JAKIE WĄTPLIWOŚCI BUDZĄ KWESTIE CYBERBEZPIECZEŃSTWA?

WYZWANIA W CYBERBEZPIECZEŃSTWIE

Technologie oferują nowe możliwości, które wcześniej nie były możliwe. Na przykład nowa fala łączności wykracza poza tablety i laptopy; do połączonych samochodów i budynków; Telewizory i konsole do gier; inteligentne liczniki i kontrola ruchu; z perspektywą inteligentnego łączenia prawie wszystkiego i każdego. Nieuniknione jest, że dalsza integracja technologii informacyjno-komunikacyjnych (ICT) z życiem codziennym będzie kontynuowana. Rozwojowi społeczeństwa informacyjnego towarzyszą jednak nowe i poważne zagrożenia. Poniżej omówiono najważniejsze wyzwania związane z cyberbezpieczeństwem, od obaw związanych z prywatnością, przez kwestie techniczne, kwestie prawne po zobowiązania przywódcze. Wszystkie inteligentne urządzenia przechowują informacje o swoich użytkownikach, od planu diety po miejsce pracy; urządzenia inteligentne zawierają dane dotyczące życia osobistego i często dane bankowe. Dlatego gromadzenie i wykorzystywanie danych Internetu rzeczy (IoT) może stać się problemem prywatności, gdy osoby obserwowane przez urządzenia IoT mają inne perspektywy prywatności dotyczące zakresu i wykorzystania tych danych niż osoby zbierające dane. Dlatego prywatność jest często wymieniana jako jeden z najważniejszych problemów we wdrażaniu IoT na dużą skalę. IoT na nowo definiuje pojęcie kwestii prywatności, ponieważ wiele wdrożeń może radykalnie zmienić sposób gromadzenia, analizowania, wykorzystywania i ochrony danych osobowych. ICT są obecnie odpowiedzialne za funkcje kontroli i zarządzania w budynkach, samochodach i usługach lotniczych. Podstawowe usługi, takie jak zaopatrzenie w wodę i energię elektryczną, opierają się obecnie na ICT. Od sprawnego funkcjonowania ICT zależą również samochody, kontrola ruchu, windy, klimatyzacja i telefony. Rosnące uzależnienie od technologii informatycznych jest jednym z głównych wyzwań, przed którymi stoi wiele narodów. Wraz ze wzrostem liczby osób podłączonych do Internetu wzrasta liczba celów i przestępców. Trudno oszacować, ile osób korzysta z internetu do nielegalnych działań. Nawet gdyby tylko 0,1% użytkowników popełniło przestępstwa, łączna liczba przestępców przekroczyłaby milion. Rosnąca liczba internautów sprawia również trudności organom ścigania, gdyż stosunkowo trudno jest zautomatyzować procesy dochodzeniowe. Usługi komputerowe i technologie związane z Internetem od czasu wprowadzenia tej technologii doprowadziły do powstania nowych form przestępczości. Szybki postęp w funkcjonalności technologii i wrodzone rozbieżności między systemami prawa na całym świecie stanowią poważne wyzwania dla służb ratowniczych, organów śledczych, śledczych, organów ścigania i organów wymiaru sprawiedliwości w sprawach karnych. Przestępstwa związane z cyberprzestępczością mogą być skomplikowane technicznie i zawiłe prawnie. Środki prawne, kluczowa rola w zapobieganiu i zwalczaniu cyberprzestępczości, są wymagane we wszystkich obszarach, w tym kryminalizacji, uprawnień proceduralnych, jurysdykcji, współpracy międzynarodowej oraz odpowiedzialności i odpowiedzialności dostawcy usług internetowych. Według kluczowych wniosków PwC z badania US State of Cybercrime Survey z 2015 r. prawie połowa (49%) zarządów postrzega cyberbezpieczeństwo jako zagrożenie informatyczne, podczas gdy 42% z nich postrzega cyberbezpieczeństwo przez pryzmat ładu korporacyjnego. Zbyt wiele organizacji pozostawia pierwszą odpowiedź swoim zespołom IT bez odpowiedniej interwencji lub wsparcia ze strony kierownictwa wyższego szczebla i innych kluczowych graczy. Przy tak dużym zagrożeniu kadra kierownicza i zarządy wyższego szczebla nadal niechętnie podchodzą do kwestii cyberbezpieczeństwa. Poniższe sekcje zawierają szczegółowe informacje na temat wyzwań związanych z cyberbezpieczeństwem, w tym problemów związanych z prywatnością, problemów technicznych, kwestii prawnych i zaangażowania kierownictwa.

PROBLEMY DOTYCZĄCE PRYWATNOŚCI

IoT, duża sieć urządzeń obsługujących czujniki, zaprojektowana do zbierania danych o swoim otoczeniu, często zawiera dane dotyczące ludzi. Dane te prawdopodobnie przynoszą korzyść właścicielowi urządzenia, producentowi urządzenia i dostawcy. Gromadzenie i wykorzystywanie danych IoT może stać się problemem prywatności, gdy osoby obserwowane przez urządzenia IoT mają inne perspektywy prywatności dotyczące zakresu i wykorzystania tych danych niż osoby zbierające dane. Dlatego prywatność jest często wymieniana jako jeden z najważniejszych problemów we wdrażaniu IoT na dużą skalę. Poszanowanie prawa do prywatności jest integralną częścią zapewnienia zaufania do Internetu. Kwestie dotyczące prywatności mają kluczowe znaczenie, ponieważ mają wpływ na nasze podstawowe prawa i naszą wspólną zdolność do zaufania do Internetu. Ważne jest, aby zrozumieć różnicę między prywatnością a anonimowością. Prywatność, związana z poufnością, to możliwość określenia docelowej grupy docelowej danych. Anonimowość to cecha lub stan bycia nieznanym większości ludzi. Na przykład elektroniczne akta dotyczące zdrowia są prywatne i poufne, ale nie anonimowe. Naruszenie bezpieczeństwa nie zawsze może skutkować utratą prywatności. Zależy to od pobranych danych i sposobu ich późniejszego wykorzystania. Bez odpowiednich zabezpieczeń intruzi mogą włamywać się do systemów i sieci IoT, aby uzyskać dostęp do potencjalnie wrażliwych danych osobowych użytkowników, naruszając w ten sposób ich prywatność, zwłaszcza gdy urządzenia są używane w przestrzeniach prywatnych, takich jak domy poszczególnych osób. Ponadto operatorzy systemów IoT z autoryzowanym dostępem do wytwarzanych danych prawdopodobnie będą w stanie „zbierać, analizować i działać na danych z wcześniej prywatnych przestrzeni". Obawy dotyczące prywatności mogą nadal pojawiać się, gdy systemy są bezpieczne i działają zgodnie z przeznaczeniem. Na przykład, czy czujemy się komfortowo, dzieląc się naszymi danymi z osobami, których nawet nie jesteśmy świadomi? Czy sponsorowanie projektów przez osoby trzecie uprawnia ich do dostępu do uzyskanych danych? Gdy dane są przetwarzane przez stronę trzecią, ważne jest, aby dane były chronione umową o przetwarzanie danych z tą stroną trzecią, ponieważ odpowiedzialność za ochronę tych danych jest również przenoszona na stronę trzecią wraz z przekazaniem danych. Niepokojące jest jednak to, że większość dostawców usług w chmurze nie posiada obecnie polityki prywatności lub ma nieprzejrzyste polityki. W innych sytuacjach użytkownik może nie być świadomy, że urządzenie IoT zbiera dane o danej osobie i potencjalnie udostępnia je stronom trzecim. Ten rodzaj gromadzenia danych staje się coraz bardziej powszechny w urządzeniach konsumenckich, takich jak inteligentne telewizory i urządzenia do gier wideo. Tego typu produkty mają funkcje rozpoznawania głosu lub wizji, które stale słuchają rozmów lub obserwują aktywność w pomieszczeniu i selektywnie przesyłają te dane do usługi w chmurze w celu przetworzenia, która czasami obejmuje stronę trzecią. Osoba może znajdować się w obecności tego rodzaju urządzeń, nie wiedząc, że jej rozmowa lub działania są monitorowane, a jej dane są przechwytywane. Chociaż tego rodzaju funkcje mogą przynosić korzyści poinformowanemu użytkownikowi, mogą stanowić problem z prywatnością dla osób, które nie są świadome obecności urządzeń i nie mają znaczącego wpływu na sposób wykorzystania zebranych informacji. Niezależnie od tego, czy użytkownik jest świadomy i wyraża zgodę na gromadzenie i analizę danych IoT, sytuacje te podkreślają monetyzację tych spersonalizowanych strumieni danych dla firm, które chcą wykorzystać dane IoT. Zapotrzebowanie na te informacje nasila wyzwania prawne i regulacyjne, przed którymi stoją przepisy dotyczące ochrony danych i prywatności. Z szerokiej perspektywy ludzie uznają, że ich prywatność jest z natury cenna i mają oczekiwania co do tego, jakie dane na ich temat mogą być gromadzone i jak inne strony mogą z nich korzystać. To ogólne pojęcie o prywatności dotyczy danych gromadzonych przez urządzenia IoT, ale urządzenia te mogą osłabiać zdolność użytkownika do wyrażania i egzekwowania preferencji prywatności. Jeśli użytkownicy stracą zaufanie do Internetu, ponieważ ich preferencje dotyczące prywatności nie są respektowane w IoT, większa wartość Internetu może zostać zmniejszona.

