działań zamierzonych lub niezamierzonych. Poniesione koszty mogą obejmować roszczenia odszkodowawcze, kary, dochodzenia, koszty środków zaradczych lub odzyskiwania środków.

• Wymuszenie cybernetyczne — wzrasta ryzyko, gdy hakerzy lub „haktywiści" grożą zakłóceniem działalności Twojej firmy poprzez wprowadzenie wirusa lub zamknięcie witryny internetowej w wyniku ataku typu „odmowa usługi" (DoS), chyba że zostanie przekazana suma pieniędzy. Dodatkowe ryzyko obejmuje groźbę umieszczenia na stronach internetowych lub katalogach internetowych zniesławiających (lub nieodpowiednich) materiałów w celu zdyskredytowania firmy. Cyber-wymuszenie obejmuje również ujawnienie informacji poufnych, chyba że zostanie uiszczona opłata.

• Dowodzenie i kontrola — do zarządzania incydentem i zapewnienia podjęcia wszelkich niezbędnych działań w celu zminimalizowania zakłóceń w działalności oraz zapewnienia, że wszystkie zainteresowane strony zostaną poinformowane o podejmowanych działaniach (w tym klienci, dostawcy i organy regulacyjne) może być wymagana wiedza specjalistyczna. . Może to również obejmować koszty związane z zewnętrznymi agencjami PR zajmującymi się zarządzaniem komunikacją z szerszą społecznością i ostatecznie będzie obejmować koszty związane ze świadczeniem usług ochrony kredytowej osobom, których to dotyczy.

Jak podkreślono powyżej w „Dowodzenie i kontrola”, szersza ochrona zapewniana przez niektóre polityki cybernetyczne rozciąga się na koszty public relations, które mogą wynikać z ujawnienia przedsiębiorstwa, że doszło do naruszenia cyberbezpieczeństwa. Reputacja firmy może szybko się zepsuć, gdy klienci stracą zaufanie do jej bezpieczeństwa. Posiadanie szybkiego i profesjonalnego zespołu PR, który pomoże zarządzać kryzysem i przywrócić zaufanie klientów, ma ogromne znaczenie w epoce cyfrowej.

KTO OFERUJE UBEZPIECZENIE CYBER ODPOWIEDZIALNOŚCI I NA CO KLIENCI POWINNI UWAŻAĆ?

Ubezpieczenie Cyber Liability Insurance istnieje na rynku ubezpieczeniowym od wielu lat, ale dopiero proponowane zmiany w przepisach, zwiększone wykorzystanie mobilnych urządzeń elektronicznych oraz seria głośnych cyberataków sprawiły, że Ubezpieczenie Cyber Liability Insurance znalazło się na czele przedsiębiorstw i uwagę brokera. Wybór odpowiedniego brokera, który rozumie zabezpieczenia i ryzyko, ma ogromne znaczenie dla zapewnienia firmie odpowiedniej ochrony. W miarę wzrostu zapotrzebowania na znaczącą ochronę przed odpowiedzialnością cybernetyczną nie brakuje możliwości rynkowych dla tego produktu. Do uznanych rynków tego ubezpieczenia należą AIG, Hiscox, ACE, Chubb i Zurich; jednakże wybór właściwej polisy jest kluczem do zapewnienia odpowiedniej ochrony. Kompleksowy produkt Cyber Liability powinien obejmować następujące kluczowe obszary:

• Koszty obrony i szkody pokryte w przypadku strat pierwszej i strony trzeciej

• Przerwa w działalności z powodu przestoju serwera

• Usługa dochodzeń kryminalistycznych i wsparcia w celu zarządzania naruszeniami i pomocy w przywróceniu systemu firmy

• Usługa reagowania w zakresie public relations, pomagająca złagodzić negatywny rozgłos po włamaniu cybernetycznym

• Ochrona oferowana w związku z wymuszeniami cybernetycznymi

Ważne jest również rozważenie, czy dostawca oferujący produkt z zakresu odpowiedzialności cybernetycznej rozumie cyberprzestrzeń, w której działa. Skuteczna reakcja na zagrożenie ma ogromne znaczenie, a zrozumienie procesu powiadamiania i zarządzania da nabywcy pewność, że w razie potrzeby wszyscy zrozumieją, co się stanie.

WNIOSEK

Ze szczegółowych informacji na temat cyberzagrożeń i cyberataków jasno wynika, że każda firma lub organizacja posiadająca stronę internetową lub prowadząca działalność w cyberprzestrzeni potrzebuje ochrony przed coraz większą gamą zagrożeń i musi podejmować proaktywne kroki, aby zabezpieczyć się przed wystąpieniem incydentów. Środki te powinny obejmować podstawową wiedzę i wdrożenie odpowiednich środków kontroli bezpieczeństwa. Znaczenie „odpowiedniego” różni się w zależności od branży i biznesu, ale każda organizacja powinna przynajmniej przyjąć zasady ochrony danych i rozważyć stosowność międzynarodowego standardu bezpieczeństwa informacji, ISO27001. Dobre procesy bezpieczeństwa informacji zawsze wymagały dobrego zarządzania incydentami i tutaj wkracza CL Insurance. CL Insurance zapewnia poziom komfortu, dzięki któremu w przypadku (lub „kiedy”) dojdzie do naruszenia, osoba składająca roszczenie może ostatecznie polegać na czymś, co pomoże zmniejszyć wpływ na jego organizację, jeśli zostanie przeprowadzona kontrola prawna lub regulacyjna (lub sankcje) lub jest potrzeba wiedzy specjalistycznej lub eksperckiej. W miarę jak coraz więcej transakcji biznesowych odbywa się w cyberprzestrzeni, wzrasta wykorzystanie mobilnych urządzeń elektronicznych, a „Big Data” staje się coraz większe, prawdopodobieństwo, że coś pójdzie nie tak,

niewątpliwie wzrośnie. Potencjalne bezpośrednie lub pośrednie straty, które mogą wystąpić w wyniku kradzieży, utraty, zniszczenia kluczowych danych, zniesławienia, zniesławienia, naruszenia praw autorskich lub znaków towarowych, wandalizmu, gróźb lub ataków typu „odmowa usługi", rosną i nie wykazują oznak spowolnienia. Zmiany regulacyjne i legislacyjne dotyczące ochrony danych i powiadamiania o naruszeniach mogą spowodować, że grzywny i kary staną się znacznie powszechniejsze, dlatego firmy muszą zdać sobie sprawę z ryzyka, jakie stwarza Cyber Liability, i dokładnie rozważyć środki bezpieczeństwa wymagane do zapewnienia ochrony danych. Chociaż istnieje wiele podejść do tego zagadnienia, które należy dokładnie ocenić i zrozumieć, korzyści płynące z kompleksowej i skutecznej polityki w zakresie odpowiedzialności cybernetycznej nie będą w pełni zrozumiałe, dopóki nie staną się potrzebne. Rynek ubezpieczeniowy historycznie powolnie rozwija produkty, dla których dostępnych jest niewiele informacji statystycznych lub nie ma ich wcale, ale w miarę jak szczegóły dotyczące naruszeń staną się łatwiej dostępne, oferta ubezpieczeń CL będzie rosła wraz z popytem na rynku. Przyszłość CL Insurance jest zabezpieczona i niewątpliwie będzie ewoluować w nadchodzących latach. Pytanie tylko, jak szybko CL Insurance przekształci się w pełne ubezpieczenie ochrony danych. Jest to krok, który jeszcze nie został wykonany, ale niewątpliwie musi zostać wykonany.

Reagowanie na cyberprzestępczość i cyberterroryzm – botnety stanowią podstępne zagrożenie

WSTĘP

Jednym z najbardziej podstępnych zagrożeń cybernetycznych dla społeczności IT jest obecnie rozprzestrzenianie się sieci zawierających zainfekowane komputery (zwane botami lub zombie), które są zarządzane przez osoby atakujące i nazywane są botnetami. Wykorzystywanie botnetów jest bardzo powszechne w różnych kontekstach IT, od cyberprzestępczości po cyberwojnę. Są w stanie zapewnić bardzo wydajną rozproszoną platformę IT, którą można wykorzystać do szeregu nielegalnych działań, takich jak uruchamianie rozproszonej odmowy usługi (DDoS), ataki na cele krytyczne lub rozpoczynanie od „próbnego" ataku, po którym następuje e-mail lub inna komunikacja grożenie większym atakiem DDoS (w przypadku niezapłacenia określonej kwoty pieniędzy – wymuszenie cybernetyczne), rozpowszechnianiem złośliwego oprogramowania, phishingiem i oszustwami (np. gromadzeniem informacji bankowych) lub prowadzeniem cyberszpiegostwa kampanie mające na celu kradzież poufnych informacji. W tych scenariuszach kontroler botnetu, zwany także botmasterem, kontroluje działania całej struktury, wydając rozkazy każdemu zombie za pośrednictwem różnych kanałów komunikacji. Rozprzestrzenianie się botnetów mierzy poziom ich niebezpieczeństwa i zależy od zdolności menedżerów do zaangażowania jak największej liczby maszyn, które również próbują ukryć działania szkodliwej architektury — jest to szczególny rodzaj gry w chowanego. Krytyczną fazę organizacji botnetów reprezentuje ich struktura. Atakujący mogą rekrutować boty rozprzestrzeniające złośliwe oprogramowanie, zwykle poprzez phishing lub wysyłanie złośliwego agenta za pośrednictwem poczty elektronicznej. Zainfekowane maszyny otrzymują polecenia z serwerów dowodzenia i kontroli (C&C), które instruują ogólną architekturę, jak ma działać, aby osiągnąć cel, dla którego została skomponowana. Rozprzestrzenianie się botnetów wzrosło ostatnio z powodu różnych czynników, takich jak:

• zwiększona dostępność wydajnych łączy internetowych i hostów (rozumianych nie tylko jako komputery osobiste, ale jako przedmioty życia codziennego, coraz bardziej połączone i inteligentne). Oczekuje się, że do roku 2020 do Internetu będzie podłączonych od pięćdziesięciu do stu miliardów rzeczy. Paradygmat ten jest zwykle określany jako „Internet rzeczy";

• możliwość personalizacji szkodliwego oprogramowania (wprowadzonego przez botnet Zeus i jego Software Development Kit);

• obecność na podziemnym/czarnym rynku cyberprzestępców wynajmujących usługi i struktury składające się na szkodliwe systemy.

Istnieją różne klasyfikacje botnetów w oparciu o ogólną topologię oraz wykorzystywane kanały dowodzenia i kontroli, za pośrednictwem których można je aktualizować i kierować, wykorzystywaną rozwijającą się technologię oraz zakres wdrożonych usług. Pojawiające się trendy pokazują, że nowsze architektury migrują w kierunku całkowicie rozproszonych topologii (sieci P2P), zamiast scentralizowanych struktur, mobilnych implementacji złośliwego oprogramowania oraz wykorzystania sieci TOR i platform społecznościowych jako technik ukrywania serwerów kontroli. Wysoki poziom zaawansowania i rozprzestrzenianie się botnetów doprowadził do pojawienia się nowego przestępczego modelu biznesowego, który można zsyntetyzować w oparciu o „cyberprzestępczość jako usługę" (CaaS). Tu zawarto opis botnetu (zawierający dwa przypadki użycia) i powiązane środki zaradcze.

PLAN DZIAŁANIA BOTNETU

Szkodliwe oprogramowanie, które wprowadziło koncepcję maszyny ofiary podłączonej do kanału komunikacyjnego w celu nasłuchiwania szkodliwych poleceń, począwszy od tak zwanej ery botnetów, to „Sub7" i „Pretty Park" – odpowiednio trojan i robak. Te dwa szkodliwe programy pojawiły się po raz pierwszy w 1999 r. i od tego czasu liczba botnetów stale rośnie (Ferguson, 2010). W roku 2002 miało miejsce kilka znaczących zmian w technologii botnetów wraz z wypuszczeniem zarówno SDBota, jak i Agobota. SDBot był napisanym pojedynczym, małym plikiem binarnym w C++, sprzedawany przez jego twórcę, który również szeroko udostępnił kod źródłowy. W rezultacie wiele botów zawiera później kod lub pomysły zaczerpnięte z SDbota. Zamiast tego Agobot wprowadził koncepcję ataku modułowego. Pierwszy atak polegał na zainstalowaniu „tylnych drzwi", drugi miał na celu wyłączenie oprogramowania antywirusowego, a trzeci zablokował dostęp do stron internetowych dostawców zabezpieczeń. Te dwa szkodliwe programy zapoczątkowały ogromny wzrost liczby wariantów i rozwój funkcjonalności. Twórcy szkodliwego oprogramowania stopniowo wprowadzali szyfrowanie oprogramowania Ransomware (przejmowanie zaszyfrowanych plików przez zakładników), serwery proxy HTTP i SOCKS, umożliwiające im wykorzystywanie ofiar do dalszego połączenia lub serwery FTP do przechowywania nielegalnych treści. Botnety stopniowo migrowały z pierwotnego kanału dowodzenia i kontroli IRC — protokół można łatwo zidentyfikować w ruchu sieciowym, a porty TCP rzadko otwierane przez zapory ogniowe — i zaczęły komunikować się za pośrednictwem portów HTTP, ICMP i SSL, często przy użyciu niestandardowych protokołów. Kontynuowali także wdrażanie i udoskonalanie komunikacji typu peer-to-peer, co wykazał 5 lat później inny słynny botnet znany pod nazwą Conficker. Około 2003 roku zaczęło być widoczne zainteresowanie przestępczości możliwościami botnetów. Na początku dekady spamowanie było w dalszym ciągu zajęciem „odrabianym w domu" i obejmowało duże ilości spamu wysyłanego z dedykowanych farm serwerów, otwartych przekaźników lub zaatakowanych serwerów. Bagle i Bobax były pierwszymi botnetami spamującymi, a złośliwym oprogramowaniem był Mytob w zasadzie połączenie wcześniejszych robaków masowych MyDoom i SDbot. Umożliwiło to przestępcom tworzenie dużych botnetów i rozpowszechnianie spamu na całych komputerach ofiar, zapewniając im elastyczność i elastyczność oraz pomagając im uniknąć działań związanych z egzekwowaniem prawa, które zaczęły być agresywnie stosowane. W 2005 roku rosyjska grupa pięciu programistów znana jako UpLevel rozpoczęła prace nad Zeusem, programem typu „wskaż i kliknij" służącym do tworzenia i kontrolowania sieci zaatakowanych systemów komputerowych . W następnym roku wypuścili pierwszą wersję programu, podstawowego trojana zaprojektowanego do ukrywania się w zainfekowanym systemie i kradzieży informacji. W 2007 roku grupa wypuściła bardziej modułową wersję, która umożliwiła innym podziemnym programistom tworzenie wtyczek rozszerzających jej funkcjonalność. Pięć lat później najnowsza wersja tego