PRZYKŁAD Z PRAWDZIWEGO ŚWIATA

Przegląd korporacji

Sony jest bardzo szanowanym międzynarodowym konglomeratem z siedzibą w Japonii, którego przychody w 2011 roku wyniosły 86 miliardów USD. Chociaż firma ma wiele odrębnych jednostek biznesowych, Sony jest najbardziej znane z produkcji wysokiej jakości elektroniki.

Trwałe naruszenia

Wyzwania Sony rozpoczęły się w kwietniu 2011 r. od masowego naruszenia PlayStation Network, po którym nastąpiły dodatkowe naruszenia, w tym skierowane przeciwko działowi rozrywki online. Naruszenia te spowodowały utratę 100 milionów rekordów klientów i zamknięcie działalności biznesowej kilku jednostek Sony w ciągu kilku tygodni.

Odpowiedź

Głównym wyzwaniem firmy Sony w odpowiedzi na te naruszenia bezpieczeństwa danych było umiejętne nawigowanie w percepcji i zarządzaniu obrazem. Pod tym względem Sony zawiodło. Firma spotkała się z bardzo negatywnym zainteresowaniem mediów z powodu postrzeganego opóźnienia w powiadamianiu klientów o naruszeniu, które stało się tak dużym problemem, że sam dyrektor generalny, Howard Stringer, był zmuszony odpowiadać na pytania mediów. Obrona przez Stringera jednotygodniowego czasu reakcji Sony padła na niedowierzające uszy i tylko pogorszyła wściekłą reakcję publiczną. Rozważając publiczne przeprosiny, należy pamiętać, że Sony ma siedzibę w Japonii, gdzie tego rodzaju przeprosiny zostałyby po prostu przyjęte, a sprawa zamknięta. Dość powiedzieć, że ten szerszy kontekst kulturowy zaginął pośród burzy niszczącej reklamy. Z punktu widzenia specjalisty ds. bezpieczeństwa firma Sony była technicznie rozważna i szybko odpowiadała. Jednak z perspektywy konsumenta postrzeganie błędnej reakcji Sony wywołało reakcję. Chociaż miało to być pozytywne wydarzenie, ogłoszenie z maja 2011 r., że Sony tworzy globalną rolę CISO, wzbudziło więcej obaw, niż zostało rozstrzygniętych. Biorąc pod uwagę szeroki zakres naruszonych systemów i dotkniętych jednostek biznesowych, spóźnione wdrożenie tej roli nasuwa pytanie, dlaczego Sony nie posiadało CISO przed tymi naruszeniami. Uważa się, że bezpieczeństwo było refleksją, której Sony nie potraktowało poważnie, i że poszczególne jednostki biznesowe pozostawiono do samodzielnego zarządzania bezpieczeństwem. Niewiele więcej może wyjaśnić całkowity demontaż zabezpieczeń cybernetycznych firmy Sony. Pierwsze reakcje klientów firmy Sony obejmowały oferowanie usług monitorowania kredytów klientom, których to dotyczy, ulepszoną obsługę klienta, tworzenie programów powitalnych i wdrażanie nowych systemów bezpieczeństwa. Dotychczasowe koszty bezpośrednie wynoszą około 171 mln USD, ale biorąc pod uwagę opłaty prawne i inne potencjalne utracone przychody, łączne szacunkowe koszty Sony wynikające z tych naruszeń wahają się od 13 do 20 mld USD w perspektywie długoterminowej.

Wiktymologia

Naruszenia Sony zachęcają do szczegółowego zbadania wiktymologii. Wstępne raporty sugerują, że dane osobowe 75 milionów użytkowników PlayStation zostały naruszone w wyniku tych naruszeń. Można sobie wyobrazić tych użytkowników PlayStation jako nastoletnich i młodych dorosłych graczy; w rzeczywistości wielu z tych graczy nie posiada kart kredytowych, a zatem to ich rodzice lub opiekunowie zostali utracone. Prawdziwą stratą jest jednak zaufanie. Zepsuta reputacja Sony może zasiać to pytanie w umysłach milionów konsumentów: jeśli ta firma nie dba wystarczająco o zabezpieczenie moich informacji, czy naprawdę tworzy rodzaj niezawodnych urządzeń wysokiej klasy, których moja rodzina będzie potrzebować w przyszłości?

KWESTIE TECHNICZNE

NADMIERNE ZAUFANIE DO TECHNOLOGII

Nieuniknione jest, że dalsza integracja technologii informacyjno-komunikacyjnych z życiem codziennym będzie kontynuowana. Infrastruktura nowoczesnego społeczeństwa nie może już funkcjonować bez komputerów i sieci. Cyberprzestrzeń dotyka praktycznie wszystkiego i wszystkich, ponieważ ICT poprawiły codzienne życie. Ta nowa fala łączności wykracza poza tablety i laptopy; do połączonych samochodów i budynków; Telewizory i konsole do gier; inteligentne liczniki i kontrola ruchu; z perspektywą inteligentnego łączenia prawie wszystkiego i każdego. ICT są obecnie odpowiedzialne za funkcje kontroli i zarządzania w budynkach, samochodach i usługach lotniczych. Rozwojowi społeczeństwa informacyjnego towarzyszą nowe i poważne zagrożenia. Podstawowe usługi, takie jak zaopatrzenie w wodę i energię elektryczną, opierają się obecnie na ICT. Od sprawnego funkcjonowania ICT zależą również samochody, kontrola ruchu, windy, klimatyzacja i telefony. Ponieważ technologia już kontroluje krytyczne systemy, takie jak trasy linii lotniczych, sieci energetyczne, rynki finansowe, broń wojskowa, pociągi podmiejskie, sygnalizacja świetlna i nasze linie komunikacyjne, ataki na infrastrukturę informacyjną i usługi internetowe mogą teraz zaszkodzić społeczeństwu w nowych i krytyczne sposoby. Według przewodnika ITU National Cybersecurity Strategy Guide, nasze stale rosnące poleganie na cyberprzestrzeni naraża rządy, firmy i użytkowników indywidualnych na ryzyko oszustw, sabotażu i wandalizmu. Cyberzagrożenia regularnie uzyskują dostęp, kradną i korumpują wrażliwe informacje osobiste, korporacyjne i rządowe. Ponadto rosnące uzależnienie od technologii informacyjno-komunikacyjnych sprawia, że systemy i usługi są bardziej podatne na ataki na infrastrukturę krytyczną. Nawet krótkie przerwy w świadczeniu usług mogą spowodować ogromne straty finansowe dla firm zajmujących się handlem elektronicznym. Na przykład „problem z routerem" w United Airlines uziemił swoje samoloty na prawie dwie godziny, co doprowadziło do 800 opóźnień lotów i 60 odwołań. Akcje o łącznej wartości 28 bilionów dolarów zostały zawieszone na trzy i pół godziny w lipcu 2015 r. na giełdzie nowojorskiej. Nie tylko komunikacja cywilna może zostać przerwana przez ataki; zależność od technologii informacyjno-komunikacyjnych stanowi poważne zagrożenie dla komunikacji wojskowej. W ciągu ostatnich kilku lat cyberataki ewoluowały w kierunku wykorzystywania broni online uderzającej w podmioty rządowe. Według KPMG cyberprzestępczość motywowana politycznie przeniknęła globalną cyberprzestrzeń. Systemy uzbrojenia i kontroli przeniosły się w cyberprzestrzeń, aby wdrażać i przeprowadzać szpiegostwo i sabotaż, na przykładzie cyfrowych ataków szpiegowskich na sieć komputerową w Lockheed Martine i NASA. Bezpieczeństwo narodowe i gospodarcze USA zależy od niezawodnego funkcjonowania infrastruktury krytycznej. Infrastrukturę krytyczną definiuje się jako kluczowe systemy i aktywa dla Stanów Zjednoczonych, których niesprawność lub zniszczenie miałoby wyniszczający wpływ na społeczeństwo, narodowe bezpieczeństwo gospodarcze, krajowe zdrowie lub bezpieczeństwo publiczne lub na dowolną kombinację tych kwestii. Zagrożenia cyberbezpieczeństwa wykorzystują zwiększoną złożoność i łączność systemów infrastruktury krytycznej, narażając na ryzyko bezpieczeństwo kraju, gospodarkę oraz bezpieczeństwo i zdrowie publiczne. Pracownik Białego Domu USA odpowiedzialny za zwalczanie terroryzmu i cyberbezpieczeństwo, zauważa, że cyberatak na pełną skalę na ważną infrastrukturę kraju, taką jak wojskowe systemy poczty elektronicznej, systemy kontroli ruchu lotniczego, rynki finansowe i narzędzia, może mieć bezprecedensowy długofalowy skutek . Istniejąca infrastruktura techniczna ma szereg słabości, takich jak monokultura czy jednorodność systemów operacyjnych. Ponieważ większość komputerów na świecie obsługuje systemy operacyjne Microsoft, większość komputerów na świecie jest jednocześnie podatna na te same wirusy i robaki. Przestępcy mogą projektować skuteczne ataki, koncentrując się na tym jednym celu. Przełamanie monokultury w komputerowych systemach operacyjnych w celu złagodzenia tej podatności jest tak samo rozsądne i oczywiste, jak unikanie monokultury w rolnictwie. Niezwykle ważne jest, aby społeczeństwo było mniej zależne od jednego systemu operacyjnego od jednego dostawcy, ponieważ

krytyczna infrastruktura nie może zostać zakłócona podczas jednego ataku. Monokultura komputerów w sieci jest wygodnym i podatnym rezerwuarem platform, z których można przeprowadzać ataki. Tworzy to zagregowane ryzyko, że dywersyfikacja ryzyka jest podstawową obroną przed takim ryzykiem.

Infrastruktura krytyczna

1) Chemikalia

2) Obiekty handlowe

3) Komunikacja

4) Produkcja krytyczna

5) Tamy

6) Obronna baza przemysłowa

7) Służby ratownicze

8) Energia

9) Usługi finansowe

10) Żywność i rolnictwo

11) Obiekty rządowe

12) Opieka zdrowotna i zdrowie publiczne

13) Technologia informacyjna

14) Reaktory jądrowe, materiały i odpady

15) Systemy transportowe

16) Systemy wodno-ściekowe

LICZBA UŻYTKOWNIKÓW

Rozwój taniego sprzętu i dostępu bezprzewodowego umożliwia dostęp do Internetu większej liczbie osób. Obecnie w sieci WWW jest ponad miliard witryn. Ten kamień milowy osiągnięto po raz pierwszy w 2014 r. Sam portal społecznościowy Facebook ma ponad 1,79 miliarda aktywnych użytkowników miesięcznie w trzecim kwartale 2016 r. Nic dziwnego, że dramatyczny wzrost korzystania z Internetu, przy ponad połowie światowej populacji, korzystających z internetu do 2020 r. Raport Verizon IoT 2015 przewiduje, że liczba połączeń Business-to-Business (B2B) IoT wzrośnie o 28% rok do roku w latach 2011-2020. Branże takie jak produkcja, energetyka, transport i handel detaliczny już przyjmują inicjatywy IoT. W swoim pozycjonowaniu Industrial Internet of Things z 2015 r. Accenture przewiduje, że do 2030 r. „przemysłowy" IoT będzie wart 7,1 bln USD w samych Stanach Zjednoczonych. Do 2050 roku świat doświadczy prawie podwojenia populacji miejskiej do 6,2 miliarda - 70% przewidywanej światowej populacji wynoszącej 8,9 miliarda. Wraz ze wzrostem liczby urządzeń podłączonych do Internetu oczekuje się znacznego wzrostu natężenia ruchu. Na przykład Cisco szacuje, że ruch internetowy generowany przez urządzenia inne niż komputery PC wzrośnie z 40% w 2014 r. do prawie 70% w 2019 r. Cisco prognozuje również, że liczba połączeń „Machine to Machine" („M2M") (w tym w przemysł, dom, opieka zdrowotna, motoryzacja i inne branże IoT) wzrośnie z 24% wszystkich

podłączonych urządzeń w 2014 r. do 43% w 2019 r. Wraz ze wzrostem liczby osób podłączonych do Internetu rośnie liczba celów i przestępców. Trudno oszacować, ile osób korzysta z internetu do nielegalnych działań. Nawet gdyby tylko 0,1% użytkowników popełniło przestępstwa, łączna liczba przestępców przekroczyłaby milion. Rosnąca liczba internautów sprawia również trudności organom ścigania, gdyż stosunkowo trudno jest zautomatyzować procesy dochodzeniowe. Ponadto przestępcy wykorzystują ICT na różne sposoby do przygotowania i wykonania swoich przestępstw, a organy ścigania potrzebują odpowiednich instrumentów do prowadzenia dochodzeń w sprawie potencjalnych czynów przestępczych. Według Biura Narodów Zjednoczonych ds. Narkotyków i Przestępczości (UNODC) rzeczywistość globalnej łączności należy uznać za centralny element współczesnej cyberprzestępczości, a w szczególności cyberprzestępczości jutra. Wraz ze wzrostem cyberprzestrzeni i ruchu IP, ponieważ ruch z urządzeń bezprzewodowych przewyższa ruch z urządzeń przewodowych, a coraz większy ruch internetowy pochodzi z urządzeń innych niż komputery PC, może być trudno wyobrazić sobie przestępstwo „komputerowe" bez łączności IP. Szczególnie osobisty charakter urządzeń mobilnych i pojawienie się połączonych z IP przedmiotów gospodarstwa domowego lub rzeczy osobistych oznacza, że elektroniczne dane i transmisje mogą być nawet generowane przez lub stać się integralną częścią prawie każdego ludzkiego działania - legalnego lub nielegalnego.