oprogramowania (którą można pobrać bezpłatnie i wymaga niskich umiejętności technicznych do obsługi) jest jedną z najpopularniejszych platform botnetów dla spamerów, oszustów i osób handlujących skradzionymi danymi osobowymi (Należy pamiętać, że wzrosła liczba działań, które można wykonać przy użyciu złośliwego oprogramowania). Najnowsza platforma Zeus umożliwia użytkownikom tworzenie niestandardowego złośliwego oprogramowania w celu infekowania systemów docelowych, zarządzania szeroką siecią zaatakowanych maszyn i wykorzystywania powstałego botnetu do nielegalnych celów. Zestaw konstrukcyjny zawierał program do budowy oprogramowania bota oraz skrypty internetowe służące do tworzenia i hostowania centralnego serwera dowodzenia i kontroli . Ankieta przeprowadzona przez firmę zajmującą się bezpieczeństwem — Damballa z siedzibą w Atlancie — wykazała, że w 2009 r. programy kontrolowane przez Zeusa były drugimi pod względem rozpowszechnienia w sieciach korporacyjnych. Damballa wyśledziła ponad 200 botnetów opartych na Zeusie w sieciach korporacyjnych. Największy pojedynczy botnet kontrolowany przy użyciu platformy Zeus składał się z 600 000 zaatakowanych komputerów. W rezultacie niezależni programiści stworzyli kompatybilne „pakiety exploitów", które mogą infekować systemy ofiar przy użyciu luk w zabezpieczeniach systemu operacyjnego lub przeglądarki. Inni programiści skupiają się na tworzeniu oprogramowania wtyczek, które pomaga „niedoszłym" cyberprzestępcom w zarabianiu pieniędzy na botnecie Zeus. Na przykład niektóre dodatki skupiają się na atakach phishingowych, dostarczając obrazy i strony internetowe potrzebne do tworzenia fałszywych witryn bankowych. Dzięki wspomnianym funkcjom oprogramowanie antywirusowe bardzo trudno jest zidentyfikować ładunek Zeusa. Zeus nie jest oczywiście jedynym narzędziem dostępnym do budowy botnetu, ale jego narodziny są kamieniem milowym dla całego sektora cyberprzestępczego, ponieważ został zaprojektowany z myślą o „nieekspertach" i zawiera proste interfejsy typu „wskaż i kliknij" do zarządzania zainfekowanymi maszynami (z tych powodów nazywana rodziną ZeuS Crimeware). Na przykład botnet ZeroAccess – specjalizujący się w atakach związanych z oszustwami związanymi z kliknięciami, który najwyraźniej uległ zakłóceniom w 2013 r. – był prawdopodobnie szerszy niż Zeus (szacuje się, że w 2012 r. doszło do milionów infekcji na całym świecie, z maksymalnie 140 000 unikalnych adresów IP w USA i Europie). Tak jak Zeus był kamieniem węgielnym botnetów nowej generacji, tak Blackhole jest z pewnością kamieniem węgielnym zestawów exploitów nowej generacji. Od czasu pojawienia się pod koniec 2010 roku zestaw exploitów Blackhole stał się jednym z najbardziej znanych zestawów exploitów, jakie kiedykolwiek napotkano (Howard, 2012). W ciągu ostatnich kilku lat ilość szkodliwego oprogramowania wykrywanego w terenie dramatycznie wzrosła, głównie dzięki zastosowaniu automatyzacji i zestawów ułatwiających jego tworzenie i dystrybucję. Termin „oprogramowanie przestępcze", używany już w odniesieniu do Zeusa, został ukuty specjalnie w celu opisania procesu „automatyzacji cyberprzestępczości". Osoby fizyczne nie czerpią już zysków wyłącznie z pisania i rozpowszechniania swojego złośliwego oprogramowania. Dzisiejsza scena szkodliwego oprogramowania jest wysoce zorganizowana, ustrukturyzowana i profesjonalna w swoim podejściu, a użytkownicy mogą wybierać role przestępcze, która najlepiej pasują. Zestawy, jako nieodłączna część oprogramowania przestępczego, zapewniają przestępcom narzędzia do tworzenia i rozpowszechniania złośliwego oprogramowania, ale także systemy używane do zarządzania sieciami zainfekowanych maszyn. Niektóre z tych zestawów skupiają się na tworzeniu i zarządzaniu ładunkiem złośliwego oprogramowania — Zeus jest być może najlepszym tego przykładem. Inne zestawy to te, które skupiają się na infekowania użytkowników poprzez ataki internetowe, w szczególności ataki znane jako pobieranie typu drive-by. To właśnie ta druga grupa zestawów jest powszechnie nazywana zestawami exploitów lub pakietami exploitów (terminy te są używane zamiennie). Istnieje kilka wersji zestawu exploitów Blackhole, pierwsza to wersja 1.0.0 (wydana pod koniec 2010 roku). Zestaw składa się z szeregu skryptów PHP zaprojektowanych do działania na serwerze internetowym (wszystkie chronione komercyjnym koderem ionCube). Ma to prawdopodobnie na celu uniemożliwienie innym złoczyńcom kradzieży ich kodu (istnieje wiele zestawów exploitów, które są niczym więcej niż kopiami

innych) i utrudnienie analizy. Ogólna charakterystyka zestawu exploitów Blackhole jest wymieniona poniżej:

• Zestaw jest pochodzenia rosyjskiego.

• Opcje konfiguracji wszystkich typowych parametrów (parametry zapytania, ścieżki plików dla ładunków lub komponentów exploitów, adresy URL przekierowań, nazwy użytkowników, hasła itp.).

• Zaplecze MySQL.

• Czarna lista/blokowanie (uderzaj tylko raz w dowolny adres IP, prowadź czarną listę adresów IP, czarną listę według adresu URL strony odsyłającej, importuj zakresy z czarnej listy).

• Automatyczna aktualizacja (oczywiście).

• Konsola zarządzająca zapewnia podsumowanie statystyczne z podziałem udanych infekcji według exploita, systemu operacyjnego, kraju, partnera/partnera (odpowiedzialnego za kierowanie ruchu użytkowników do zestawu exploitów) i przeglądarki.

• Wykorzystuje różne luki w zabezpieczeniach klienta.

• Dodatki do skanowania antywirusowego.

Istnieją jednak pewne funkcje, które są (lub były w pierwszym wydaniu) unikalne dla Blackhole:

• Model biznesowy „Wynajem". Historycznie rzecz biorąc, zestawy exploitów to towary (płatne za użycie), które są sprzedawane osobom fizycznym, a następnie wykorzystywane według ich uznania. Blackhole obejmuje strategię wynajmu, w ramach której poszczególne osoby płacą za korzystanie z hostowanego zestawu exploitów przez pewien okres.

• Konsola zarządzająca zoptymalizowana do użytku z urządzeniami PDA.

Celem Blackhole jest zainfekowanie ofiar pewnym ładunkiem. Ładunki są zazwyczaj polimorficzne, wyposażone w niestandardowe narzędzia szyfrujące i zaprojektowane tak, aby uniknąć wykrycia przez program antywirusowy (proces ten jest wspomagany przez wbudowaną funkcję sprawdzania AV Blackhole). Do najpowszechniejszych ładunków zainstalowanych w ciągu ostatnich kilku lat należą fałszywe programy AV, Zeus, rootkit ZeroAccess i oprogramowanie ransomware. Jedną z najważniejszych nowych funkcji Blackhole jest automatyzacja, dzięki której możesz wykorzystywać serwery i klientów poprzez dużą liczbę luk w zabezpieczeniach (pamiętaj, że zarówno Zeus, jak i Blackhole to sieci stale zarządzane i aktualizowane zdalnie). Serwery internetowe z pewnymi lukami w zabezpieczeniach (zaatakowane serwery) mogą być wykorzystywane do bezpośredniego hostowania Blackhole lub do przekierowywania klientów do „tworzonych ad hoc" witryn internetowych Blackhole. Osoba atakująca może wykorzystać zaatakowany serwer w celu kradzieży informacji wszystkich użytkowników tego samego serwera, co jest również nazywane atakiem Watering Hole. Osoby atakujące badają zachowanie osób pracujących dla docelowej organizacji, aby poznać ich nawyki przeglądania. Następnie atakują witrynę internetową, z której często korzystają pracownicy — najlepiej hostowaną przez zaufaną organizację, która stanowi cenne źródło informacji. W idealnym przypadku użyją exploita zero-day. Kiedy więc pracownik odwiedza stronę internetową w witrynie, zostaje zainfekowany. Zwykle instalowany jest trojan typu backdoor, umożliwiający atakującym dostęp do wewnętrznej sieci firmy. W efekcie zamiast ścigać ofiarę, cyberprzestępca przebywa w miejscu, które ofiara z dużym prawdopodobieństwem odwiedzi – stąd analogia do wodopoju (Kaspersky, 2013; Symantec, 2013). Drugim ważnym aspektem z punktu widzenia przestępczości jest zmiana modelu

biznesu przestępczego. Starsze wersje szkodliwego oprogramowania były oferowane do sprzedaży po bardzo wysokich cenach. W rzeczywistości wczesne wersje są dystrybuowane bezpłatnie i często te poprzednie wersje zostały „wdrożone" przez przestępców, co oznacza, że ofiarą staje się także początkujący złodziej (tzw. lamer). Zamiast tego w niedawnej przeszłości nadmiar swobodnie dostępnych narzędzi przestępczych obniżył barierę kosztową wejścia do cyberprzestępczości i zachęcił większą liczbę niedoszłych cybergangsterów (lamerów) do przestępczości internetowej. Jak wspomniano, dzisiejsza scena szkodliwego oprogramowania jest wysoce zorganizowana, ustrukturyzowana i profesjonalna w swoim podejściu. Rozprzestrzenianie się Internetu, zwłaszcza do celów rządowych i komercyjnych, doprowadziło do ewolucji modelu biznesowego rynku przestępczego stojącego za współczesnymi zagrożeniami. Można sobie wyobrazić warstwową strukturę odwróconej piramidy (pod względem zaangażowanych organizacji, wielkości tych organizacji, umiejętności i celów). Organizacje posiadające większe umiejętności techniczne (prawdopodobnie mniej liczne i porównywalne do cybernajemników) to te, które projektują i dystrybuują różnego rodzaju oprogramowanie przestępcze (ładunki i zestawy exploitów) zgodnie z różnymi sposobami rozprzestrzeniania się (spam, phishing, socjotechnika, podjazd lub wodopoj), ale nie podejmuj żadnych szczególnych działań. W wielu przypadkach cybernajemnicy zamiast zarabiać na działalności botnetu poprzez bezpośrednie wdrażanie schematów oszustwa, wynajmują szereg usług innym przestępcom – trend ten potwierdza stałe monitorowanie ofert rynku podziemnego. Przygotowana infrastruktura jest gotowa do „sprzedania" lub lepiej „wynajęcia" oferentowi, który zaoferuje najwyższą cenę. Model wynajmu wykazał lepsze przychody niż model sprzedaży. W rzeczywistości wielu przestępców zarabiało pieniądze po prostu wynajmując dostęp do swoich botnetów, zamiast angażować się w wymyślone przez siebie kampanie spamowe, DDoS lub kradzieży informacji (pamiętaj, że tak zwana „strona docelowa" Blackhole może być sama w sobie zaatakowanym serwerem lub serwer hostingowy). Ci, którzy płacą za podjęcie działań przestępczych, nie potrzebują wysokich umiejętności technicznych, ale ich ataki są zwykle bardziej motywowane i liczniejsze. Dwie najczęstsze przyczyny to społeczno-polityczne (haktywiści) i ekonomiczne (cyberprzestępcy). Przestępcy płacą za użycie (PPU) tysiącom już zainfekowanych komputerów lub dostarczają dodatkowe złośliwe oprogramowanie do tych już zainfekowanych komputerów. Boty spamujące mogą dostarczać informacje wtórne, na przykład poprzez kradzież złośliwego oprogramowania, fałszywego oprogramowania antywirusowego i oprogramowania ransomware, aby zwiększyć elastyczność zainfekowanych maszyn i zmaksymalizować potencjalne przychody z każdego zainfekowanego komputera. Aby dać wyobrażenie o wpływie ekonomicznym botnetów, w „Raporcie o zagrożeniach F-Secure 2012" ujawniono, że zagrożenie ZeroAccess powoduje według doniesień 140 milionów reklam dziennie. Szacuje się, że botnet kosztuje legalnych reklamodawców internetowych aż do 900 000 dolarów codziennych strat w przychodach. Co więcej, jak zobaczymy później, w jednym z dwóch przypadków użycia Eugrograbber zarobił ponad 36 milionów euro. Trzeci poziom to oczywiście ofiary (właściciel zainfekowanych maszyn), którymi w zależności od rodzaju ataku może być zwykły użytkownik Internetu (jeśli liczba ofiar jest najważniejszą zmienną, np. w kampanii DDoS) lub przynależność do określonej kategorii osób (jeśli najważniejsza zmienna jest jakość odejmowanych informacji). Co więcej, warstwa użytkowników niekoniecznie jest monolityczna, ale można ją dalej podzielić na poziomy pośrednie (np. organizacje najbardziej doświadczone w tworzeniu szkodliwego oprogramowania mogą nie być jednakowe w jego dystrybucji) i składa się z różnych przestępców uczestniczących w czymś w rodzaju programu partnerskiego, w którym wyższy poziom gwarantuje minimalną liczbę „klientów" niż niższy (patrz model biznesowy ZeroAccess Pay-per-Install – PPI –). Za miarę realnego zagrożenia uważa się poprzednią piramidę, a także przestępczy model biznesowy (im większa jest warstwa ofiar, tym większe jest zagrożenie destrukcyjne). Wspomniane modele monetyzacji botnetów (PPI i PPU) wpływają zarówno na kierunek, jak i wielkość „przepływów wartości przestępczej". Ponadto w konkretnym przypadku modelu PPU wielkość przepływu jest proporcjonalna do niebezpieczeństwa

zagrożenia. W rzeczywistości, o ile w przypadku botnetu nastawionego na oszustwa związane z kliknięciami, przepływy pieniężne i ich wielkość są prawie pewne, o tyle w przypadku botnetu ogólnego przeznaczenia przestępca (Użytkownik), który chce zaatakować na przykład bank, mógłby chcieć zainwestować większą sumę pieniędzy na zakup lub wynajęcie botnetu (przez Projektantów) wystarczająco szerokiego i posiadającego wystarczające umiejętności dla konta bankowego kampanie eksfiltracyjne lub DDOS. Zatem przepływy ekonomiczne botnetu w dwóch modelach monetyzacji można przedstawić jak na rysunku (grubość strzałek wskazuje ilość pieniędzy).

PODSTAWOWE DZIAŁANIA:

• Logistyka przychodząca: wszelkie działania logistyczne potrzebne do realizacji usług na sprzedaż lub wynajem. Logistyka sprzętu i oprogramowania, wynajem kuloodpornych usług hostingowych i anonimowa łączność.

• Operacje: podstawowa działalność. Twórz ładunki, konfigurowalne oprogramowanie Crimeware, zestawy exploitów i infrastrukturę zaplecza do tworzenia, ukrywania i uzyskiwania dostępu do serwerów kontroli (być może hostowanych w domenach kuloodpornych), metod/usług dystrybucji złośliwego oprogramowania itp.

• Logistyka wychodząca: Hw & Sw do zarządzania bezpieczną infrastrukturą e-marketingu, e-sprzedaży i elektronicznego transferu pieniędzy.

• Marketing i sprzedaż: MARKETING: posty na forach, czarne rynki, wskaźnik i cel sukcesu. SPRZEDAŻ: sprzedaż/wynajem odbywa się wyłącznie za pośrednictwem działu operacyjnego.

• Usługi: amplituda botnetu, stale aktualizowane funkcje złośliwego oprogramowania (spam, DDOS, eksfiltracja itp.).

DZIAŁANIA WSPIERAJĄCE:

• Infrastruktura firmowa: laboratoria, własny serwer C&C, technologie anonimowej łączności i/lub sieci VPN w krajach o słabym ustawodawstwie dotyczącym cyberprzestępczości.

• Zarządzanie zasobami ludzkimi: Pracownicy wykwalifikowani i godni zaufania.

• Rozwój technologiczny: warianty pakietu Crimeware SDK lub zupełnie nowe ładunki, zestawy exploitów, kuloodporny host C&C, bezpieczne płatności elektroniczne, bezpieczny e-marketing.