PROBLEMY PRAWNE

Usługi komputerowe i technologie związane z Internetem od czasu wprowadzenia tej technologii doprowadziły do powstania nowych form przestępczości. Przestępstwa związane z cyberprzestępczością mogą być skomplikowane technicznie i zawiłe prawnie. We wszystkich obszarach wymagane są środki prawne, kluczowa rola w zapobieganiu i zwalczaniu cyberprzestępczości, w tym kryminalizacja, uprawnienia proceduralne, jurysdykcja, współpraca międzynarodowa oraz odpowiedzialność i odpowiedzialność dostawcy usług internetowych. Według UNODC nastąpił znaczny postęp w ogłaszaniu międzynarodowych i regionalnych instrumentów mających na celu zwalczanie cyberprzestępczości. Należą do nich instrumenty wiążące i niewiążące. Można zidentyfikować pięć klastrów składających się z instrumentów opracowanych w kontekście lub inspirowanych przez:

* Rada Europy lub Unia Europejska

* Wspólnota Niepodległych Państw lub Szanghajska Organizacja Współpracy

* Międzyrządowe organizacje afrykańskie

* Liga Państw Arabskich

* Organizacja Narodów Zjednoczonych

Szybki postęp w funkcjonalności technologii i wrodzone rozbieżności między systemami prawa na całym świecie stanowią poważne wyzwania dla służb ratowniczych, organów śledczych, śledczych, organów ścigania i organów wymiaru sprawiedliwości w sprawach karnych. W poniższej tabeli wymieniono główne wyzwania związane z cyberprzestępczością, przed którymi stoi wymiar sprawiedliwości w sprawach karnych.

Najważniejsze wyzwania związane z cyberprzestępczością, przed którymi stoją ramy prawne wymiaru sprawiedliwości w sprawach karnych i należyty proces

• Luki w przepisach i opóźnienia administracyjne wynikające z niepewności sądów co do charakteru przestępstwa cyberprzestępczości mogą uniemożliwić śledczym uzyskanie wymaganego upoważnienia prawnego do przechwytywania danych elektronicznych.

• Przepisy prawne, które nie są zharmonizowane wśród członków społeczności międzynarodowej, mogą tworzyć bezpieczne jurysdykcje dla cyberprzestępstw i możliwych kolizji prawa.

• Przepisy, które nie zostały opracowane tak, aby obejmowały technologię szeroko w ramach ustalonych kategorii zachowań przestępczych, szybko staną się przestarzałe, co ograniczy zdolność władz do prowadzenia dochodzeń w sprawie cyberprzestępczości i wszczynania skutecznych postępowań karnych.

Prywatność i przywileje

• Dochodzenia mogą naruszać podstawowe prawa człowieka i prowadzić do braku odpowiedzialności, jeśli sądownictwo nie jest wystarczająco upoważnione do sprawowania nadzoru.

• Pojawiające się na całym świecie przepisy dotyczące ochrony danych i prywatności sprawiają, że informacje elektroniczne znajdują się poza zasięgiem organów śledczych.

Identyfikacja

• Trudności w przypisaniu własności i autorstwa informacji przechowywanych elektronicznie.

• Trudności w identyfikacji osób w kontroli systemów i urządzeń informatycznych.

• Niemożność szybkiego zlokalizowania istotnych informacji wśród dużych zbiorów danych.

• Nieskuteczność w śledzeniu działalności przestępczej w przypadku zastosowania technik anonimizacji i zaciemniania danych.

• Powszechna dostępność oprogramowania do czyszczenia danych i czyszczenia urządzeń dla urządzeń konsumenckich, co może prowadzić do zniszczenia dowodów.

Dostęp

• Brak możliwości uzyskania upoważnienia do przeprowadzania kontroli online i gromadzenia zdalnie przechowywanych danych, szczególnie jeśli docelowym hostem jest dostawca usług w chmurze, którego baza operacyjna znajduje się poza jurysdykcją władz lokalnych.

• Brak możliwości pozyskania danych ze względu na postępy w bezpieczeństwie konsumentów na urządzeniach standardowych, w tym silne szyfrowanie, narzędzia do ochrony prywatności typu open source i technologie antykryminalistyczne.

• Dostawcy usług, którzy odpowiadają na autoryzowane prośby o wytworzenie i zachowanie danych, mogą spowodować utratę krytycznych dowodów.

Dopuszczalność i uczciwość

• Dokumentacja łańcucha dowodowego, która jest niekompletna lub niedokładna, może skutkować uznaniem dowodów elektronicznych za niedopuszczalne.

• Organy ścigania, które nie są w stanie potwierdzić wiarygodności lub autentyczności informacji elektronicznych, mogą udaremnić wysiłki radcy prawnego, aby przedstawić ten materiał jako dowód w sądzie.

Kapitał Ludzki

• Analitycy, którzy nie mają kwalifikacji do obsługi sprzętu technicznego lub pozyskiwania danych z systemów informatycznych, mogą zanieczyścić dowody i poważnie podważyć wiarygodność raportów kryminalistycznych sporządzonych na potrzeby dochodzeń policyjnych.

• Agencje, które nie posiadają wystarczającej wiedzy fachowej w danej dziedzinie, ograniczą zdolność prokuratorów do przedstawiania opinii biegłych, które wyjaśniają podstawy techniczne i znaczenie materiału przed sądem.

• Policja, która nie jest wyposażona w specjalistyczne narzędzia do wydobywania informacji lub nie dysponuje wystarczającą mocą obliczeniową do celowego przetwarzania danych, może przeoczyć krytyczne dowody podczas analizy w laboratorium lub podczas przeprowadzania segregacji w terenie.

• Funkcjonariusze policji, prokuratorzy i sędziowie, którym nie zapewnia się stałego szkolenia, które koncentruje się na sposobach popełniania przestępstw kryminalnych, dyplomatycznych kanałach współpracy, zagranicznych mechanizmach wymiaru sprawiedliwości, kwestiach suwerenności, pojawiających się źródłach informacji elektronicznej i technologiach komunikacyjnych więcej generalnie będą ewidentnie słabo przygotowani do zarządzania sprawami cyberprzestępczości.

UZNANIE NOWYCH PRZESTĘPSTW

Aby zrozumieć wyzwania prawne w świecie cybernetycznym, musimy najpierw poznać podstawowe koncepcje tworzenia praw cybernetycznych wymienionych poniżej:

* Opracowywanie nowych praw lub zmiana istniejących praw przez narody w ich obecnych granicach terytorialnych

* Zawieranie wielostronnych umów międzynarodowych w celu ustanowienia nowych i jednolitych zasad mających zastosowanie do narodów

* Utworzenie nowej organizacji międzynarodowej, która opracowuje nowe zasady i sposoby ich egzekwowania

Opóźnienie między rozpoznaniem potencjalnych nadużyć nowych technologii a niezbędnymi zmianami krajowego prawa karnego było głównym wyzwaniem dla krajowego systemu prawa karnego. To wyzwanie pozostaje tak długo, jak tempo innowacji sieciowych będzie przyspieszać.

IDENTYFIKACJA LUK W KODEKSIE KARNYM

Właściwe ustawodawstwo, stanowiące podstawę dochodzenia i ścigania cyberprzestępczości, wymaga, aby prawodawcy stale reagowali na rozwój Internetu i monitorowali skuteczność istniejących przepisów, zwłaszcza biorąc pod uwagę szybkość rozwoju technologii sieciowych. Obecnie wiele krajów ciężko pracuje, aby nadrobić zaległości legislacyjne. Przestępstwa kryminalizowane na mocy krajowego prawa karnego wymagają przeglądu i aktualizacji. Na przykład informacje cyfrowe muszą mieć status równoważny tradycyjnym podpisom i wydrukom. Jednak niektóre kraje nie zakończyły jeszcze aktualizacji krajowego prawa karnego w celu ścigania nowych form cyberprzestępczości online. Bez integracji przestępstw związanych z cyberprzestępczością nie można ścigać naruszeń. W poniższej tabeli wymieniono funkcje przepisów dotyczących cyberprzestępczości. Funkcje ustawodawstwa dotyczącego cyberprzestępczości

* Ustalenie jasnych standardów zachowania przy korzystaniu z urządzeń komputerowych

* Odstraszanie sprawców i ochrona obywateli

* Umożliwienie dochodzeń organów ścigania przy jednoczesnej ochronie prywatności osób

* Zapewnienie uczciwych i skutecznych procedur wymiaru sprawiedliwości w sprawach karnych

* Wymaganie minimalnych standardów ochrony w obszarach takich jak przetwarzanie i przechowywanie danych

* Umożliwienie współpracy między krajami w sprawach karnych dotyczących cyberprzestępczości i dowodów elektronicznych

Niezbędne jest porównanie statusu przepisów prawa karnego w prawie krajowym z wymogami wynikającymi z nowych rodzajów przestępstw w celu zapewnienia skutecznych podstaw legislacyjnych. Kraje powinny ocenić, czy ich krajowe przepisy dotyczące cyberprzestępczości, prywatności, ochrony danych, prawa handlowego, podpisów cyfrowych i szyfrowania są odpowiednie. Przegląd powinien obejmować jak najwięcej zainteresowanych stron, takich jak departamenty rządowe, wywiad i organy ścigania, firmy prywatne, społeczeństwo obywatelskie, naukowcy i obywatele. W wielu przypadkach istniejące przepisy mogą obejmować nowe rodzaje istniejących przestępstw (np. przepisy dotyczące fałszerstw można z łatwością zastosować do dokumentów elektronicznych). Potrzeba zmian legislacyjnych jest jednak ograniczona do tych przestępstw, które zostały pominięte lub niewystarczająco ujęte w prawie krajowym. Na przykład niektóre kraje miały odpowiednie przepisy dotyczące regularnych oszustw, ale nie były w stanie poradzić sobie z przestępstwami, w których wpłynęło to na system komputerowy, a nie na człowieka. W przypadku tych krajów, oprócz zwykłych oszustw, konieczne było przyjęcie nowych przepisów kryminalizujących oszustwa komputerowe. Co więcej, rozróżnienie między legalną a nielegalną działalnością staje się coraz bardziej zamazane, ponieważ praktyki takie jak zbieranie i przechwytywanie danych oraz manipulacja reputacją będą jeszcze ściślej związane z generowaniem zysków. Obecna bliskość między spamowaniem kryminalnym a legalnymi technikami marketingowymi, takimi jak reklama behawioralna, już teraz służy jako wskaźnik tego problemu. Według UNODC, Comprehensive Study on Cybercrime, na pytanie o główne luki w prawie karnym dotyczącym cyberprzestępczości wiele krajów odniosło się albo do faktu, że ogólnie przepisy karne nie są dobrze dostosowane do cyberprzestępczości, albo do braku przestępstw w odniesieniu do poszczególnych cyberprzestępczości. przeprowadzić. Oto przykłady odpowiedzi z krajów w różnych regionach:

Respondent : Zgłoszony wynik

Kraj w Afryce : Nie ma przestępstw o charakterze cybernetycznym lub informacyjnym.

Kraj w Afryce Zachodniej: Formy i istotne elementy przestępstw naturalnych wymienionych w kodeksie karnym nie mogą być stosowane do przestępstw elektronicznych.

Kraj w Azji Południowej : Potrzebujemy szczegółowych i szczegółowych przepisów, które powinny czynić różne aspekty aktów cybernetycznych przestępstwem. Niestety czekamy na jedno takie prawo, które nie zostało jeszcze zatwierdzone.

Kraj w Azji Zachodniej: istnieje luka prawna dotycząca kryminalizacji kradzieży danych w celu uzyskania korzyści ekonomicznych.

Kraj na Karaibach : Nie ma konkretnych przepisów dotyczących wysyłania spamu, aktów komputerowych związanych z rasizmem i ksenofobią, dyskryminacją, cyberprzemocą i kradzieżą tożsamości itp.,

Kraj w Azji Południowo-Wschodniej: Niektóre określone cyberprzestępstwa nie są obecnie przestępstwami kryminalnymi, takimi jak ataki typu „odmowa usługi” (DOS) i spam.

Kraj w Europie : Obecnie [my] nie kryminalizujemy botnetów, podszywania się i groomingu.

Inny kraj Azja Południowo-Wschodnia : Obecnie nękanie w Internecie, cyberstalking i niektóre przestępstwa związane z tożsamością nie są odpowiednio rozwiązywane.

ITU radzi, aby kraje przyjęły strategię środków prawnych w celu zapewnienia wspólnego kierunku i uzyskania zaangażowania wszystkich zainteresowanych stron. Strategia miałaby alokować zasoby, koordynować i kontrolować wszelkie działania mające na celu uchwalenie i egzekwowanie kompleksowego zestawu przepisów dotyczących cyberbezpieczeństwa. Poniżej przedstawiono działania, które rząd powinien rozważyć w ramach priorytetu/sposobu działań prawnych.

Pozycja: Środki prawne

Ustawodawstwo dotyczące cyberprzestępczości: Ustal, czy:

1) W kraju obowiązują przepisy dotyczące cyberprzestępczości w obszarach takich jak niewłaściwe użycie komputera, podpisy elektroniczne, ochrona danych, własność intelektualna, odpowiedzialność i rozstrzyganie sporów;

2) Właściwi interesariusze uważają, że kodeks karny w Twoim kraju odpowiednio odnosi się do obecnych (i przyszłych) problemów związanych z cyberprzestępczością oraz

3) Krajowe przepisy dotyczące cyberprzestępczości są zgodne z arkuszem roboczym ITU Toolkit for Cybercrime Legislation.

Organ prawny ds. cyberbezpieczeństwa: Ustal, czy rząd krajowy ma uprawnienia do:

1) stanowić narodowy program cyberbezpieczeństwa;

2) Przydziel role i obowiązki;

3) Wyznaczyć systemy jako krytyczną krajową infrastrukturę informacyjną;

4) Wymagaj od interesariuszy zabezpieczenia krytycznych systemów pozostających pod ich kontrolą oraz

5) Uczestniczyć we wspólnych działaniach międzynarodowych dotyczących cyberprzestępczości.

Zdolność do cyberprzestępczości: Ustal, czy:

1) Policja ma zdolność wykrywania, odstraszania i ścigania cyberprzestępczości;

2) istnieją powiązania kooperacyjne z innymi elementami krajowej infrastruktury cyberbezpieczeństwa i sektorem prywatnym;

3) Organy sądowe i ustawodawcze mają świadomość zagrożeń związanych z cyberprzestępczością, środków zapobiegawczych i naprawczych oraz

4) Program nauczania zawodów prawniczych obejmuje cyberprzestępczość.

Współpraca międzynarodowa : W sprawie współpracy międzynarodowej i pomocy dochodzeniowej oceń, czy:

1) Krajowe przepisy dotyczące cyberprzestępczości mają zastosowanie na całym świecie i są interoperacyjne z istniejącymi regionalnymi i globalnymi środkami prawnymi oraz

2) Krajowe przepisy dotyczące cyberprzestępczości umożliwiają globalną współpracę w zakresie dochodzeń i ścigania cyberprzestępczości.