• Zakupy: prognozowanie i planowanie zapytań rynkowych o charakterze przestępczym, bezpieczne systemy płatności, procedury zaufania i oceny umiejętności dostawców i partnerów (model biznesowy PPI)

BOTNETY JAK DZIAŁAJĄ. TOPOLOGIE I PROTOKOŁY SIECI

Jak wspomniano we wstępie, botnet to sieć zainfekowanych komputerów (botów lub zombie) zarządzana przez osoby atakujące za pośrednictwem jednego lub większej liczby serwerów dowodzenia i kontroli oraz w wyniku zaszczepienia złośliwego oprogramowania. Kontroler botnetu, zwany także Botmasterem, kontroluje działania całej struktury (od konkretnych zamówień po aktualizacje oprogramowania) za pośrednictwem różnych kanałów komunikacji. Poziom rozprzestrzeniania się botnetów zależy od zdolności botmasterów do zaangażowania jak największej liczby maszyn próbujących ukryć zarówno działania szkodliwej architektury, jak i lokalizację serwerów C&C. Nie będziemy odnosić się do praktyk w zakresie infekcji lub rozpowszechniania ładunku, ponieważ zostało to już wspomniane we wstępie (np. Blackhole) i ponieważ jest ono ściśle powiązane z wykorzystaniem luk w zabezpieczeniach zaatakowanych systemów (poza zakresem). Próba sklasyfikowania koncepcji botnetu nie jest łatwym zadaniem. Istnieje wiele celów, dla których te architektury są projektowane i tworzone. Nieuchronnie wpływają one na takie czynniki, jak złośliwe oprogramowanie wykorzystywane do narażania ofiar na zagrożenia, a nie na technologię, z której korzystają. Botnety mogą być rozróżniane na przykład ze względu na swoją architekturę. Niektóre sieci opierają się na jednym lub większej liczbie C&C, każdy bot jest bezpośrednio połączony z serwerami dowodzenia i kontroli. Centrum kontroli zarządza listą zainfekowanych komputerów, monitoruje ich status i wydaje im instrukcje operacyjne. Architektura tego typu jest dość prosta w organizacji i zarządzaniu, ale ma tę wadę, że jest bardzo podatna na ataki, ponieważ wyłączenie serwerów kontroli i kontroli spowodowałoby nieprawidłowe działanie całego botnetu. Serwer(y) w rzeczywistości stanowią pojedynczy punkt awarii, ponieważ działanie całego botnetu jest funkcjonalne w stopniu umożliwiającym jego botom dotarcie do systemów kontroli. Początkowo adresy IP C&C były zakodowane na stałe w każdym bocie, co ułatwiło ich identyfikację i ostatecznie doprowadziło do zakłócenia ich działania przez badaczy, ale „napastnicy" za każdym razem uczą się na swoich błędach. Na przykład naturalną ewolucją może być użycie odwrotnego proxy (w niektórych środowiskach zwanego punktem spotkania) w celu adresowania serwera kontroli. W ten sposób łatwiej jest ukryć adresy IP C&C i tożsamości Otmaster (ale właśnie przenieśliśmy pojedynczy punkt awarii z C&C do Reverse Proxy). Dzieje się tak w przypadku architektur scentralizowanych. Bardziej radykalnym i coraz bardziej popularnym sposobem na zwiększenie odporności botnetu jest zorganizowanie botnetu w zdecentralizowanej architekturze jako sieć peer-to-peer (P2P). W botnecie P2P boty łączą się z innymi botami w celu wymiany ruchu C&C, eliminując potrzebę stosowania scentralizowanych serwerów. W rezultacie nie można zakłócać działania botnetów P2P przy użyciu tradycyjnego podejścia polegającego na atakowaniu scentralizowanych infrastruktur. Zatem boty niekoniecznie są połączone z serwerami kontroli i kontroli, ale tworzą strukturę siatkową, w której polecenia są również przesyłane „zombie do zombie". Każdy węzeł sieci posiada listę adresów „sąsiadujących" botów, z którymi wymieniają polecenia. W podobnej strukturze każdy bot mógłby wysyłać rozkazy innym i atakującym, aby przejąć kontrolę nad całym botnetem, ale potrzebuje dostępu do co najmniej jednego komputera. Śledzenie botnetów P2P wymaga pełnego wyliczenia węzłów, podczas gdy w zwykłych botnetach konieczne jest odnalezienie jedynie serwerów C&C. Społeczność zajmująca się bezpieczeństwem próbowała w ten sposób zidentyfikować zainfekowane maszyny, zbierając adresy IP uczestniczących węzłów. Zebrane elementy mogą zostać wykorzystane przez systemy ochrony bezpieczeństwa do zidentyfikowania źródeł infekcji, jest to jednak bardzo trudne, ponieważ w wielu przypadkach boty znajdują się za zaporami sieciowymi lub urządzeniami NAT. Badacze bezpieczeństwa firmy Symantec wykryli odmianę popularnego szkodliwego oprogramowania Zeus, które opiera się na komunikacji P2P jako systemie

zapasowym na wypadek, gdyby serwery C&C były nieosiągalne. Wariant wyizolowany przez firmę Symantec nie wykorzystuje serwerów C&C realizujących autonomiczny botnet. Ten typ botnetu jest naprawdę niepokojący i trudny do zwalczania ze względu na brak pojedynczego punktu awarii, jak ma to miejsce w klasycznej architekturze botnetów. Pomimo tego, że zniszczenie zdecentralizowanego botnetu jest trudniejsze (a może niemożliwe?), ten typ architektury charakteryzuje się większą złożonością zarządzania. Powinno być teraz jasne, że kontrolery i kontrolery odgrywają zasadniczą rolę w funkcjonowaniu botnetów, które zazwyczaj są hostowane na zhakowanych, kupionych lub wynajmowanych serwerach. Co więcej, niezależnie od zastosowanej architektury, botnet musi połączyć każdego bota z jednym lub większą liczbą serwerów kontroli, aby otrzymywać polecenia lub kraść informacje. Wtedy kanał komunikacyjny jest kolejnym istotnym czynnikiem różnicującym botnety. Dlatego botnety można klasyfikować również na podstawie używanego protokołu sieciowego. Stary schemat botnetu był klasyczny, zorientowany na IRC, czyli oparty na programie Internet Relay. Każdy bot otrzymuje polecenie poprzez kanał IRC od bota IRC. Bot IRC składa się z zestawu skryptów łączących się z Internet Relay Chat jako klientem. Od tego czasu nastąpiło jednak wiele zmian, a wszystkie miały na celu zaciemnienie rzeczywistości i/lub szyfrować kanał komunikacyjny. Większość zaawansowanych botnetów wykorzystuje własne protokoły oparte na protokołach takich jak TCP, ICMP czy UDP. Przykładowo przed wariantem Zeusa P2P ekspert zauważył, że autorzy zaimplementowali komunikację poprzez protokół UDP. Historycznie rzecz biorąc, protokół UDP był już używany w przeszłości jako rzeczywisty kanał transmisji danych (fałszywe zapytania A DNS przenoszące ładunek), ale to protokół UDP, a raczej protokół DNS, był intensywnie wykorzystywany przez boty do identyfikacji nazwy domeny własnych serwerów C&C. Botmasterzy zakodowali algorytmy w swoim złośliwym oprogramowaniu, automatycznie i dynamicznie generując dużą liczbę w pełni kwalifikowanych nazw domen internetowych, znanych również jako algorytm generowania domeny (DGA). W ten sposób autorzy, wykonując te same algorytmy, mogą ukryć swoje serwery C&C za różnymi i bardzo dynamicznymi nazwami domen. Oczywiście wszystkie domeny generowane przez DGA mają krótki okres życia, ponieważ są używane tylko przez ograniczony czas i generują duży ruch NXDomain. Potrzebują także współpracy ze strony określonego rodzaju dostawców usług hostingowych, którzy zagwarantują operatorom, że nie będą reagować na skargi na nadużycia ani nie będą współpracować w przypadku żądań usunięcia treści. Dostawcy ci są powszechnie znani jako „kuloodporny hosting" i są szeroko wykorzystywani w ekosystemie cyberprzestępczości (jednak ich usługi są zazwyczaj droższe i mogą nie być w 100% niezawodne). Oczywiście nie możemy zapominać o botnetach internetowych, które stanowią zbiór zainfekowanych maszyn kontrolowanych za pośrednictwem sieci WWW. Boty HTTP łączą się z określonym serwerem internetowym, odbierają polecenia i wysyłają dane. Ten typ architektury jest bardzo łatwy we wdrożeniu i zarządzaniu, a także bardzo trudny do śledzenia w przypadku dodania szyfrowania (HTTP). Botnet Nugache , który pojawił się na początku 2006 roku, jako jeden z pierwszych zastosował silne szyfrowanie. Polecenia podpisano 4096-bitowym kluczem RSA, aby zapobiec nieuprawnionej kontroli, a komunikację pomiędzy urządzeniami równorzędnymi szyfrowano przy użyciu indywidualnie negocjowanych kluczy sesyjnych pochodzących z określonego schematu RSA. Najważniejszą zaletą botnetów jest możliwość zapewnienia anonimowości poprzez wykorzystanie zarówno wielowarstwowej architektury C&C, jak i różnych kanałów komunikacji. Korzystanie ze standardowych protokołów aplikacji, takich jak HTTPS, może również ułatwić rozprzestrzenianie się do sieci korporacyjnych. Zamiast tego użycie niestandardowych protokołów (typowych dla botnetu P2P), zapewniając jednocześnie większą elastyczność, może zostać zneutralizowane przez systemy firewall. Wreszcie poszczególne boty nie mogą być fizycznie własnością botmastera (odwrotna piramida kryminalna w poprzednim akapicie) i mogą znajdować się w kilku lokalizacjach na całym świecie. Różnice w strefach czasowych, językach i przepisach utrudniają śledzenie szkodliwych działań botnetów ponad granicami międzynarodowymi.

STUDIUM PRZYPADKU — EUROGRABBER (2012)

To studium przypadku wyrafinowanego, wielowymiarowego i ukierunkowanego ataku, w wyniku którego ponad 30 000 klientów wielu banków w całej Europie ukradło ponad 36 milionów euro. Ataki rozpoczęły się we Włoszech, a wkrótce potem w Niemczech, Hiszpanii i Holandii wykryto dziesiątki tysięcy zainfekowanych klientów banków internetowych. Całkowicie przejrzyści: klienci bankowości internetowej nie mieli pojęcia, że zostali zainfekowani trojanami, że ich sesje bankowości internetowej zostały naruszone lub że środki zostały skradzione bezpośrednio z ich kont. Ta kampania ataków została odkryta i nazwana „Eurograbber" przez firmy Versafe i Check Point Software Technologies (Kalige i Burkley, 2012). Atak Eurograbber wykorzystuje nową, bardzo skuteczną odmianę trojana ZITMO, czyli Zeus-In-The-Mobile. Jak dotąd exploit ten został wykryty jedynie w krajach strefy euro, ale odmiana tego ataku może potencjalnie wpłynąć również na banki w krajach spoza Unii Europejskiej. Wieloetapowy atak zainfekował komputery i urządzenia mobilne klientów bankowości internetowej, a po zainstalowaniu na obu urządzeniach trojanów Eurograbber sesje bankowości internetowej klientów banku były całkowicie monitorowane i manipulowane przez osoby atakujące. Nawet mechanizm uwierzytelniania dwuskładnikowego stosowany przez banki w celu zapewnienia bezpieczeństwa transakcji w bankowości internetowej został w ataku ominięty i wykorzystany przez atakujących do uwierzytelnienia nielegalnego przelewu finansowego. Co więcej, trojan używany do atakowania urządzeń mobilnych został opracowany zarówno dla platformy Blackberry, jak i Androida, aby ułatwić utworzenie szerokiego „rynku docelowego" i jako taki był w stanie infekować zarówno użytkowników bankowości korporacyjnej, jak i prywatnej oraz nielegalnie przelewać środki z kont klientów w kwotach od 500 do 250 000 euro każdy. To studium przypadku zawiera szczegółowy opis przebiegu pełnego ataku, od początkowej infekcji aż do nielegalnego transferu środków finansowych. Aby zwiększyć bezpieczeństwo transakcji internetowych, banki dodały drugi mechanizm uwierzytelniania, inny niż numer rachunku i hasło, który potwierdza tożsamość klienta i integralność transakcji internetowej. W szczególności, gdy klient banku dokonuje transakcji w bankowości internetowej, bank wysyła SMS-em numer uwierzytelniający transakcję (TAN) na urządzenie mobilne klienta. Następnie klient potwierdza i kończy transakcję bankową, wprowadzając otrzymany numer TAN na ekranie sesji bankowości internetowej. Eurograbber jest dostosowany do specjalnego obejścia nawet tego uwierzytelniania dwuskładnikowego. Problemy klientów banku zaczynają się, gdy klikną „zły link", który pobiera na ich komputer dostosowanego trojana. Dzieje się tak podczas przeglądania Internetu lub, co bardziej prawdopodobne, w wyniku odpowiedzi na wiadomość e-mail typu phishing, która zachęca klienta do kliknięcia fałszywego łącza. Jest to pierwszy etap ataku i następnym razem, gdy klient loguje się na swoje konto bankowe, zainstalowany teraz trojan (dostosowane warianty trojanów Zeus, SpyEye i CarBerp) rozpoznaje login, co uruchamia kolejną fazę ataku . Jest to kolejna faza, w której Eurograbber pokonuje uwierzytelnianie banku metodą wo-factor i stanowi doskonały przykład wyrafinowanego, ukierunkowanego ataku. Podczas pierwszej sesji bankowości internetowej klienta po zainfekowaniu jego komputera Eurograbber wprowadza do sesji instrukcje, które proszą klienta o podanie numeru telefonu komórkowego. Następnie zostaje poinformowany o konieczności dokończenia „aktualizacji zabezpieczeń oprogramowania bankowego", postępując zgodnie z instrukcjami przesłanymi na jego urządzenie mobilne za pomocą wiadomości SMS. Wiadomość SMS atakującego instruuje klienta, aby kliknął łącze w celu dokończenia „aktualizacji zabezpieczeń" na swoim telefonie komórkowym; jednakże kliknięcie łącza powoduje pobranie wariantu trojana „Zeus in the mobile" (ZITMO). Wariant ZITMO został specjalnie zaprojektowany do przechwytywania SMS-ów banku zawierających najważniejszy „numer autoryzacji transakcji" (TAN). Kluczowym elementem autoryzacji dwuskładnikowej banku jest SMS banku zawierający numer TAN. Trojan Eurograbber na urządzeniu mobilnym klienta przechwytuje SMS-y i wykorzystuje numer TAN do sfinalizowania własnej transakcji, aby po cichu przelać pieniądze z konta klienta banku. Atak Eurograbbera odbywa się

całkowicie w tle. Po zakończeniu „modernizacji zabezpieczeń” klient banku jest monitorowany i kontrolowany przez osoby atakujące Eurograbber, a sesje bankowości internetowej klienta nie dają żadnych dowodów na nielegalną działalność. Aby ułatwić tak wyrafinowany, wieloetapowy atak, należało stworzyć infrastrukturę serwerów dowodzenia i kontroli (C&C). Infrastruktura ta otrzymywała, przechowywała i zarządzała informacjami wysyłanymi przez trojany, a także organizowała ataki. Zebrane informacje zostały zapisane w bazie danych SQL w celu późniejszego wykorzystania podczas ataku. Aby uniknąć wykrycia, napastnicy wykorzystali kilka różnych nazw domen i serwerów, z których niektóre były serwerami proxy, co jeszcze bardziej skomplikowało wykrywanie. W przypadku wykrycia napastnicy mogliby łatwo i szybko wymienić swoją infrastrukturę, zapewniając w ten sposób integralność infrastruktury ataku oraz ciągłość działania i nielegalny przepływ pieniędzy.

INFEKCJA

Krok 1: Komputer stacjonarny lub laptop klienta jest zainfekowany.

Krok 2: Trojan Eurograbber przechwytuje sesję bankową i wstawia JavaScript na stronę bankową klienta. Ten złośliwy JavaScript informuje klienta o „aktualizacji zabezpieczeń” i instruuje go, jak postępować.

Krok 3: Trojan Eurograbber dostarcza następnie informacje mobilne klienta banku do strefy zrzutu w celu przechowywania i wykorzystania w kolejnych atakach.

Krok 4: Otrzymanie informacji mobilnej klienta uruchamia proces Eurograbber polegający na wysłaniu wiadomości SMS na urządzenie mobilne klienta. Wiadomość SMS instruuje klienta, aby dokończył aktualizację zabezpieczeń, klikając załączony link. Spowoduje to pobranie na urządzenie mobilne klienta pliku z odpowiednią mobilną wersją trojana Eurograbber.

Krok 5: Równocześnie z wysłaniem wiadomości SMS na urządzenie mobilne klienta banku, na pulpicie klienta pojawia się komunikat instruujący, aby postępować zgodnie z instrukcjami zawartymi w wiadomości SMS wysłanej na urządzenie mobilne w celu aktualizacji oprogramowania systemu w celu zwiększenia bezpieczeństwa. Po zakończeniu należy wprowadzić kod weryfikacyjny instalacji w polu poniżej, aby potwierdzić, że proces aktualizacji mobilnej został ukończony.

Krok 6: Po zakończeniu instalacji w ojczystym języku klienta pojawia się to pole tekstowe, potwierdzające pomyślną instalację i wyświetlające kod weryfikacyjny, który użytkownik musi wprowadzić w wierszu poleceń na swoim komputerze.

Krok 7: Eurograbber kończy proces, wyświetlając na pulpicie klienta komunikaty informujące użytkownika o pomyślnym ukończeniu aktualizacji „bezpieczeństwa” i możliwości kontynuowania czynności związanych z bankowością internetową

KRADZIEŻ PIENIĘDZY

Krok 1: Klient bankowości loguje się do swojego internetowego konta bankowego.

Krok 2: Zaraz po zalogowaniu się klienta banku cyberprzestępca inicjuje trojana komputerowego Eurograbber, aby rozpocząć własną transakcję mającą na celu przelanie określonego procentu pieniędzy z rachunku bankowego klienta na konto „muła” należące do atakujących.