DALSZE ROZWAŻANIE

Zestaw narzędzi ITU do przepisów dotyczących cyberprzestępczości

ITU współpracowało z Komitetem ds. Prywatności i Przestępczości Komputerowej (PACC) Amerykańskiego Stowarzyszenia Adwokackiego (ABA) oraz ponad setką specjalistów ds. prawa i cyberbezpieczeństwa, aby stworzyć dokument zatytułowany „ITU Toolkit for Cybercrime Legislation". Zestaw narzędzi analizuje ustawodawstwo dotyczące cyberprzestępczości w Australii, Kanadzie, Unii Europejskiej, Radzie Europy, Niemczech, Japonii, Meksyku, Singapurze, Indiach, Chinach, Wielkiej Brytanii i Stanach Zjednoczonych. Dlatego w niniejszym przewodniku zaleca się, aby państwa członkowskie ITU rozważyły dostosowanie swoich krajowych przepisów dotyczących cyberprzestępczości z zestawem narzędzi ITU, ponieważ:

• zawiera najistotniejsze punkty z ustawodawstwa głównych krajów (rozwiniętych i rozwijających się), a także wpływowych organów regionalnych, oraz

• Pomaga usunąć luki w krajowym i regionalnym ustawodawstwie cybernetycznym.

WSPÓŁPRACA MIĘDZYNARODOWA

Szybki rozwój technologii sieciowych i ich złożone struktury utrudniają organom krajowym przeprowadzenie procesu opracowywania cyberprzestępczości bez współpracy międzynarodowej. Oddzielne opracowywanie przepisów dotyczących cyberprzestępczości może powodować znaczne powielanie i marnowanie zasobów. Dlatego ważne jest monitorowanie rozwoju międzynarodowych standardów i strategii. Prawo międzynarodowe przewiduje szereg podstaw jurysdykcji nad takimi aktami, w tym formy jurysdykcji terytorialnej i jurysdykcji narodowościowej. Niektóre z tych baz znajdują się również w wielostronnych instrumentach cyberprzestępczych. Bez międzynarodowej harmonizacji krajowych przepisów prawa karnego walka z transnarodową cyberprzestępczością napotka poważne problemy z powodu niespójnych lub niekompatybilnych przepisów krajowych. Nieuchronnie coraz bardziej krytyczne stają się międzynarodowe próby harmonizacji różnych krajowych przepisów karnych. Konwencja Rady Europy o cyberprzestępczości, znana również jako Konwencja Budapeszteńska o Cyberprzestępczości lub Konwencja Budapeszteńska, jest pierwszym międzynarodowym traktatem mającym na celu rozwiązanie problemu przestępczości internetowej i komputerowej poprzez harmonizację przepisów krajowych, poprawę technik śledczych i zacieśnienie współpracy między narodami. W celu ustanowienia „wspólnej polityki kryminalnej" w celu lepszego zwalczania przestępstw komputerowych na całym świecie poprzez harmonizację ustawodawstwa krajowego, wzmocnienie zdolności organów ścigania i wymiaru sprawiedliwości oraz poprawę współpracy międzynarodowej, Konwencja wymaga od każdego państwa-sygnatariusza wdrożenia następujących mechanizmów proceduralnych w ramach swojego prawa krajowego.

Konwencja o głównych postanowieniach dotyczących cyberprzestępczości

* Zdefiniowanie przestępstw kryminalnych i sankcje na mocy prawa krajowego dla czterech kategorii przestępstw komputerowych. Oszustwa i fałszerstwa, pornografii dziecięcej, naruszenia praw autorskich i naruszenia bezpieczeństwa, takiego jak włamania, nielegalne przechwytywanie danych i zakłócenia systemu, które zagrażają integralności i dostępności sieci. Sygnatariusze muszą również uchwalić przepisy ustanawiające jurysdykcję nad takimi przestępstwami popełnionymi na ich terytoriach, zarejestrowanych statkach lub samolotach lub przez ich obywateli za granicą.

* Ustanowienie krajowych procedur wykrywania, prowadzenia dochodzeń i ścigania przestępstw komputerowych oraz zbierania elektronicznych dowodów wszelkich przestępstw kryminalnych. Procedury takie obejmują przyspieszone zachowanie danych przechowywanych na komputerze i

komunikacji elektronicznej (dane „ruchu”), przeszukiwanie i zajmowanie systemu oraz przechwytywanie danych w czasie rzeczywistym. Strony Konwencji muszą zagwarantować warunki i zabezpieczenia niezbędne do ochrony praw człowieka i zasady proporcjonalności.

* Ustanowienie szybkiego i efektywnego systemu współpracy międzynarodowej. Konwencja uznaje cyberprzestępstwa za przestępstwa podlegające ekstradycji i zezwala organom ścigania w jednym kraju na zbieranie dowodów komputerowych na rzecz tych w innym. Wzywa również do ustanowienia całodobowej sieci kontaktów przez siedem dni w tygodniu, aby zapewnić natychmiastową pomoc w dochodzeniach transgranicznych.

Prawo krajowe może w dużym stopniu skorzystać z doświadczeń innych krajów lub międzynarodowych fachowych porad prawnych. Na przykład niektóre kraje, takie jak Argentyna, Pakistan, Filipiny, Egipt, Botswana i Nigeria, wykorzystały Konwencję jako wzór i opracowały części swojego ustawodawstwa zgodnie z Konwencją o cyberprzestępczości bez formalnego przystąpienia do niej. Ważne jest, aby wiedzieć, że przepisy bardzo rzadko były powielane słowo w słowo, ale zostały dostosowane do wymogów krajów. Wspólne ramy prawne mogłyby wyeliminować przeszkody sądowe, aby ułatwić egzekwowanie prawa w przypadku cyberprzestępczości bez granic. Jednak pełna realizacja wspólnych ram prawnych może nie być możliwa, zwłaszcza jeśli transpozycja postanowień Konwencji do prawa krajowego wymaga włączenia merytorycznych rozszerzeń, które są sprzeczne z zasadami konstytucyjnymi. Na przykład Stany Zjednoczone mogą nie być w stanie kryminalizować wszystkich przestępstw związanych z pornografią dziecięcą, które są określone w Konwencji, w szczególności zakazu wirtualnej pornografii dziecięcej, ze względu na zasady wolności słowa zawarte w Pierwszej Poprawce. Cyberprzestępczość szybko urosła do rangi biznesu, którego wartość może przekroczyć 3 biliony dolarów rocznie. W wielu krajach walka z cyberprzestępczością okazała się trudna bez odpowiednich przepisów i niewystarczających możliwości. Formy współpracy międzynarodowej obejmują:

* Ekstradycja

* Wzajemna pomoc prawna

* Wzajemne uznawanie orzeczeń zagranicznych

* Nieformalna współpraca policji z policją.

Ze względu na niestabilny charakter dowodów elektronicznych współpraca międzynarodowa w zakresie cyberprzestępczości wymaga szybkiego reagowania i możliwości zlecania specjalistycznych działań dochodzeniowych, takich jak ochrona danych komputerowych. Następujące obserwacje UNODC stanowią znaczące globalne wyzwania dla skutecznej współpracy międzynarodowej w zakresie dowodów elektronicznych w sprawach karnych:

• Rozbieżności w zakresie zapisów o współpracy w instrumentach wielostronnych i bilateralnych

• Brak obowiązku czasu reakcji

• Brak porozumienia w sprawie dopuszczalnego bezpośredniego dostępu do danych eksterytorialnych

• Wiele nieformalnych sieci organów ścigania

• Różnice w zabezpieczeniach współpracy

Brak wspólnego podejścia, w tym w ramach obecnych wielostronnych instrumentów dotyczących cyberprzestępczości, oznacza, że wnioski o podjęcie działań, takich jak przyspieszone zabezpieczenie danych poza krajami, które mają międzynarodowe zobowiązania do zapewnienia takiego obiektu i udostępnienia go na żądanie, mogą nie być łatwo realizowane . Dlatego globalna współpraca jest nie tylko potrzebna, ale także kluczowa, aby zapewnić lepszą ochronę i mocniejsze regulacje, ponieważ cyberprzestępcy ukryli się w lukach prawnych w krajach o mniejszej liczbie regulacji.