Krok 3: Po złożeniu nielegalnej transakcji bankowej bank wysyła SMS-em numer autoryzacji transakcji (TAN) na urządzenie mobilne użytkownika.

Krok 4: Jednakże mobilny trojan Eurograbber przechwytuje wiadomość SMS zawierającą numer TAN, ukrywa ją przed klientem i przekazuje na jeden z wielu numerów telefonów przekaźnikowych skonfigurowanych przez atakujących. Wiadomość SMS jest następnie przekazywana z numeru telefonu przekaźnikowego do strefy zrzutu, gdzie jest przechowywana w bazie danych dowodzenia i kontroli wraz z innymi informacjami o użytkowniku. Gdyby wiadomość SMS została przekazana bezpośrednio do strefy zrzutu, byłaby łatwiejsza do wykrycia.

Krok 5: Numer TAN jest następnie pobierany z pamięci przez trojana komputerowego, który z kolei wysyła go do banku w celu dokończenia nielegalnego przelewu pieniędzy z konta klienta banku na konto „muła" atakującego. Na ekranie klienta nie widać żadnej z tych aktywności i jest on całkowicie nieświadomy oszukańczego działania, które właśnie miało miejsce .

W tym momencie na koncie bankowym ofiary nastąpi utrata środków bez jej wiedzy. Cyberprzestępcy zarabiają na kontach typu mule. Cały proces odbywa się za każdym razem, gdy klient banku loguje się na swoje konto bankowe.

STUDIUM PRZYPADKU — ZEROWY DOSTĘP (2013)

Najszybciej rozwijającym się botnetem był z pewnością ZeroAccess, który w 2012 roku spowodował miliony infekcji na całym świecie, obsługując aż 140 000 unikalnych adresów IP w USA i Europie (F-Secure 2012). Szkodliwe oprogramowanie, które zamienia komputery użytkowników w boty, jest zazwyczaj obsługiwane przez złośliwe witryny, do odwiedzenia których użytkownik zostaje oszukany. Szkodliwa witryna zawiera zestaw exploitów, zwykle Blackhole, którego celem jest wykorzystanie luk w zabezpieczeniach komputera użytkownika podczas odwiedzania witryny. Po zhakowaniu komputera zestaw usuwa złośliwe oprogramowanie, które następnie zamienia komputer w bota ZeroAccess. Następnie bot codziennie pobiera nową listę reklam z serwera dowodzenia i kontroli (C&C) ZeroAccess. Według doniesień botnet ZeroAccess klika 140 milionów reklam dziennie. Ponieważ jest to zasadniczo oszustwo związane z kliknięciami, oszacowano, że botnet kosztuje legalnych reklamodawców internetowych nawet 900 000 USD dziennie. Liczba oszustw związanych z kliknięciami rośnie, ponieważ dostawcy reklam internetowych tak naprawdę nie mają możliwości odróżnienia kliknięcia uzasadnionego od fałszywego. ZeroAccess to jeden z najbardziej znanych obecnie botnetów. Został on po raz pierwszy odkryty przez badaczy w 2010 roku, kiedy wzbudził duże zainteresowanie ze względu na jego zdolność do kończenia wszystkich procesów związanych z narzędziami bezpieczeństwa, w tym tymi należącymi do produktów antywirusowych. Kiedy jednak zbyt wielu badaczy skupiło się na tej możliwości samoobrony, autorzy ZeroAccess zdecydowali się porzucić tę funkcję i bardziej skupić się na ulepszeniu niestandardowego protokołu sieciowego peer-to-peer (P2P), który jest unikalny dla ZeroAccess. Zaobserwowano cztery różne warianty: Po zmianie ZeroAccess stał się łatwiejszy do wykrycia przez produkty antywirusowe, mimo to nadal rozprzestrzeniał się błyskawicznie po całym świecie dzięki ulepszonej technice P2P. Sukces ten można w dużej mierze przypisać programowi partnerskiemu, dobrze znanej strategii marketingowej szeroko stosowanej w wielu witrynach e-commerce. Zasadniczo właściciel firmy prowadzącej witrynę handlu elektronicznego może promować prowizje dla innych właścicieli witryn, aby przyciągnąć do niej klientów (i, miejmy nadzieję, ostatecznie dokonać zakupu). Właściciele witryn internetowych otrzymują następnie wynagrodzenie za dostarczanie potencjalnych klientów. Przyjmując tę koncepcję, autorowi lub operatorowi ZeroAccess udało się rozpowszechnić program na dużej liczbie komputerów przy pomocy zarejestrowanych partnerów. Zespół ZeroAccess reklamuje instalator złośliwego oprogramowania na rosyjskich podziemnych forach, aktywnie poszukując partnerów-dystrybutorów. Ich celem było znalezienie innych cyberprzestępców, którzy są w stanie skuteczniej i skuteczniej dystrybuować szkodliwe oprogramowanie. Dystrybutorzy złośliwego oprogramowania zazwyczaj składają się z doświadczonych partnerów, z których każdy stosuje własne metody dystrybucji instalatorów Zeroaccess, aby spełnić

wymagania osoby rekrutującej. Najpopularniejsze metody dystrybucji obejmują zestawy exploitów, wiadomości e-mail ze spamem, trojany pobierające i fałszywe pliki multimedialne dostępne w serwisach wymiany plików P2P i witrynach wideo, chociaż szczegółowe informacje zależą od dystrybutora obsługującego te operacje. Różnorodność schematów dystrybucji i metod stosowanych przez licznych partnerów przyczyniła się do dużej liczby wariantów „trojanów dropperów" wykrywanych codziennie przez produkty antywirusowe. Wszystkim kierują się tym samym motywem, którym jest uzyskanie atrakcyjnego udziału w przychodach od gangu. Partnerzy otrzymują wynagrodzenie w oparciu o schemat usługi Pay-Per-Install (PPI), a stawka różni się w zależności od położenia geograficznego komputera, na którym pomyślnie zainstalowano złośliwe oprogramowanie. Pomyślna instalacja w Stanach Zjednoczonych zapewni najwyższą wypłatę, a gang będzie skłonny zapłacić 500 dolarów za 1000 instalacji w tej lokalizacji. Biorąc pod uwagę stawkę wynagrodzenia, nie jest zaskoczeniem, że ZeroAccess jest szeroko rozpowszechniony w samych Stanach Zjednoczonych. Po Stanach Zjednoczonych stawka prowizji posortowana od najwyższej do najniższej to Australia, Kanada, Wielka Brytania i inne. Niektórzy dystrybutorzy publikują nawet na nielegalnych forach zrzuty ekranu przedstawiające otrzymane płatności, aby pokazać wiarygodność swojego rekrutera. Zespół ZeroAccess może sobie pozwolić na płacenie swoim rekrutom tak wysokich premii, ponieważ armia botów stworzona dzięki wysiłkom partnera jest w stanie wygenerować w zamian jeszcze większe przychody. Po pomyślnym zainstalowaniu złośliwego oprogramowania na komputerach ofiar ZeroAccess rozpocznie pobieranie i instalowanie dodatkowego złośliwego oprogramowania na komputerach, co będzie generować zyski dla operatorów botnetu w wyniku oszustw związanych z kliknięciami. Program partnerski, jako interesujący przestępczy model biznesowy, zachęca do rozprzestrzeniania złośliwego oprogramowania i przyciąga więcej cyberprzestępców ze względu na ugruntowaną reputację operatorów botnetów w zakresie niezawodnych płatności dla swoich podmiotów stowarzyszonych i dostosowywania stawek prowizji w celu utrzymania ich atrakcyjności. Organizacje przestępcze stojące za botnetem pokazały, że są skłonne eksperymentować i modyfikować swój „produkt", aby zwiększyć swoje możliwości zarabiania pieniędzy. Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3) Europolu, wspierane przez Jednostkę ds. Przestępczości Cyfrowych Microsoft Corporation i innych partnerów branżowych, ogłosiło, że w 2013 r. skutecznie zakłócało działanie sieci ZeroAccess, jednak, jak wiemy, sieci P2P są bardzo odporne na zakłócenia i należy spodziewać się pewnych skutków ubocznych.

ŚRODKI ZARADCZE MAJĄCE NA CELU ZWALCZANIE BOTNETÓW LUB ŁAGODZENIE SKUTKÓW BOTNETÓW

Ze względu na wysoki poziom dostosowywania złośliwych programów, dość trudno jest zastosować skuteczny i skuteczny środek zaradczy poprzez analizę kodu i definicję odcisków palców, co oczywiście jest dobrze znaną praktyką systemów antywirusowych. Potrzebujemy więc metod analizujących zachowanie złośliwego oprogramowania (niezależnie od używanej architektury i protokołów, boty muszą kontaktować się ze swoimi kontrolerami i kontrolerami — możesz ukryć wszystko oprócz ruchu sieciowego!). Jednak nawet analiza behawioralna nie jest łatwa w zarządzaniu. Zwykle włożono już wiele pracy w analizę standardowych protokołów (zazwyczaj poziomu 4 i 5 stosu TCP/IP), aby odróżnić legalny ruch od botnetu. Niestety coraz częstsze stosowanie mechanizmów wysokiego szyfrowania oraz technik dostosowywania/zaciemniania ruchu (jak zobaczymy w następnej sekcji) sprawi, że ta praca będzie nieskuteczna w perspektywie średnio- i długoterminowej, nawet jeśli większość prac wspomnianych w tym akapicie została wykonana ujawniło świetną reakcję tylko w przypadku określonych architektur botnetów. Po pierwsze, z operacyjnego punktu widzenia jest to warunek konieczny (prawdopodobnie niewystarczający!), w którym trzeba być gotowym na radzenie sobie z trwającym atakiem botnetu, biorąc pod uwagę na przykład dwa przypadki doskonałości, czyli kampanię spamową i atak DDOS , polega na sprawdzeniu, czy:

• zapora sieciowa obsługująca Internet ma pojemność „Systemu wykrywania/zapobiegania włamaniom” i przepustowość znacznie zawyżoną w porównaniu do normalnych warunków pracy i dostępnej przepustowości Internetu;

• System antyspamowy jest skonfigurowany tak sztywno, jak to możliwe (np. akceptuje tylko wiadomości od MTA, które mają poprawnie skonfigurowane wspólne rekordy DNS MX, PTR i A);

• Twój dostawca usług internetowych jest wyposażony w narzędzia monitorujące, które wykrywają w odpowiednim czasie wzrost ruchu w Twoich usługach internetowych, a w najgorszych przypadkach mogą szybko wyłączyć całe fragmenty Internetu (np. wszystkie trasy międzynarodowe), aby tymczasowo zmniejszyć siłę botnetu;

Jeśli chodzi o cele, które należy osiągnąć, poprzednio musieliśmy rozróżnić dwa różne podejścia. W rzeczywistości administratorzy sieci i bezpieczeństwa są zazwyczaj zainteresowani wykryciem obecności botów i serwerów C&C w swoich sieciach lub przeciwstawieniem się atakowi botnetu (łagodzenie), podczas gdy badacze skupiają swoją uwagę na bezpośredniej identyfikacji samego botnetu (ładunek, architektura , protokoły, przestępcy zdolności itp.) na jego podatność, a w konsekwencji na zakłócenia. Ze względu na zastosowaną metodologię metody polowania na botnety można podzielić na dwie kluczowe kategorie:

• Pasywne: takie możliwości są zwykle organizowane za pomocą rozwiązań do monitorowania sieci w korporacyjnych sieciach LAN. Techniki te opierają się zasadniczo na analizie statystycznej ruchu TCP i UDP, analizie protokołów konkretnych aplikacji, takich jak HTTP lub DNS, a także rozpoznawaniu wzorców określonych słów kluczowych lub adresów IP, które mają zostać umieszczone na czarnej liście.

• Aktywne: techniki te zwykle opierają się na skanowaniu, przeszukiwaniu lub pogłębianiu zakresów adresów IP, sondowaniu obecności botów i/lub partnerów C&C w wyniku analizy konkretnych odpowiedzi na zapytania (zwykle za pośrednictwem sieci Honeynet). Praktyki te mają również na celu wykorzystanie luk w protokołach lub serwerach C&C.

Jak wspomniano wcześniej, możemy założyć, że botnety różnią się od innych form złośliwego oprogramowania tym, że korzystają z kanałów kontroli i kontroli, które stanowią podstawowy mechanizm umożliwiający botmasterowi kierowanie działaniami botów w botnecie. W związku z tym kanał C&C można uznać za najsłabsze ogniwo scentralizowanego botnetu. Oznacza to, że jeśli uda nam się zniszczyć aktywny serwer C&C lub po prostu przerwać komunikację z serwerem C&C, botmaster nie będzie mógł kontrolować botnetu. Co więcej, wykrycie kanału C&C ujawni zarówno serwery C&C, jak i boty w monitorowanej sieci. Dlatego zrozumienie i wykrycie serwerów C&C ma ogromną wartość w walce ze scentralizowanymi botnetami. Ruch C&C botnetów jest trudny do wykrycia, ponieważ: następuje normalne użycie protokołu i jest podobny do normalnego ruchu; natężenie ruchu jest niskie; w monitorowanej sieci może znajdować się bardzo niewiele botów i może zawierać szyfrowaną komunikację. Jednakże boty scentralizowanego botnetu wykazują korelację przestrzenno-czasową i podobieństwa ze względu na charakter ich wstępnie zaprogramowanych działań w odpowiedzi na polecenia kontrolne. Na przykład w podobnym czasie wszystkie boty w tym samym botnecie wykonają to samo polecenie i zgłoszą serwerowi kontroli postęp/wynik zadania (a raporty te prawdopodobnie będą miały podobną strukturę i treść). Jest mało prawdopodobne, aby regularne działania sieciowe wykazywały takie zsynchronizowane i skorelowane zachowanie i chociaż ruch jest szyfrowany, przydatne może być zbadanie ruchu generowanego przez grupy klientów mających tę samą parę docelową (IP, port TCP).

Kiedy botnety przełączają się na strukturę peer-to-peer (P2P) i wykorzystują wiele protokołów do celów kontroli i kontroli, powyższe założenia tracą ważność. W rezultacie wykrywanie botnetów P2P

jest trudniejsze. Jednym z możliwych podejść jest zaprojektowanie szczególnego rodzaju „hurtowni danych o ruchu sieciowym". Przechwytując wystarczającą ilość danych o ruchu sieciowym (dane szkoleniowe), proponowane podejście może profilować (klastrować) zachowanie normalnych działań aplikacji/użytkowników od innych. W rzeczywistości sekwencja działań różni się znacznie w przypadku zwykłego użytkownika i botnetu. Ponieważ botnet ma charakter dynamiczny: elementy równorzędne w botnecie można w dowolnym momencie dynamicznie zamykać lub usuwać z botnetu, bot może najpierw wygenerować ruch, aby znaleźć na swojej liście równorzędnych partnerów online na określonych portach, a następnie wysłać polecenie do wszystkich dostępnych rówieśników. Z drugiej strony jest bardzo mało prawdopodobne, aby zwykły użytkownik (lub większość zwykłych użytkowników) zachowywał się w ten sposób normalnie. Chociaż zwykli użytkownicy mają możliwość wyboru dowolnych miejsc docelowych, zazwyczaj kojarzą się z niewielkim zakresem miejsc docelowych o różnej popularności. Z drugiej strony, równorzędni wybierani w botnetach P2P są losowi, niezależnie od popularności miejsca docelowego. W ten sposób moglibyśmy obliczyć pewne miary statystyczne (np. test oparty na proporcjach zachowania lub test oparty na średniej odległości zachowania) w celu zidentyfikowania nowych próbek danych o ruchu sieciowym. Jeżeli nie można wyłączyć serwera kontroli, inną opcją jest przekierowanie szkodliwego ruchu do „sinkhole" – strategia, która znalazła zastosowanie w najnowszych technikach ograniczania zagrożeń, zarówno lokalnie, jak i globalnie. Zapadliska rejestrują złośliwy ruch, analizują go, a następnie upuszczają w taki sposób, że nie może dotrzeć do pierwotnego celu, dla którego jest przeznaczony. Jednym z przykładów typu „sinkholing" jest routing zerowy DDoS. W przypadku, gdy ruch należy do trwającej próby DDoS, jest on odrzucany i czasami zliczany do późniejszej analizy. Routing zerowy DDoS na routerach granicznych to obiecujące podejście do łagodzenia ataków DDoS, ale wiąże się z wyzwaniami polegającymi na niezawodnej identyfikacji ruchu związanego z atakiem i czystej separacji strumieni danych o dużej przepustowości na wczesnym etapie. Jest to zasadniczo możliwe jedynie na poziomie dostawcy usług internetowych. Dwa zupełnie różne podejścia do polowania na botnety opierają się na analizie informacji o błędach protokołu i pasywnej analizie protokołu DNS w celu wykrycia zombie. Pierwszy z nich wykorzystuje nowe podejście oparte na zachowaniu do wykrywania zainfekowanych hostów w sieci korporacyjnej. Celem jest opracowanie systemu niezależnego od rodziny złośliwego oprogramowania i niewymagającego „apriorycznej" wiedzy na temat semantyki złośliwego oprogramowania ani mechanizmów dowodzenia i kontroli (C&C). Podejście to opiera się na prostej obserwacji, że wiele wzorców komunikacji złośliwego oprogramowania skutkuje nienormalnie wysokimi wskaźnikami awaryjności, co rozciąga się na szeroką klasę błędów zarówno na poziomie protokołu TCP/IP transportu, jak i aplikacji. W rzeczywistości ankieta przeprowadzona na 32 różnych instancjach złośliwego oprogramowania ujawniła niektóre typowe komunikaty o błędach. Z ilościowego punktu widzenia wspomniane badanie wykazało, że większość przypadków złośliwego oprogramowania (18 z 24 przypadków) spowodowała awarie DNS. Ze względu na ważną rolę, jaką DNS odgrywa w działaniu Internetu, drugie podejście opiera się na wyłącznej analizie tego protokołu. Nie jest zaskakujące, że szeroka gama szkodliwych działań wiąże się w taki czy inny sposób z usługą nazw domen. Boty rozpoznają nazwy DNS, aby zlokalizować swoje serwery C&C, a wiadomości spamowe zawierają adresy URL prowadzące do domen, które są rozpoznawane jako serwery oszustwa. Dlatego skuteczne wydaje się monitorowanie wykorzystania systemu DNS w celu sprawdzenia, czy dana nazwa jest wykorzystywana w ramach złośliwej operacji. Jeśli adres IP centrum kontroli jest zakodowany na stałe w pliku binarnym bota, istnieje pojedynczy punkt awarii botnetu. Ilekroć ten adres zostanie zidentyfikowany i usunięty, botnet zostanie utracony. Zatem atakujący, korzystając z DNS, zapewniają elastyczność i odporność na awarie, których potrzebują w złośliwych architekturach, którymi zarządzają. ponadto mogą ukryć swoje krytyczne serwery za usługami proxy, co utrudnia ich identyfikację i usunięcie. Dlatego też badanie zachowania DNS znanych złośliwych i łagodnych domen, w możliwie największym stopniu pod względem czasu obserwacji i zaobserwowanego natężenia ruchu,

mogłoby ewentualnie zidentyfikować wyróżniające się cechy ogólne, które są w stanie określić złośliwość danej domeny. Na przykład 15 różnych funkcji może wskazywać na wykrywanie złośliwych zachowań. Istnieje wiele innych podejść mających na celu identyfikację, wyliczenie i zatrucie, zwykle określanych jako botnet P2P (peer crawling). Podejścia te zwykle dotyczą bardzo pionowych badań małych rodzin botnetów, jeśli nie pojedynczego botnetu. Podstawową ideą jest próba przyłączenia się do konkretnego botnetu i kontekstowego zrozumienia jego architektury, protokołów, rozmiaru, a następnie nakreślenie sposobów jego zakłócania lub po prostu łagodzenia skutków.

WNIOSKI I PRZYSZŁE TENDENCJE (TOR, SIECI MOBILNE I SPOŁECZNOŚCIOWE)

Świątynia botnetów opiera się na trzech głównych filarach. Wszechobecne rozpowszechnienie Internetu wzmacnia te trzy filary. Wszystkie urządzenia wyposażone w łącze internetowe mogą potencjalnie stać się przyszłymi zombie. W rzeczywistości głównymi kandydatami są obecnie smartfony i tablety, a my byliśmy już świadkami działań przestępczych związanych z rozprzestrzenianiem szkodliwego oprogramowania dla urządzeń mobilnych (np. ZITMO). Wciąż niewiele osób zdaje sobie sprawę z zagrożeń, jakie może nieść ze sobą nowoczesne urządzenie. Konwergencja technologiczna jest coraz bardziej inwazyjna – prawie wszystkie przedmioty codziennego użytku są „podłączone do Internetu" i inteligentne. Raczej nie będzie żadnego przeciwnego trendu. Oprócz powszechnego stosowania szyfrowania kanałów komunikacyjnych, w ostatnim czasie zaobserwowaliśmy rozpowszechnianie się wykorzystywania sieci społecznościowych w ramach botnetu. Jednym z głównych celów botmasterów jest dotarcie do szerokiego grona użytkowników, więc naturalne jest, że badają możliwość wykorzystania platform mediów społecznościowych do rekrutacji nowych zombie i kontrolowania zainfekowanych maszyn (zazwyczaj tworzenia fałszywych kont, które wysyłają zaszyfrowane wiadomości do złośliwe oprogramowanie na ofiarach), ponieważ sieci społecznościowe zmonopolizowały większość korzystania z Internetu przez użytkownika. Botmasterzy zaczęli wykorzystywać witryny sieci społecznościowych (np. Twitter.com) jako centralę C&C, co okazuje się dość ukryte, ponieważ trudno odróżnić działania C&C od normalnego ruchu w sieciach społecznościowych. „UPD4T3" to przykład fałszywego konta na Twitterze, którego właścicielem jest oczywiście botmaster. Co więcej, wiemy, że TOR to anonimowa sieć obsługiwana przez wolontariuszy, która zapewnia funkcje szyfrowania i ochrony tożsamości. Tor to świetne narzędzie, które pomaga ludziom na całym świecie chronić się przed cenzurą Internetu. Jest powszechnie używany przez każdego, kto troszczy się o prywatność i bezpieczeństwo swojej komunikacji. Jednocześnie jednak dochodzi do częstych nadużyć, jak w przypadku, który będziemy opisywać. Potencjalne wykorzystanie TOR w infrastrukturze botnetów było omawiane w przeszłości kilka razy (np. podczas konferencji „Defcon 18" prowadzonej przez Dennisa Browna). We wrześniu 2012 roku niemiecki dostawca oprogramowania antywirusowego G-Data pokrótce opisał podobny przypadek. Jak już wiemy, hostowanie infrastruktury C&C na „serwerach internetowych" może ujawnić botnet. Znacznie silniejszą infrastrukturę można zbudować po prostu wykorzystując Tor jako protokół komunikacji wewnętrznej i korzystając z funkcjonalności Tor Hidden Services. Usługi ukryte, wprowadzone w 2004 roku, pozwalają na tworzenie całkowicie anonimowych i ukrytych usług dostępnych wyłącznie za pośrednictwem Tora. Generowana jest pseudodomena „cebulowa", która następnie zostanie wykorzystana do rozpoznania i skontaktowania się z ukrytym serwerem. Bardzo trudno jest zidentyfikować pochodzenie usługi ukrytej i unieważnić lub przejąć powiązaną domenę cebulową. Zaletami tego podejścia są:

- Ruch jest szyfrowany.
- Usługi ukryte nie opierają się na publicznych adresach IP.

Zagrożenie, jakie stwarza rozprzestrzenianie się botnetów, jest niestety nadal domeną światów, które z różnych powodów (technicznych lub historycznych) są ściśle powiązane ze słowami „Internet" i „Komputer". Co więcej, dopiero niedawno widzieliśmy konkretne przykłady jego przełożenia na skuteczne działania przestępcze (monetyzacja możliwości operacyjnych botnetu). Google korzysta z Internetu, e-mail korzysta z Internetu, Home Banking korzysta z Internetu. Czy nadal korzystamy z Internetu, grając z przyjacielem (który mieszka na drugim końcu świata) za pośrednictwem naszego domowego Wi-Fi? Czy „Aplikacja Waze" nadal korzysta z Internetu? Oczywiście, że tak. Jeśli możesz oglądać YouTube na swoim telewizorze Smart TV, być może potrzebujesz zainstalowanego na nim programu antywirusowego lub (dlaczego nie) zapory sieciowej (zwykle instalowanej na komputerze stacjonarnym lub laptopie). Opisane w poprzednim akapicie środki zaradcze należy rozszerzyć na tych dostawców, których podstawowa działalność do tej pory była zupełnie inna. W niezbyt odległej przyszłości atak DOS na „system telewizji kablowej do transmisji telewizyjnej" lub na system VOIP operatora telefonii – dwa rzeczywiste przykłady infrastruktury krytycznej – może zwiastować scenariusze cyberterroryzmu. Wyżej wymienione scenariusze stwarzają poważne obawy dotyczące rozwoju botnetów w przyszłości, rozszerzając zagrożony obszar docelowych infrastruktur. W związku z tym do uporania się z tym problemem zostanie wezwanych wiele zainteresowanych stron, stosując różną równowagę synergicznych środków zaradczych w celu ograniczenia ryzyka.

Ewolucja TETRA poprzez integrację z wieloma platformami komunikacyjnymi w celu wsparcia ochrony ludności i pomocy w przypadku katastrof (PPDR)

WSTĘP

Organizacje zajmujące się ochroną publiczną i pomocą w przypadku katastrof (PPDR), takie jak organy ścigania, pogotowie ratunkowe, zarządzanie kryzysowe i usuwanie skutków katastrof, straż pożarna, straż przybrzeżna, służby poszukiwawczo-ratownicze, administracja rządowa itp., mają za zadanie zapewnianie bezpieczeństwa publicznego praca. Usługi bezpieczeństwa publicznego wnoszą wartość do społeczeństwa, tworząc stabilne i bezpieczne środowisko; i organizacje PPDR zajmują się sytuacjami, w których zagrożone jest życie ludzkie, akcje ratownicze i egzekwowanie prawa. Ze względu na charakter takich sytuacji głównym wymogiem jest komunikacja mobilna. Organizacje PPDR w codziennym działaniu w dużym stopniu korzystają z systemów komunikacji profesjonalnego radia mobilnego (PMR). Wiele z tych sieci komunikacyjnych opiera się na specyfikacji TETRA, TETRAPOL, GSM, Project 25 itp., jednakże TETRA stała się powszechnie akceptowanym wyborem w Europie, a TETRAPOL jest używany w niektórych krajach. PPDR jest tematem priorytetowym dla obywateli, rządów krajowych i Unii Europejskiej. Zwłaszcza od wydarzeń takich jak ataki na Światowe Centrum Handlu z 11 września, zamachy bombowe w Atocha (Madryt), ataki w londyńskim metrze i niedawne poważne trzęsienie ziemi w Van w Turcji; bezpieczeństwo, walka z terroryzmem i pomoc w przypadku klęsk żywiołowych znajdują się wśród priorytetów europejskich decydentów, zarówno na szczeblu krajowym, jak i unijnym. Dowody pochodzące z tych niedawnych katastrof pokazują, że publiczne systemy komórkowe nie są zaprojektowane do radzenia sobie z poważnymi incydentami i zawiodły w momencie, gdy najbardziej potrzebna jest dobra komunikacja, stąd znaczenie dedykowanej sieci komunikacyjnej PPDR. Jednakże, ze względu na charakter niektórych z tych wydarzeń oraz rosnącą globalizację terroryzmu (oraz innych zagrożeń bezpieczeństwa i ochrony), bardzo ważne jest, aby przyszłe organizacje PPDR działały ponad granicami państw, co stanowi ograniczenie obecnych sieci komunikacyjnych PPDR. W Europie, zwłaszcza na początku lat 90., kiedy w następstwie Układu z Schengen nastąpiło przekształcenie się w społeczeństwo bez granic, swoboda przekraczania granic oznaczała również, że osoby mające zamiary przestępcze również będą mogły swobodnie przekraczać granice. W rezultacie stało się jasne, że istnieje potrzeba zapewnienia dobrej komunikacji pomiędzy

organizacjami PPDR każdego z krajów i umożliwienia funkcjonariuszom PPDR podróżowania przez granice bez utraty łączności. Sieci krajów sąsiadujących muszą ze sobą współpracować zarówno w zakresie rutynowych, codziennych działań, jak i działań związanych z pomocą w przypadku klęsk żywiołowych. Organizacje PPDR nie mogą sobie pozwolić na ryzyko wystąpienia błędów komunikacyjnych w transmisjach głosu, danych i wideo; a można to zapewnić jedynie poprzez budowę solidnych, bezpiecznych i niezawodnych, nowoczesnych sieci komunikacji mobilnej PPDR. Ponadto, aby organizacje te były odpowiednio przygotowane na przyszłe wydarzenia, takie jak te, których byliśmy ostatnio świadkami, muszą być odpowiednio wyposażone. Istnieje zapotrzebowanie na nowe zaawansowane usługi i aplikacje przewidziane w następnej generacji systemów komunikacji PPDR, takie jak zdalne monitorowanie personelu, sieci zdalnych czujników (śledzenie pożarów lasów lub monitorowanie poziomu wody/powodzi), dwukierunkowe wideo w czasie rzeczywistym, pozycjonowanie 3D i GIS, roboty mobilne, wielofunkcyjne terminale mobilne (weryfikacja tożsamości, przesyłanie obrazów, dane biometryczne, zdalny dostęp do baz danych, urządzenia zdalnie sterowane) itp. Ponadto potrzeba bardzo niezawodnej, bezpiecznej i odpornej sieci komunikacyjnej dla ochrony publicznej, która w stanie stawić czoła zagrożeniom terroryzmem i katastrofami na wszystkich poziomach, w stosunku do obywateli, aż do infrastruktury komunikacyjnej. Jednakże rosnące zapotrzebowanie na niezawodną i bezpieczną szybką transmisję danych oznacza, że bieżąca przepustowość sieci komunikacyjnej PPDR (tj. TETRA) zostanie przekroczona, co będzie wymagało modernizacji lub wymiany na pewnym etapie w przyszłości.

TECHNOLOGIA TETRA

TETRA to nowoczesny standard cyfrowego PMR, który cieszy się szeroką akceptacją (szczególnie w Europie) i obecnie jest uważany za jedną z najbardziej dojrzałych i wiodących technologii na rynkach PPDR. Specyfikacje TETRA są stale rozwijane przez ETSI (Europejski Instytut Norm Telekomunikacyjnych) i wprowadzane są nowe funkcje, aby spełnić rosnące i wciąż wymagające wymagania PPDR. Oryginalny standard TETRA przewidziany po raz pierwszy w ETSI był znany jako standard TETRA Voice plus Data (V + D), z mniejszym naciskiem na stronę danych i obejmującym tylko dwie usługi danych w porównaniu z dziewięcioma usługami głosowymi. Ze względu na potrzebę dalszego rozwoju i udoskonalania TETRA, oryginalny standard V + D jest obecnie znany jako TETRA 1. Packet Data Optimized (PDO) to kompletna część pakietu standardów TETRA opracowanych wyłącznie dla aplikacji komunikacji bezprzewodowej „Tylko dane". (tj. pagery). Jednak bardzo niewielu producentów opracowało systemy i produkty PDO, ponieważ: wszyscy tradycyjni użytkownicy PMR korzystają zarówno z komunikacji głosowej, jak i transmisji danych; a także oczywisty obszar zastosowań takiego standardu (transfer dużych rozmiarów danych) wymagałby znacznej ilości czasu i energii. Niemniej jednak TETRA zapewnia już kompleksową ofertę usług i obiektów. Protokół TETRA określa kilka standardowych interfejsów zapewniających otwarty rynek wielu dostawców: (1) interfejs powietrzny (AIR IF), (2) interfejs urządzeń końcowych (TEI), (3) Interfejs międzysystemowy (ISI), (4) Działanie w trybie bezpośrednim (DMO). Jednakże w miarę upływu czasu istnieje potrzeba ewolucji i ulepszania wszystkich technologii, aby lepiej spełniać wymagania użytkowników, zapewnić przyszłościowe inwestycje i zapewnić długowieczność. Podobnie jak GSM przechodzący na GPRS, EDGE i UMTS/3G, TETRA również będzie ewoluować, aby zaspokoić rosnące zapotrzebowanie użytkowników na nowe usługi i udogodnienia. Z tego powodu opracowano standard TETRA 2, który jest wystarczająco kompletny do celów rozwoju produktu. Dostępność produktów będzie jednak zależała od planów badawczo-rozwojowych różnych producentów, ale producenci nie wdrożyli jeszcze produktu, a jego wykorzystanie jest powolne. Na konferencjach TETRA wyrażono opinię, że najwcześniejsze wdrożenie szerokopasmowej sieci TETRA (lub jej odpowiednika) nastąpi prawdopodobnie w 2020 r. Dzieje się tak, ponieważ istniejącej sieci nie można zmodernizować do obsługi TETRA 2 ze względu na problemy z dostępnością widma; a niektóre z nich mogą nie zostać zrealizowane ze względu na związane z tym

koszty. Dlatego istnieje zapotrzebowanie na ulepszony system komunikacji PPDR, który byłby wysoce wydajny, bezpieczny, odporny i elastyczny w nowoczesnych i wyrafinowanych zastosowaniach; oraz że nawet jeśli wprowadzenie TETRA 2 i przyszłych wersji (szerokopasmowa TETRA) ugruntuje się, będzie gwarancja, że wykorzystanie sieci pod względem gospodarczym i komercyjnym będzie uzasadnione. Istnieją jednak problemy z upowszechnieniem sieci, które będą miały wpływ na przyszłe sieci; i wynikają one z wad obecnej sieci TETRA.