BADANIE UNODC

Współpraca międzynarodowa

Według UNODC, Comprehensive Study on Cybercrime, podczas gdy wszystkie kraje w Europie uważają, że przepisy krajowe zapewniają wystarczające ramy dla kryminalizacji i ścigania eksterytorialnych aktów cyberprzestępczości, około jedna trzecia do ponad połowy krajów w innych regionach świata raport niewystarczające ramy.

INSTRUMENTY I PROCEDURY DOCHODZENIOWE

Dochodzenie i ściganie cyberprzestępczości stawia przed organami ścigania szereg wyzwań. Niezbędne jest nie tylko przygotowanie odpowiednich i skutecznych aktów prawnych, ale także edukowanie osób zaangażowanych w walkę z cyberprzestępczością. Potrzeba przeszkolonych śledczych i prokuratorów, którzy są zaznajomieni ze źródłami dowodów cyfrowych, staje się coraz bardziej krytyczna, ponieważ czyny przestępcze przechodzą z domen fizycznych do cyfrowych. Aby skutecznie sprostać rygorom śledztwa dotyczącego cyberprzestępczości, śledczy potrzebują szeregu następujących umiejętności w środowisku rzeczywistym i wirtualnym.

Zestawy umiejętności kryminalistyki cyfrowej

Umiejętność: Kompetencja

Badania : Szybkie wyszukiwanie informacji w domenie publicznej i materiałów referencyjnych przechowywanych w sieci korporacyjnej. Możliwość uzyskania wglądu poprzez triangulację informacji z różnych źródeł, które są niedostępne za pośrednictwem publicznych wyszukiwarek.

Świadomość : Czujność w utrzymaniu świadomości zmian w dziedzinie bezpieczeństwa informacji.

Ciągłość dowodów: ścisła zgodność z ustalonymi procesami wykazania łańcucha dowodowego podczas przetwarzania informacji przechowywanych elektronicznie.

Obrazowanie kryminalistyczne : Stosowana wiedza na temat technik przechowywania danych, które wykorzystują zarówno fizyczne, jak i logiczne metody do kryminalistycznego pozyskiwania danych i weryfikacji źródeł informacji.

Architektura sieci: Praktyczne zrozumienie modelu Open System Interconnection (OSI) i funkcji technologii komunikacyjnych w przechowywaniu i transmisji danych, takich jak protokoły sieciowe, adresy kontroli dostępu do mediów (MAC), zapory ogniowe, routery, serwery proxy, centra danych , aplikacje online, usługi w chmurze, aplikacje oparte na hoście, nadmiarowa macierz niezależnych dysków (RAID), klastry, serwery wirtualne i tryby uwierzytelniania wieloskładnikowego.

Sprzęt: Stosowana wiedza na temat komponentów i urządzeń peryferyjnych podłączonych do systemów informatycznych, takich jak dyski twarde, dyski półprzewodnikowe (SSD), pamięć o dostępie swobodnym (RAM), podstawowy system wejściowy i wyjściowy (BIOS), karty interfejsu sieciowego (NIC), chipsety, i pamięci flash.

Systemy plików: stosowana wiedza na temat różnych atrybutów systemu plików, takich jak FAT, FAT32, exFAT, NTFS, HFS+, XFS, Ext2, Ext3, Ext4 i UFS.

Analiza danych strukturalnych : pobieranie i interpretacja informacji o uniwersalnym formacie, takich jak stałe wpisy pól wewnątrz rekordów, a także osadzone informacje związane z systemami operacyjnymi, relacyjnymi bazami danych, arkuszami kalkulacyjnymi, rejestrami, historią internetową, dziennikami bezpieczeństwa i systemowymi oraz zaszyfrowanymi systemami plików.

Analiza danych nieustrukturyzowanych : Interpretacja wartości związanych z odłączonymi plikami przechowywanymi w różnych systemach plików, takich jak zdjęcia cyfrowe, obrazy graficzne, filmy, dane strumieniowe, strony internetowe, pliki PDF, PowerPoint, dane e-mail, wpisy na blogach, wiki i dokumenty tekstowe.

Analiza danych częściowo ustrukturyzowanych : wyodrębnianie tagów, metadanych lub innych typów znaczników tożsamości istniejących w odłączonych plikach, w tym informacji wskazujących na autorstwo, numer wersji, twórcę, nadawcę, odbiorcę, datę i godzinę, współrzędne GPS, słowa kluczowe i oprogramowanie układowe wersja. Działanie to obejmuje również analizę danych relacyjnych w plikach powiązanych z odłączonymi plikami, takimi jak XML i inne języki znaczników.

Inżynieria odwrotna: funkcjonalne zrozumienie mechaniki tworzenia oprogramowania, zdalnej administracji i rozprzestrzeniania się złośliwego oprogramowania.

Programowanie i pisanie skryptów : Znajomość kodowania w językach takich jak C, C++, C#, Perl, Delphi, Html, .NET, ASP, Python, Java, JavaScript, Ruby, Bash Scripting, VBScript, PowerShell, Unix/Linux, EnScript.

Wirtualizacja : stosowana wiedza na temat budowania, konfigurowania i wdrażania maszyn wirtualnych.

Raportowanie techniczne : Doświadczenie w tworzeniu bardzo szczegółowych raportów szczegółowo opisujących wewnętrzne działanie technologii informacyjno-komunikacyjnych, integralność plików, autentyczność informacji i przepływ danych.

KOMUNIKACJA ANONIMOWA

Ustalenie pochodzenia komunikacji jest kluczowym elementem dochodzenia w sprawie cyberprzestępczości. Rozproszony charakter sieci i dostępność niektórych usług internetowych, które powodują niepewność pochodzenia, utrudniają identyfikację przestępców. Globalny system informacyjny jest bezpłatny, więc nie ma żadnych dodatkowych wymagań, zanim użytkownik będzie mógł się zalogować, aby połączyć się z dowolnym miejscem i kimkolwiek na całym świecie. Nie ma łatwych sposobów dokładnego określenia, kto co robi i gdzie znajduje się użytkownik Internetu w dowolnym momencie. Na przykład przestępcy mogą ukrywać swoją tożsamość za pomocą fałszywych adresów e-mail. Możliwość anonimowej komunikacji może być albo produktem ubocznym usługi, albo oferowana w celu uniknięcia niedogodności dla użytkownika. Według ITU przykładami takich usług, które można nawet łączyć, są:

• Publiczne terminale internetowe (np. na terminalach lotniskowych lub w kafejkach internetowych);

• Urządzenia do translacji adresów sieciowych (NAT) i wirtualne sieci prywatne (VPN);

• Sieci bezprzewodowe;

• Usługi mobilne na kartę, które nie wymagają rejestracji;

• Pojemność pamięci dla stron domowych oferowanych bez rejestracji;