AKTUALNE TRENDY TECHNOLOGII PPDR (czyli TETRA).

Większość organizacji PPDR w Europie wykorzystuje obecnie do komunikacji dedykowane sieci PMR, zaprojektowane specjalnie pod kątem ich potrzeb. Typowo TETRA (lub TETRAPOL) i pracujący w paśmie widma 380-400 MHz. Sieci te oferują szereg usług transmisji danych o niskiej szybkości, ale dostępna prędkość i pojemność ograniczają szersze wykorzystanie aplikacji wymagających szybszej transmisji danych. Zgodnie z tendencjami społecznymi w zakresie dostępu do informacji w drodze, operacje PPDR w coraz większym stopniu opierają się na informacjach, co wymaga dostępu do szerszego zakresu łączy szerokopasmowych i zastosowań szerokopasmowych. Biorąc pod uwagę ograniczenia w możliwościach istniejących sieci dedykowanych do świadczenia mobilnych usług szerokopasmowych, uważa się za prawdopodobne, że w ciągu najbliższych 5–10 lat w całej Europie będzie wymagana nowa generacja rozwiązań, które również spełnią przyszłe wymagania PPDR. Rozwiązania te, jeśli będą dostarczane przy użyciu nowych, dedykowanych mobilnych sieci szerokopasmowych zaprojektowanych tak, aby spełniały wymogi PPDR, w dalszym ciągu będą wymagały dodatkowego widma, aby skutecznie świadczyć wymagane usługi. Powyżej podkreślono trend w zakresie obecnych i przyszłych mobilnych aplikacji do transmisji danych i multimediów PPDR, który ma zaspokoić szereg potrzeb. Oprócz tego istnieje szereg specyficznych wymagań operacyjnych, które są niezbędne dla komunikacji PPDR w celu zapewnienia dostępności, niezawodności i integralności sieci, które obejmują: Wysoki poziom dostępności sieci; Wysoki stopień kontroli sieci (wdrożenie priorytetowego dostępu dla określonych grup użytkowników lub osób i rezerwacja przepustowości tam, gdzie jest to wymagane); Blisko ogólnokrajowego zasięgu geograficznego (komunikacja w odległych obszarach); Bezpieczeństwo; Niskie opóźnienia (kompleksowe opóźnienie głosu nie większe niż 200 ms); interoperacyjność między różnymi organami PPDR i transgraniczność; Sieci o dużej odporności (różne warstwy redundancji); oraz Możliwość obsługi ruchu mieszanego. W sektorze PPDR powyższe zapotrzebowanie na dostęp do szerszego zakresu aplikacji i usług wynika ze zmian w praktykach pracy, co stwarza wymagania w zakresie dostępu do znacznie szerszego zakresu źródeł danych (tekstowych, graficznych i wideo), które są typowe w komercyjnych sieciach komórkowych. Udostępnianie tych danych wykorzystywane jest w celu ustalenia i utrzymania wspólnego obrazu operacyjnego pomiędzy agencjami PPDR oraz pomiędzy dowództwem terenowym i centralnym. Służy to poprawie responsywności, wspomaganiu rozmieszczenia zasobów oraz poprawie terminowości i podejmowania decyzji w codziennych operacjach PPDR; podczas reagowania na ważne zaplanowane i nieplanowane zdarzenia. Ponieważ istnieją ograniczenia w zakresie i objętości danych i aplikacji multimedialnych, jakie mogą zapewnić istniejące (i być może przyszłe) dedykowane sieci wąskopasmowe i szerokopasmowe (oraz istniejące sieci komercyjne), w przypadku niedostępności sieci PPDR nowej generacji niektóre z przewidywane wnioski nie zostaną dostarczone. Docelowo będzie to miało wpływ na to, jak mogą ewoluować już pojawiające się zmiany w sposobach pracy w sektorze PPDR, a w dłuższej perspektywie ograniczą dalszy rozwój sektora.

BARIERY I ZAGADNIENIA TECHNOLOGICZNE I EKONOMICZNE

Możliwości istniejących (i być może przyszłych) wąskopasmowych i szerokopasmowych dedykowanych sieci mobilnych stosowanych obecnie w sektorze PPDR nie będą wystarczające, aby sprostać przewidywanym przyszłym wymaganiom. Jest to nieuniknione, chyba że zostanie wprowadzone

podejście oparte na stałym rozwoju, w którym metody działania PPDR będą się stopniowo zmieniać, głos pozostanie dominującą metodą komunikacji o znaczeniu krytycznym, a istniejące aplikacje do transmisji danych będą nadal używane obok głosu (przy stopniowym wzroście wykorzystania). Nie jest to jednak odpowiednie w dłuższej perspektywie, ponieważ istnieje już coraz więcej dowodów na zmiany w metodach pracy i tendencje w sektorze PPDR, które sugerują, że ścieżka ta nie będzie odpowiadać przyszłym wymaganiom. Aby obsłużyć szereg przyszłych aplikacji do przesyłania danych, obrazów i multimediów, których oczekują użytkownicy PPDR, wymagana jest nowa generacja mobilnych usług szerokopasmowych. Opcje świadczenia tej nowej generacji usług obejmują wykorzystanie zmodernizowanych sieci komercyjnych lub opracowanie nowej generacji dedykowanych mobilnych sieci szerokopasmowych do wyłącznego użytku w zakresie bezpieczeństwa publicznego. Chociaż usługi transmisji danych nowej generacji mogłyby teoretycznie być świadczone poprzez modernizację i przeprojektowanie sieci komercyjnych, istnieją pewne bariery, począwszy od względów technicznych, po koszty i względy handlowe, które mogą utrudniać osiągnięcie tego w praktyce. Należą do nich:

• Sektor PPDR wymaga bardzo szerokiego zasięgu geograficznego oraz głębokiej penetracji zasięgiem wewnątrz budynków, niezależnie od lokalizacji, co nie odpowiada typowym wymaganiom wdrożeniowym sieci komercyjnej. Operatorzy komercyjni zazwyczaj inwestują w zasięg tam, gdzie istnieje duża liczba ludności, a przepustowość projektuje się w taki sposób, aby zmaksymalizować generowanie przychodów na tych obszarach, przy niewielkiej motywacji do inwestowania na obszarach o małej gęstości zaludnienia.

• Przeprojektowanie sieci komercyjnych w celu spełnienia wszystkich wymagań operacyjnych sektora bezpieczeństwa publicznego będzie prawdopodobnie bardzo kosztowne, w związku z czym pojawiają się pytania, czy operatorzy komercyjni mają do tego wystarczające zachęty. Na przykład typowe wymagania obejmują konieczność zapewnienia zasilania awaryjnego baterią w tysiącach stacji bazowych w całej sieci oraz konieczność zaprojektowania sieci w sposób zapewniający ich wysoką odporność (w tym możliwość nakładania się zasięgu, zasilacze rezerwowe i miejsca rezerwowe) oraz że nie istnieje żaden pojedynczy „punkt awarii" ani w sieciach dostępowych, ani szkieletowych.

• Istnieje pogląd, że sieci komercyjne mogą być bardziej podatne na sabotaż ze strony przestępców niż sieci dedykowane.

• Pojawiają się pytania, czy wymagany poziom usług dla zastosowań PPDR może być zagwarantowany w sieci współdzielonej z użytkownikami komercyjnymi, szczególnie w okresach bardzo dużego obciążenia ruchem; oraz czy niektóre wymagania PPDR są faktycznie osiągalne w tej sieci.

• Istnieją sprzeczne poglądy na temat możliwości szyfrowania sygnalizacji poprzez interfejs radiowy w sieci 3G/LTE.

• Zapewnienie szczególnych wymagań dotyczących przewozu dokumentów „zastrzeżonych" lub „poufnych" wymaga starannego planowania sieci i zatwierdzeń, co jest skomplikowane i kosztowne w realizacji.

• Nie jest jasne, czy sieci można wymiarować tak, aby osiągnąć wymaganą bezpośredniość i gwarantowany dostęp, jakiego wymaga PPDR.

• Organy publiczne niechętnie polegają na operatorach w pełni komercyjnych ze względu na potencjalny brak kontroli nad przyszłymi inwestycjami sieciowymi, planami biznesowymi i finansowaniem.

Jednakże, jak wyjaśniono wcześniej, obecna (i prawdopodobnie przyszła) dedykowana sieć PMR (TETRA) nie byłaby w stanie sprostać trendowi w zakresie obecnych i przyszłych mobilnych aplikacji do szybkiego przesyłania danych i multimediów PPDR, który ma obejmować szereg wymagania.

POSTĘP WYZACZĄCY NOWOCZESNY KRAJOBRAZ ARCHITEKTURY SIECI KOMUNIKACYJNEJ PPDR

Organizacje PPDR korzystają obecnie z szeregu różnych sieci komunikacyjnych, aby zaspokoić swoje potrzeby operacyjne. W Europie większość ich personelu korzysta obecnie z dedykowanych sieci do świadczenia wąskopasmowej komunikacji mobilnej z wykorzystaniem technologii TETRA lub TETRAPOL działających w paśmie 380-400 MHz i. Ten przydział widma opiera się na harmonizacji widma dla bezpieczeństwa publicznego, wprowadzonej przez ECC w 1996 r. i zawiera zalecenia dotyczące harmonizacji dodatkowych pasm częstotliwości dla cyfrowego PPDR w zakresie 380–470 MHz. Istnieją istotne bariery we wdrożeniu tej decyzji, ponieważ to samo widmo jest przeznaczone również dla wąskopasmowej i szerokopasmowej cyfrowej lądowej łączności ruchomej (PMR/PAMR). W blisko 20 krajach obecność sieci CDMA 450 będzie miała wpływ na dostępność tego widma dla organizacji PPDR. Zainteresowanie pojawia się także komercyjne wdrożenie technologii LTE w tym paśmie. W ostatnich latach można było zaobserwować coraz szybszy postęp w zakresie możliwości technologii stosowanych w sektorze komercyjnej łączności elektronicznej, szczególnie w odniesieniu do szybkości transmisji danych drogą bezprzewodową i możliwej do osiągnięcia wydajności widma. Na przykład, kiedy w 1999 r. uzgodniono pierwsze standardy technologii 3G, maksymalna przepływność możliwa do uzyskania w sieci komórkowej 3G wynosiła 2 Mb/s, chociaż w praktyce większość użytkowników doświadczała prędkości w zakresie 64–384 kb/s. Dla porównania, technologia cyfrowa stosowana głównie w sektorze PPDR (TETRA) może zapewnić prędkość do 28 kb/s. Wiele współczesnych sieci 3G zostało zmodernizowanych do najnowszej technologii szybkiego dostępu pakietowego (HSPA, HSPA+) i teoretycznie może osiągać szczytową przepływność do 21 Mb/s (tylko jeden użytkownik na komórkę, w najlepszym wypadku kanał, bez zabezpieczenia przed błędami), przy czym w rzeczywistości przepływność użytkownika wynosząca 1 Mb/s lub więcej w przypadku kilku użytkowników jest stosunkowo powszechna w niektórych sieciach w obszarach o dużym natężeniu ruchu, przy wykorzystaniu kanału o szerokości pasma 5 MHz. Nowsze systemy wykorzystujące takie standardy jak komponent TETRA Release 2 TEDS są w stanie obsługiwać bardziej zaawansowaną transmisję danych z teoretyczną maksymalną przepustowością IP do 500 kbps w kanale 150 kHz; jednakże istnieje coraz większa przepaść między możliwościami sieci komercyjnych a dedykowanymi sieciami PPDR, ponieważ rosnące zapotrzebowanie na obsługę danych szerokopasmowych wymaga szybszego opracowywania i wdrażania bardziej wydajnych technologii w sektorze komercyjnym. Pomimo poprawy efektywności widmowej poprzez wdrożenie nowych technologii, które w pewnym stopniu zmniejszą niedobory widma, wzrost popytu na częstotliwości prawdopodobnie przewyższy wzrost podaży w dającej się przewidzieć przyszłości. Widmo dostępne dla istniejących operacji PPDR nie zaspokoi przyszłego zapotrzebowania na te podstawowe usługi. Jednym z przykładów jest obecna sytuacja z TETRA TEDS, w której nie wszystkie państwa członkowskie UE są w stanie zidentyfikować kanały radiowe. Dlatego polityka komunikacyjna musi ewoluować, aby wzmocnić nowe systemy poprzez realokację widma z dywidendy cyfrowej na komunikację o znaczeniu krytycznym PPDR. Decyzji tej nie należy podejmować lekko, ponieważ leży ona na ścieżce krytycznej dla wielu innych decyzji niezbędnych przed wdrożeniem sieci PPDR nowej generacji. Historycznie rzecz biorąc, powszechną praktyką było identyfikowanie odpowiedniego widma z dużym wyprzedzeniem ze względu na ramy czasowe dotyczące uwolnienia widma, opracowania norm i sprzętu. Planowanie i wdrażanie takich sieci może zająć nawet 10 lat. Pilność tej sprawy zwiększa zapotrzebowanie na pojawienie się nowych usług w związku ze wzrostem zagrożeń terrorystycznych, częstotliwością naturalnych katastrof ekologicznych i normalnym wzrostem liczby ludności. Pasmo 450–470 MHz jest również szeroko wykorzystywane w Europie przez analogowe prywatne usługi radiowe, które w niektórych przypadkach (zwłaszcza w Wielkiej Brytanii i

Irlandii) nie są zgodne z odpowiednimi zaleceniami CEPT i wydaje się mało prawdopodobne, aby możliwe było zapewnienie wystarczającego zharmonizowanego widma do obsługi szerokopasmowego internetu mobilnego udostępnione w rozsądnych ramach czasowych. W praktyce wielu użytkowników PPDR korzysta już z komercyjnych sieci 3G obok własnych sieci dedykowanych; jednakże zasięg sieci komercyjnych jest gorszy, głównie ze względów komercyjnych, częściowo ze względu na stosowane wyższe częstotliwości i odpowiadające im mniejsze rozmiary komórek. Co więcej, sieci prawdopodobnie będą doświadczać ograniczeń przepustowości w okresach dużego zapotrzebowania, co zwykle ma miejsce w następstwie poważnych incydentów związanych z bezpieczeństwem publicznym. Rozszerzenie możliwości oferowanych przez komercyjne technologie mobilnego Internetu szerokopasmowego, takie jak HSPA, LTE, CDMA 2000 EV-DO i WiMAX, na sektor PPDR mogłoby przynieść znaczne korzyści. Przyjęcie takich standardów w ramach dedykowanego widma PPDR przezwyciężyłoby ograniczenia przepustowości sieci komercyjnych, a także umożliwiłoby interoperacyjność z sieciami publicznymi, co mogłoby ułatwić komunikację między agencjami. Takie podejście mogłoby również zapewnić korzyści skali w przypadku, gdyby od standardowych sieci komercyjnych różniły się jedynie modułami RF. Technologie takie doskonale wpasowałyby się w przyszłe trendy aplikacyjne omówione wcześniej.

NOWOCZESNY STANDARD KOMUNIKACJI MOBILNEJ

Ogólne standardy PMR Profesjonalne radio mobilne (znane również jako Private Mobile Radio [PMR] w Wielkiej Brytanii i Land Mobile Radio [LMR] w Ameryce Północnej) to polowe systemy komunikacji radiowej, które wykorzystują radiotelefony przenośne, mobilne, stacje bazowe i konsole dyspozytorskie i są w oparciu o standardy takie jak MPT-1327, TETRA, TETRAPOL i APCO 25, które są przeznaczone dla organizacji dedykowanych. Typowymi przykładami są systemy radiowe używane przez policję i straż pożarną. Kluczowe cechy profesjonalnych mobilnych systemów radiowych mogą obejmować: Łączność punkt-wielopunkt (w przeciwieństwie do telefonów komórkowych, które służą do komunikacji punkt-punkt); Naciśnij i mów, zwolnij, aby słuchać (jedno naciśnięcie przycisku otwiera komunikację na kanale częstotliwości radiowej); szybkie zestawienie połączenia; duże obszary zasięgu; zamknięte grupy użytkowników; Wykorzystanie pasm częstotliwości VHF lub UHF. Najważniejszym czynnikiem skutecznego i pomyślnego rozmieszczenia agentów PPDR jest bezpieczna i niezawodna komunikacja. W sytuacji awaryjnej niezawodność systemu komunikacji może zadecydować o życiu lub śmierci człowieka. Przydatność profesjonalnych sieci radiotelefonicznych nie powinna jednak ograniczać się do komunikacji głosowej, ale do możliwości bezpiecznego i terminowego przesyłania wrażliwych danych i informacji. Możliwość zintegrowania większej liczby czujników (w celu umożliwienia dostępu do większej liczby krytycznych danych z dużą szybkością) w terminalach PMR byłaby bardzo korzystna w przypadku reagowania kryzysowego i działań zapobiegawczych.

TETRAPOL

TETRAPOL to cyfrowy standard profesjonalnego radia mobilnego, zgodnie z definicją zawartą w Publicznie Dostępnej Specyfikacji Tetrapol (PAS), używany przez profesjonalne grupy użytkowników, takie jak organizacje bezpieczeństwa publicznego, wojsko, przemysł i transport na całym świecie. TETRAPOL to w pełni cyfrowy system profesjonalnej radiotelefonii mobilnej FDMA dla zamkniętych grup użytkowników, standaryzujący całą sieć radiową od terminali danych i głosu, poprzez stacje bazowe, po urządzenia przełączające, łącznie z interfejsami do publicznej komutowanej sieci telefonicznej i sieci danych. Szyfrowanie typu end-to-end jest integralną częścią standardu, podobnie jak w TETRA. Matra/EADS opracowała TETRAPOL i już na wczesnym etapie dostarczyła działający cyfrowy system łączności trankingowej. Jednym z pierwszych użytkowników systemu RUBIS była francuska żandarmeria Nationale w 1988 roku. EADS (Connexity) i Siemens (S-PRO) należą do czołowych producentów profesjonalnych systemów radiowych opartych na specyfikacji TETRAPOL.

TETRA jest jednak standardem nowszym niż TETRAPOL, a w Europie obserwuje się bardzo znaczący trend w kierunku standardów TETRA ze względu na trwałość i możliwości ewolucyjne standardu TETRA po przejściu z TETRA 1 do TETRA 2 i mający potencjał ewoluować w stronę bardziej udoskonalonej funkcjonalności i funkcji (podobnie jak w przypadku sieci GSM).

GSM

Globalny system komunikacji mobilnej (GSM) to akceptowany na całym świecie standard cyfrowej komunikacji komórkowej. GSM to nazwa grupy normalizacyjnej utworzonej w 1982 r. w celu stworzenia wspólnego europejskiego standardu telefonii komórkowej, który określałby specyfikacje dla paneuropejskiego mobilnego systemu radiowego działającego na częstotliwości 900 MHz. GSM jest siecią komórkową, co oznacza, że telefony komórkowe łączą się z nią wyszukując komórki znajdujące się w bezpośrednim sąsiedztwie. Jednak GSM został zaprojektowany z umiarkowanym poziomem bezpieczeństwa. Komunikacja pomiędzy abonentem a stacją bazową może być szyfrowana. Ze względów bezpieczeństwa GSM wykorzystuje kilka algorytmów kryptograficznych. Szyfry strumieniowe A5/1 i A5/2 służą do zapewnienia prywatności głosu w trybie bezprzewodowym. A5/1 został opracowany jako pierwszy i jest silniejszym algorytmem używanym w Europie i Stanach Zjednoczonych; A5/2 jest słabszy i używany w innych krajach. W obu algorytmach wykryto poważne słabości: możliwe jest złamanie szyfru A5/2 w czasie rzeczywistym ataku tekstowego, a w lutym 2008 roku firma Pico Computing, Inc. ujawniła swoje możliwości i plany komercjalizacji układów FPGA, które umożliwiają złamanie A5/1 za pomocą ataku Rainbow Table. System obsługuje wiele algorytmów, dzięki czemu operatorzy mogą zastąpić dany szyfr silniejszym.

TETRA

Standard TETRA (pierwotnie przeznaczony na rynek europejski) stał się obecnie standardem globalnym z potencjalnym rynkiem światowym. TETRA jest często używana obok ustalonych pasm częstotliwości o różnych standardach. Zwykle pasma częstotliwości TETRA sąsiadują z ważnymi pasmami komunikacyjnymi, więc nie mogą w żaden sposób zakłócać ustalonych sąsiednich kanałów. Zatem transmisja sygnałów TETRA musi charakteryzować się bardzo niskimi sygnałami pozapasmowymi i mocą wyjściową o częstotliwości fałszywej. Odbiór sygnałów TETRA może odbywać się praktycznie w dowolnym środowisku widmowym, dlatego odbiorniki radiowe TETRA wymagają wysokich specyfikacji blokowania i liniowości. TETRA wykorzystuje modulację o niestałej obwiedni, która wymaga wysoce liniowego nadajnika, aby zapobiec wysokiemu poziomowi zakłóceń sąsiednich kanałów (ACI) w wyniku ponownego wzrostu widma. Liniowe wzmacniacze mocy (PA) mają zazwyczaj niską wydajność, co jest niepożądane w komunikacji mobilnej, ponieważ wydajność PA jest jednym z najważniejszych parametrów w systemie określającym czas rozmów, rozmiar baterii itp. Konwencjonalne podejście do osiągnięcia niskich zniekształceń polega na używać wzmacniaczy mocy pracujących na poziomie wyjściowym znacznie poniżej ich rzeczywistych możliwości (podejście back-off). Jednak takie podejście drastycznie zmniejsza efektywność energetyczną, zwiększając pobór mocy systemu do niedopuszczalnego poziomu. Zahamowało to wzrost liczby użytkowników. Ważną zaletą standardu TETRA jest jednak to, że posiada on szereg specyfikacji otwartego interfejsu, z których twórcy aplikacji mogą korzystać w celu dalszego zwiększania możliwości TETRA. Chociaż TETRA wykorzystuje wiele zasad GSM, TETRA została specjalnie zaprojektowana, aby umożliwić komunikację służb ratowniczych (policji, straży pożarnej, pogotowia ratunkowego itp.), ponieważ ma inne funkcje niż GSM i przez GSM, w tym:

• Komunikacja grupowa — zdolność jednej osoby do komunikowania się z dużą liczbą innych agentów w trybie działania typu walkie-talkie.

• Bardzo krótki czas nawiązywania połączeń, zapewniający szybkie nawiązanie krytycznej komunikacji.

• Techniki zarządzania priorytetami/przeciążeniami zapewniające, że w okresach przeciążenia może nastąpić ważna (potencjalnie zagrażająca życiu) komunikacja.

• Bezpieczeństwo komunikacji. W normie uwzględniono szereg technik, a na sposób projektowania produktów nałożono ograniczenia, aby zapewnić, że komunikacja nie może zostać „podsłuchiwana" i manipulowana przy jednostkach.

• Niezawodność — dzięki różnym poziomom usług i sposobowi instalacji infrastruktury sieci TETRA są bardziej odporne w sytuacjach awaryjnych niż komercyjne nośniki komunikacji.

TETRA jest wyraźnym zwycięzcą komercyjnej bitwy o technologię komunikacyjną w sektorze PPDR. Aby jednak TETRA mogła w pełni wykorzystać swój potencjał i aby możliwe było osiągnięcie zaawansowanych usług przewidzianych w sieci komunikacyjnej PPDR nowej generacji, niezbędny jest znaczny rozwój. Pomimo zalet TETRA istnieje szereg problemów, które uniemożliwiają szersze zastosowanie TETRA. Należą do nich: Koszt produktu; Rozmiar produktu; Możliwości danych produktów. Kierują się one wymagającymi wymaganiami dotyczącymi protokołu, wydajności i bezpieczeństwa, które różnią się od komercyjnych sieci komórkowych. Te aspekty z kolei uniemożliwiają zarówno pełną integrację personelu ratunkowego przy użyciu bezpiecznego systemu komunikacji, jak i nieprzekazywanie krytycznych/przydatnych danych za pośrednictwem bezpiecznych i gwarantowanych nośników komunikacji. Udoskonalanie technologii wykorzystywanej przez służby ratownicze w Europie, a w szczególności TETRA, poprawi jakość usług i stosunek jakości do ceny.

PROPONOWANE ROZWIĄZANIA ARCHITEKTONICZNE SIECI KOMUNIKACYJNEJ PPDR TETRA W MOBILNEJ SIECI IP

Wielotechnologiczna komunikacyjna mobilna bramka IP (MIPGATE) W ostatniej dekadzie poczyniono intensywne prace badawcze nad rozwojem i integracją nowych technologii bezprzewodowego dostępu do mobilnego dostępu do Internetu. Wśród głównych koncepcji badawczych dotyczących wykorzystania dostępności różnych heterogenicznych technologii sieciowych w centrum uwagi znajdują się koncepcje Always Best Connected (ABC), Quality of Experience (QoE) i Bandwidth Aggregation. Always Best Connected oznacza, że użytkownicy końcowi oczekują możliwości łączenia się w dowolnym miejscu i czasie – także będąc w ruchu – za pomocą wybranego przez siebie terminala. Użytkownicy końcowi oczekują również możliwości określenia w każdej sytuacji, czy „najlepszy" jest definiowany na podstawie ceny czy możliwości. Jednakże obecne, najnowocześniejsze rozwiązania, takie jak IETF Mobile IPv6 (MIP) czy powstający protokół Host Identity Protocol (HIP), skupiają się głównie na zarządzaniu mobilnością, zamiast uwzględniać dodatkowe kwestie związane z użytkownikiem, takie jak preferencje użytkownika , powiązane koszty, reputacja operatora sieci dostępowej oraz zaufanie i głównie kwestie związane z aplikacjami, takie jak (jakość usług) QoS i odzyskiwanie po awarii w połączeniu z mobilnością. Jakość doświadczenia (QoE) odzwierciedla zbiorowy efekt świadczenia usług, który określa stopień zadowolenia użytkownika końcowego, np. to, co użytkownik naprawdę postrzega pod względem użyteczności, dostępności, możliwości utrzymania i integralności usługi. Jak dotąd bezproblemowa komunikacja opiera się głównie na technicznych parametrach QoS sieci, ale do połączenia pomiędzy QoS i QoE potrzebny jest prawdziwy obraz QoS przez użytkownika końcowego. Chociaż istniejące specyfikacje 3GPP lub IETF opisują procedury negocjacji QoS, sygnalizacji i rezerwacji zasobów dla aplikacji multimedialnych (takich jak komunikacja audio/wideo i wiadomości multimedialne, obsługa bardziej zaawansowanych usług, obejmujących aplikacje interaktywne z różnorodnymi i współzależnymi komponentami medialnymi) nie są szczegółowo omówione . Dodatkowo, choć parametry QoS wymagane przez aplikacje multimedialne są dobrze znane, nie ma standardowej specyfikacji QoS umożliwiającej wdrożenie podstawowych mechanizmów zgodnie z potrzebami QoS aplikacji. Jedną z pierwszych prób zapewnienia architektury

opartej wyłącznie na protokole IP i zintegrowania różnych technologii dostępu do komunikacji w zakresie bezpieczeństwa publicznego był projekt MESA (Mobility for Emergency and Safety Applications), międzynarodowy projekt partnerski ETSI i TIA, którego początki sięgają 2000 r. (Projekt MESA, 2001). Salkintzis (2002) zaproponował rozwiązanie integracji sieci WLAN i TETRA, które pasuje do architektury all-IP MESA i umożliwia terminalom TETRA łączenie infrastruktury TETRA za pośrednictwem szerokopasmowej radiowej sieci dostępowej WLAN zamiast konwencjonalnej wąskopasmowej sieci radiowej TETRA, pozostając jednocześnie w pełni interoperacyjny z konwencjonalnymi terminalami i usługami TETRA. Chiti i inni proponują sieć bezprzewodową, której celem jest połączenie kilku heterogenicznych systemów i zapewnienie dostępu multimedialnego grupom ludzi w celu zarządzania katastrofami. Autorzy poruszają zagadnienia heterogenicznego powiązania sieci, pełnego i odpornego na awarie pokrycia obszaru katastrofy, lokalizacji umożliwiającej efektywną koordynację działań ratowniczych oraz bezpieczeństwa. Prace skupiają się na wykorzystaniu sieci bezprzewodowej opartej na WiMAX jako szkieletu zapewniającego operatorom niezawodną i bezpieczną komunikację multimedialną podczas zarządzania kryzysowego. Durantini i inni przedstawiają rozwiązanie zapewniające interoperacyjność i integrację systemów profesjonalnej łączności radiowej (TETRA i Simulcast), systemów publicznych (GSM/GPRS/UMTS) i szerokopasmowych technologii bezprzewodowych, takich jak WiMAX, w celu umożliwienia rozproszonego świadczenia usług przy jednoczesnym zapewnieniu zawsze najlepsze połączenie z aplikacjami wymagającymi dużej przepustowości, zapewnianymi przez sieć szkieletową opartą na protokole IP. Ponadto autorzy poruszają kwestię optymalizacji jakości zarządzania usługami w środowisku wielosieciowym oraz proponują mapowanie QoS pomiędzy klasami WiMAX QoS a typolo usługi TETRA Istnieje wiele innych podobnych prac skupiających się na integracji różnych technologii sieciowych w zakresie komunikacji związanej z bezpieczeństwem publicznym i poza nim. Jednakże dostępne dotychczas rozwiązania są fragmentaryczne i każde z nich uwzględnia jedynie podzbiór idealnego, autonomicznego rozwiązania w zakresie łączności, obsługującego QoE, które może jednocześnie wykorzystywać wszystkie dostępne interfejsy sieciowe. W przypadku sytuacji awaryjnych i katastrof na dużą skalę kluczowe znaczenie ma agregacja ograniczonych zasobów komunikacyjnych wielu technologii i możliwość jednoczesnego korzystania z nich, ponieważ pozostała przepustowość pojedynczej technologii może ucierpieć z powodu uszkodzeń infrastruktury.

Wielościeżkowy TCP

Protokół kontroli transmisji (TCP), będący podstawą transportu danych wielu współczesnych usług telekomunikacyjnych, został zaprojektowany do pracy na pojedynczych łączach i nie radzi sobie dobrze z jednoczesnym wykorzystaniem wielu łączy w tym samym czasie. Badanie wydajności protokołu TCP w sieciach heterogenicznych ukazuje istniejące rozwiązania i związane z nimi problemy. Magalhaes i inni przedstawiają rozwiązanie do agregacji kanałów w warstwie transportowej, zwane R-MTP (Reliable Multiplexing Transport Protocol), które multipleksuje dane z pojedynczego strumienia danych aplikacji przez wiele interfejsów sieciowych. W ramach niedawno zakończonego projektu Trilogy finansowanego przez UE wprowadzono rozwiązanie MultiPath TCP (MPTCP), aby umożliwić jednoczesne korzystanie z kilku ścieżek poprzez modyfikację protokołu TCP, która przedstawia aplikacjom normalny interfejs TCP, jednocześnie rozkładając dane na kilka podprzepływów (Barré, 2011). . Utworzono grupę roboczą IETF w celu opracowania protokołu MPTCP, co stanowi ciągły wysiłek. Jednak w wyniku szeroko zakrojonych badań oceniających MPTCP niektórzy autorzy (Nguyen, 2011) podają, że heterogeniczne środowisko sieciowe (Ethernet, Wi-Fi i 3G) ma ogromny wpływ na przepustowość MPTCP i ujawnia potrzebę inteligentnego algorytmu wyboru interfejsu w MPTCP.

Bezpieczeństwo

Terrestrial Trunked Radio (TETRA) obsługuje dwa rodzaje zabezpieczeń: bezpieczeństwo interfejsu radiowego i bezpieczeństwo typu end-to-end. Bezpieczeństwo interfejsu radiowego (TETRA, 2010) chroni tożsamość użytkownika, sygnalizację, głos i dane między stacją mobilną (MS) a stacją bazową (BS). Określa szyfrowanie interfejsu radiowego, (wzajemne) uwierzytelnianie, zarządzanie kluczami (OTAR: ponowne kluczowanie bezprzewodowe) oraz włączanie/wyłączanie funkcjonalności. Kompleksowe bezpieczeństwo (TETRA, 2010) szyfruje głos z MS na MS. Obecnymi kandydatami na algorytmy szyfrowania są IDEA (własność MediaCrypt AG) i AES jako schematy szyfrowania. Jednym z głównych wyzwań komunikacji wielotechnologicznej jest problem kompatybilności pomiędzy mechanizmami bezpieczeństwa (szyfrowanie, uwierzytelnianie, integralność i zarządzanie kluczami) obsługiwanymi przez te technologie. Bezprzewodowa sieć LAN obsługuje różne mechanizmy bezpieczeństwa, których użycie jest w większości opcjonalne. Filtrowanie adresów MAC i identyfikator zestawu usług ukrytych (SSID) to najprostsze techniki. Obecnie bardzo niewiele punktów dostępu korzysta z protokołu WEP (Wired Equivalent Privacy), ponieważ wiele narzędzi do łamania zabezpieczeń jest publicznie dostępnych w Internecie. Aby rozwiązać ten problem, wprowadzono funkcję Wi-Fi Protected Access (WPA i WPA2 oparte na standardzie 802.11i), ale słabe hasła nadal stanowią problem. Standard 802.1x definiuje hermetyzację protokołu Extensible Authentication Protocol (EAP) i umożliwia uwierzytelnianie za pośrednictwem serwerów uwierzytelniających innych firm, takich jak Radius i Diameter. Kompleksowe bezpieczeństwo można zapewnić poprzez wykorzystanie protokołu Internet Protocol Security (IPSEC), Transport Layer Security (TLS), Secure Sockets Layer (SSL), Secure Shell (SSH), całkiem dobrej prywatności (PGP) itp. W sieciach GSM i 3G występują podobne problemy ze zgodnością z TETRA. Bezpieczeństwo GSM definiuje moduł identyfikacji abonenta (SIM), MS i sieć GSM. Hosty SIM subskrybują klucz uwierzytelniający (K), osobisty numer identyfikacyjny (PIN), algorytm generowania klucza (A8) i algorytm uwierzytelniania (A3). MS zawiera algorytm szyfrowania (A5) dla interfejsu radiowego. Szyfrowanie jest zapewnione tylko dla interfejsu radiowego. Bezpieczeństwo 3G opiera się na bezpieczeństwie GSM. Eliminuje słabe strony systemów 2G poprzez integralność i ulepszone uwierzytelnianie, a także ulepszone szyfrowanie przy użyciu dłuższych kluczy i silniejszych algorytmów. Projekt „Bezproblemowa komunikacja w zarządzaniu kryzysowym" (SECRICOM – 7PR) częściowo odpowiada na to wyzwanie w zakresie bezpiecznych systemów „naciśnij i mów" w ramach istniejącej infrastruktury (sieci GSM, UMTS). Kolejnym wyzwaniem w komunikacji wielotechnologicznej jest to, że większość mechanizmów bezpieczeństwa jest opcjonalna i są one utrzymywane w oparciu o polityki różnych domen administracyjnych. Połączenie typu end-to-end między dwoma komputerami PC może przebiegać przez niezabezpieczoną sieć publiczną, co może umożliwiać różnorodne ataki, w tym typu „odmowa usługi" i „man-in-the-middle". Koszt łagodzenia tych ataków po stronie MS może być wyższy niż korzyści z połączenia pod względem wskaźników jakości usług (QoS) i jakości doświadczenia (QoE). Dlatego mechanizmy QoS i QoE muszą obejmować powiązane metryki, aby zapewnić użytkownikom końcowym przewidywalny poziom usług bezpieczeństwa.

TETRA W MOBILNEJ SIECI AD-HOC

Mobilne sieci ad-hoc to sieci wieloprzeskokowe, w których węzły mogą być stacjonarne lub mobilne; i powstają one dynamicznie. Pozwalają ludziom efektywnie wykonywać zadania, oferując niespotykany dotąd poziom dostępu do informacji. W mobilnych sieciach ad hoc topologia jest wysoce dynamiczna i losowa; ponadto ważną rolę odgrywa rozmieszczenie węzłów i ich zdolność do samoorganizacji. Ich główne cechy można podsumować w następujący sposób: Topologia jest bardzo dynamiczna i częste zmiany w topologii mogą być trudne do przewidzenia; Mobilne sieci adhoc opierają się na łączach bezprzewodowych, które w dalszym ciągu będą miały znacznie mniejszą przepustowość niż ich przewodowe odpowiedniki; Bezpieczeństwo fizyczne jest ograniczone ze względu na transmisję bezprzewodową; Mobilne sieci ad hoc charakteryzują się wyższymi współczynnikami strat i mogą

powodować większe opóźnienia i wahania niż sieci stacjonarne ze względu na transmisję bezprzewodową; oraz Węzły mobilnej sieci ad hoc wykorzystują baterie lub inne wyczerpujące się źródła energii. W rezultacie oszczędność energii jest ważnym kryterium projektowania systemu. Co więcej, węzły muszą być świadome zużycia energii: zestaw funkcji oferowanych przez węzeł zależy od jego dostępnej mocy (procesor, pamięć itp.). Dobrze zaprojektowana architektura mobilnych sieci ad hoc obejmuje wszystkie warstwy sieciowe, począwszy od warstwy fizycznej po warstwę aplikacji. Zarządzanie energią ma ogromne znaczenie; należy uwzględnić ogólne strategie oszczędzania energii, a także dostosować do specyfiki węzłów ogólnych metod kodowania kanałów i źródeł, zarządzania zasobami radiowymi i wielokrotnym dostępem. W mobilnych sieciach ad hoc, charakteryzujących się całkowitą niezależnością od wszelkich organów i infrastruktury, kryje się ogromny potencjał dla użytkowników. W rzeczywistości, z grubsza rzecz biorąc, dwóch lub więcej użytkowników może stać się siecią mobilną ad hoc, po prostu znajdując się wystarczająco blisko, aby spełnić ograniczenia radiowe, bez żadnej interwencji zewnętrznej. Problemy z routingiem rozwiązano w drodze badań; gdzie protokoły routingu między dowolną parą węzłów w sieci ad hoc mogą być trudne, ponieważ węzły mogą przemieszczać się losowo, a także przyłączać się do sieci lub ją opuszczać. Oznacza to, że optymalna trasa w określonym momencie może nie działać kilka sekund później. Dwa z najlepszych protokołów multiemisji, jakie można zastosować, to MAODV (protokół routingu wektorów odległości na żądanie Adhoc Multicast) i ODMRP (protokół routingu multiemisji na żądanie). Ocenionymi miarami wydajności są PDR (współczynnik dostarczania pakietów) i opóźnienie. W poprzednich badaniach oceniano te algorytmy pod kątem ruchu sieciowego, prędkości węzła, obszaru i zasięgu anteny dla różnych scenariuszy symulacji. Ogólnie rzecz biorąc, MAODV działa lepiej w przypadku dużego ruchu. ODMRP działa lepiej w przypadku dużych obszarów i dużych prędkości węzłów, ale gorzej w przypadku małych zasięgów anten. Dlatego w tym projekcie zostanie zastosowany MAODV i jego pochodna AODV ALMA. Ze względu na heterogeniczny, dynamiczny charakter tego hybrydowego MANET-u stoi dziś przed wieloma wyzwaniami technicznymi. Hybrydowy schemat routingu AODV ALMA może działać jednocześnie, łącząc agentów mobilnych w celu znalezienia ścieżki do bramy, a podejście oparte na wektorze odległości na żądanie w celu znalezienia ścieżki w lokalnym MANET jest jednym z unikalnych rozwiązań. Adaptacyjny mechanizm wykrywania bramek oparty na agentach mobilnych wykorzystujących wartość feromonów, czas zaniku feromonów i wskaźnik równowagi służy do oszacowania ścieżki i następnego przeskoku do bramy. Węzły mobilne automatycznie konfigurują adres za pomocą agentów mobilnych, najpierw wybierając bramę, a następnie używając adresu prefiksu bramy. Agenci mobilni są również wykorzystywani do śledzenia zmian w topologii, umożliwiając wysoką łączność sieciową przy zmniejszonych opóźnieniach w transmisji pakietów do Internetu. Klastrowanie to skuteczna technika zarządzania węzłami w sieci MANET. Tworzenie klastra polega na wyborze węzła mobilnego na szefa klastra, który będzie kontrolował pozostałe węzły w nowo utworzonym klastrze. Połączenia między węzłami a głowicą klastra zmieniają się szybko w mobilnej sieci ad hoc. Zatem utrzymanie klastra jest również niezbędne. Przewidywanie utrzymania klastra opartego na mobilności obejmuje proces ustalania następnej pozycji, jaką może zająć węzeł mobilny na podstawie poprzednich odwiedzonych lokalizacji. Narzut można zmniejszyć w komunikacji, przewidując ruchliwość węzła za pomocą autoregresji liniowej i tworzenia klastrów.

TETRA W SIECI DVB-T/DTTV

Digital Video Broadcasting — Terrestrial (DVB-T) to europejski standard konsorcjum DVB dotyczący transmisji naziemnej telewizji cyfrowej, który został po raz pierwszy opublikowany w 1997 r., a pierwsza transmisja DVB-T miała miejsce w Wielkiej Brytanii w 1998 r. Standard DVB-T system przesyła skompresowany cyfrowy dźwięk, cyfrowe wideo i inne dane w strumieniu transportowym MPEG, wykorzystując modulację kodowanego multipleksowania z ortogonalnym podziałem częstotliwości (COFDM lub OFDM) (ETSI, 2004-2006). W ostatnim czasie podejmuje się wiele wysiłków w kierunku

wykorzystania infrastruktury DVB-T do ostrzegania o sytuacjach awaryjnych i alarmowania społeczeństwa w obliczu katastrofalnych zdarzeń, w ramach zintegrowanych systemów rozgłoszeniowych ostrzegania o sytuacjach awaryjnych (EWBS). EWBS zwykle wykorzystuje sieci nadawcze telewizyjne i radiowe, aby ostrzegać ludzi o zbliżających się katastrofach i umożliwiać im przygotowanie się na sytuacje awaryjne. EWBS wykorzystuje specjalne sygnały ostrzegawcze lub alarmowe wbudowane w sygnały telewizyjne i radiowe, aby automatycznie włączyć odbiornik (jeśli jest na wyposażeniu) w domu i wydać biuletyn alarmowy, ostrzegając ludzi o zbliżającej się katastrofie, takiej jak tsunami lub trzęsienie ziemi . Poza tym zaproponowano co najmniej jeden specjalny standard systemu ostrzegania o katastrofach dla DVB-T, który obejmuje specyficzną architekturę przepływu komunikatów oraz standard nadajnika i odbiornika. Jednakże nie są dostępne żadne implementacje systemów opartych na DVB-T, które byłyby szczególnie przydatne w środowiskach ochrony publicznej i pomocy w przypadku katastrof (PPDR), gdyż zasadniczo stanowią część zintegrowanego systemu nadawczego reagowania kryzysowego (ERBS). Ponieważ systemy nadawcze telewizji, w tym systemy telewizji cyfrowej (DTV), są powszechnie dostępne na obszarach wiejskich i miejskich, a na ich działanie i zasięg fal radiowych nie ma wpływu rodzaj terenu, morfologia terenu ani warunki pogodowe, wykorzystanie DVB-T systemy oparte na systemie DVB-T w kontekście powstających systemów ERBS byłyby bardzo korzystne, szczególnie biorąc pod uwagę: wyższą szybkość transmisji obrazu i dźwięku w systemach opartych na DVB-T w porównaniu z ich analogowymi odpowiednikami lub wcześniejszymi wdrożeniami telewizji cyfrowej; Wyższa wydajność widmowa w porównaniu do ich analogowych odpowiedników; Zaawansowane możliwości wykrywania błędów w przód (FEC), które również zapewniają znaczne zwiększenie wydajności; oraz Poprawioną odporność sygnału na wpływy zewnętrzne, takie jak uderzenia(-a) spowodowane położeniem geograficznym, warunkami pogodowymi oraz budynkami/przeszkodami technicznymi.

WNIOSEK

Ogólnie rzecz biorąc, ważne jest zapewnienie ram, które będą wykorzystywać dodatkowe sieci (mobilne IP, sieci mobilne Ad-Hoc i DVB-T) do wspierania komunikacji w sytuacjach kryzysowych (którą obecnie i w przewidywalnej przyszłości będzie TETRA). i zarządzanie zasobami podczas katastrof w dwóch aspektach:

(i) gwarantowane możliwości i usługi komunikacyjne pomiędzy zespołami i jednostkami reagowania niezależnie od lokalizacji i poziomu kryzysu,

(ii) możliwości komunikacji między ratownikami a ogółem społeczeństwa, osobami dotkniętymi katastrofą i ich rodzinami Zaangażowanie rodzin, obywateli i grup społecznych w akcje ratownicze (miliony oczu/agentów dostarczających za pośrednictwem Internetu nieustrukturyzowanych informacji krytycznych pod względem czasowym, takich jak możliwe lokalizacje uwięzionych osób) zilustrował już korzyści płynące z tego rozwiązania podczas akcji ratowniczych po niedawnym poważnym trzęsieniu ziemi w Van w Turcji.

Trzęsienie ziemi , Van, Turcja (październik 2011 r.): Główni operatorzy GSM w Turcji zdołali naprawić swoją infrastrukturę w ciągu pierwszych 1–3 godzin od trzęsienia ziemi. Zwiększyli także wydajność swojej infrastruktury za pomocą stacji mobilnych, aby móc obsłużyć dodatkowe obciążenie. Świadczyli bezpłatne usługi w regionie trzęsienia ziemi. Wysiłki te opłaciły się wkrótce po uratowaniu życia dzięki łączności GSM i 3G.

• Yalcin Akay (19 lat) został uwięziony pod zawalonym sześciopiętrowym budynkiem z powodu kontuzji nogi. Sieć GSM działała i mógł zadzwonić na numer alarmowy Policji (155). Pan Akay opisał swoje stanowisko zespołowi pierwszego reagowania. Uratował siebie i troje innych osób, w tym dwoje dzieci, które zostały uwięzione pod tym samym budynkiem.

• Saydun Gökşin, sekretarz generalny Tureckiego Towarzystwa Poszukiwań i Ratownictwa (AKUT), powiedział reporterom, że zespołom AKUT udało się uratować trzy osoby uwięzione pod zawalonym budynkiem, korzystając z informacji z Twittera. Napisali na Twitterze. Do dokładnego określenia ich współrzędnych wykorzystano funkcję lokalizacji tweetów. W ciągu 2 godzin ekipy poszukiwawcze mogły do nich dotrzeć.

• Rodziny i przyjaciele są zorganizowani pod „hasztagami", aby informować zespoły pierwszego reagowania o lokalizacji zawalonych budynków oraz o znanych im osobach, które mogły zostać uwięzione pod tymi budynkami. Była to bardzo ważna służba dla rodzin w całej Turcji, których członkami są pracownicy państwowi pełniący służbę w regionie dotkniętym klęską (np. nauczyciele szkół podstawowych i średnich, lekarze, pielęgniarki, żołnierze…).

W tym kontekście rozważamy trzy regiony na obszarze klęski pod względem lokalizacji komunikacyjnej: miejsce zdarzenia, miejsce pierwszej pomocy i miejsce lokalne, w którym znajdują się dodatkowe zasoby. Każdy z tych regionów może mieć inne wymagania. Na przykład lokalna lokalizacja dodatkowych zasobów może już posiadać infrastrukturę do obsługi operacji. Placówka pierwszej pomocy może być lepiej zorganizowana w porównaniu do placówki ratunkowej, która może stanowić najtrudniejsze środowisko do zapewnienia niezawodnych, bezpiecznych i wysokiej jakości usług komunikacyjnych. Celem jest stworzenie struktury, która będzie mogła się dostosowywać w oparciu o wymagania i dostępne zasoby w środowisku, w którym działa.