• Anonimowe serwery komunikacyjne oraz

• Anonimowi odbiorcy e-maili

Nieograniczona wolność informacji i komunikacji umożliwia cyberprzestępcom ukrycie swojej tożsamości za pomocą różnych gadżetów telekomunikacyjnych (np. Psiphon, Cebulkowy router), aby uniemożliwić śledzenie adresu internetowego protokołu internetowego dowolnego użytkownika. Ponieważ technologie cyfrowe umożliwiają ludziom ukrycie swojej tożsamości, trudno jest z całą pewnością stwierdzić, kto korzystał z komputera, z którego pochodziła nielegalna komunikacja. Ten problem jest bardziej powszechny w środowiskach biznesowych, w których wiele osób może mieć dostęp do komputera osobistego i gdzie hasła są znane lub współdzielone, niż w prywatnych domach, gdzie często można założyć, kim była dana osoba i kto korzystał z komputera na podstawie poszlak . W związku z tym prowadzenie dochodzeń i ściganie cyberprzestępczości wymaga narzędzi i instrumentów specyficznych dla internetu, które umożliwiają właściwym organom prowadzenie dochodzeń w odpowiedni i skuteczny sposób. Instrumenty te mogą być takie same, jak te wykorzystywane w tradycyjnych śledztwach terrorystycznych niezwiązanych z technologią komputerową. Jednak w coraz większej liczbie spraw związanych z Internetem tradycyjne instrumenty dochodzeniowe nie wystarczają do zidentyfikowania sprawcy. Problemy z identyfikacją przestępców są czasami rozwiązywane za pomocą tradycyjnych technik śledczych, takich jak nadzór wideo i podsłuchy. Jednak korzystanie z natrętnego nadzoru lub podsłuchu nie zawsze jest skuteczne, ponieważ należy zwrócić uwagę na kwestie praw człowieka i przywilejów prawnych. Dlatego konieczne są nowe rozwiązania techniczne wraz z powiązanymi instrumentami prawnymi

TECHNOLOGIA SZYFROWANIA

Dostępność i wykorzystanie technologii szyfrowania przez przestępców stanowi wyzwanie dla organów ścigania. Szyfrowanie to technika przekształcania zwykłego tekstu w format zaciemniony za pomocą algorytmu. Podobnie jak anonimowość, szyfrowanie nie jest niczym nowym, ale technologia komputerowa zmieniła dziedzinę, która może skomplikować dochodzenie w sprawie cyberprzestępczości. Obecne oprogramowanie szyfrujące znacznie wykracza poza szyfrowanie pojedynczych plików. Na przykład systemy operacyjne Microsoftu umożliwiają szyfrowanie całego dysku twardego. Ponieważ użytkownicy mogą łatwo zainstalować oprogramowanie szyfrujące, przestępcy mogą również utrudniać analizę danych treści przy użyciu tej samej technologii. Techniki można łączyć, takie jak steganografia, która idzie o krok dalej w kryptografii, ukrywając zaszyfrowaną wiadomość, aby nikt nie podejrzewał, że istnieje. Praktyka ukrywania pliku, wiadomości, obrazu lub wideo w innym pliku, wiadomości, obrazie lub wideo utrudnia organom śledczym odróżnienie nieszkodliwej wymiany zdjęć z wakacji od wymiany zdjęć z zaszyfrowanymi ukrytymi wiadomościami. Ponadto dostępne są różne produkty programowe, które umożliwiają użytkownikom skuteczną ochronę plików oraz procesów przesyłania danych przed nieautoryzowanym dostępem. Jeśli przestępcy skorzystali z takiego produktu, a organy prowadzące dochodzenie nie mają dostępu do klucza użytego do zaszyfrowania plików, wymagane odszyfrowanie może zająć dużo czasu. Chociaż niektórzy eksperci informatyki śledczej uważają, że ta funkcja im nie zagraża, powszechna dostępność tej technologii dla każdego użytkownika może spowodować większe wykorzystanie szyfrowania. Dostępne są również narzędzia do szyfrowania komunikacji, takie jak wiadomości e-mail i telefon, które można wysyłać za pomocą VoIP. Przestępcy mogą chronić rozmowy głosowe przed przechwyceniem za pomocą szyfrowanej technologii VoIP. Według ITU różne podejścia prawne do rozwiązania problemu, gdzie problem jest obecnie dyskutowany, w tym potencjalne zobowiązania twórców oprogramowania do instalowania tylnych drzwi dla organów ścigania, ograniczenia długości

klucza oraz obowiązki ujawniania kluczy w przypadku dochodzeń kryminalnych. Jednak nie ma jeszcze powszechnie akceptowanego międzynarodowego podejścia do rozwiązania tego tematu. Ponadto istnieją pewne obawy zgłaszane przez przeciwników. Na przykład ograniczenia długości klucza nie tylko umożliwiają śledczym złamanie szyfrowania, ale także ekonomiczni szpiedzy mogą potencjalnie uzyskać dostęp do zaszyfrowanych informacji biznesowych. Obowiązek opracowania systemu depozytowego klucza/procedury odzyskiwania klucza może nie być skutecznym rozwiązaniem, ponieważ przestępcy mogliby opracować swoje oprogramowanie szyfrujące, które nie wymaga przedłożenia klucza organowi w celu obejścia przepisów. Ważne jest również, aby wiedzieć, że podczas gdy przepisy krajowe mogą wymagać od firm działających w danej jurysdykcji udzielania władzom dostępu do danych przechowywanych na ich lokalnych serwerach, ustawodawstwo nie może zmusić firm zagranicznych, które nie posiadają kluczy do urządzeń konsumenckich, do ich tworzenia. W odpowiedzi na rosnącą presję ze strony konsumentów i społeczności międzynarodowej (Biuro Wysokiego Komisarza Narodów Zjednoczonych ds. Praw Człowieka), międzynarodowe korporacje, takie jak Apple i Google, integrują technologię szyfrowania nowej generacji w smartfonach, która jest domyślnie bezpieczna, co zabrania dostępu do zawartości telefonu osobom innym niż właściciel, uniemożliwiając odczytanie danych zarówno złodziejom telefonów, jak i policji. W USA federalne organy ścigania twierdzą, że utrudnia to ściganie zachowań przestępczych, podczas gdy zwolennicy wolności obywatelskich postrzegają to jako zwycięstwo w ochronie prywatności danych użytkowników. Posunięcia podkreślają ciągłe wyzwanie dla organów ścigania w reagowaniu na nowe technologie tworzące przeszkody w monitorowaniu komunikacji. Korzystając z technologii szyfrowania i środków anonimowej komunikacji, komunikujące się strony mogą jeszcze bardziej utrudnić identyfikację i monitorowanie komunikacji przestępczej. Może to łatwo doprowadzić do sytuacji, w której prawie wszystkie komunikaty są odporne na zgodne z prawem przechwycenie.

BADANIE UNODC

Sprawiedliwość karna

Według UNODC, Comprehensive Study on Cybercrime, połowa krajów informuje, że podejrzani korzystają z szyfrowania, co utrudnia dostęp do tego rodzaju dowodów bez klucza deszyfrującego. W większości krajów zadanie analizy dowodów elektronicznych spoczywa na organach ścigania. Prokuratorzy muszą jednak przeglądać i rozumieć dowody elektroniczne, aby zbudować sprawę na rozprawie. Wszystkie kraje w Afryce i jedna trzecia krajów w innych regionach zgłosiły niewystarczające zasoby, aby prokuratorzy mogli to zrobić. Umiejętności obsługi komputera prokuratora są zazwyczaj niższe niż śledczych. Na całym świecie około 65% krajów, które udzieliły odpowiedzi, zgłasza jakąś formę specjalizacji prokuratorskiej w cyberprzestępczości. Tylko 10% krajów zgłasza wyspecjalizowane usługi sądowe. Zdecydowana większość spraw dotyczących cyberprzestępczości jest rozpatrywana przez niewyspecjalizowanych sędziów, którzy w 40% krajów odpowiadających nie przechodzą żadnego szkolenia związanego z cyberprzestępczością. Szkolenie sądowe z zakresu prawa o cyberprzestępczości, gromadzenie dowodów oraz podstawowa i zaawansowana wiedza komputerowa stanowi szczególny priorytet.

CHARAKTER DOWODÓW

Ze względu na coraz większą integrację technologii komputerowej z codziennym życiem ludzi, dowody cyfrowe stają się ważnym źródłem dowodów nawet w tradycyjnym dochodzeniu. Jednym z przykładów jest proces o morderstwo w USA, w którym zapisy zapytań wyszukiwarek przechowywane na komputerze podejrzanego zostały wykorzystane do udowodnienia, że przed morderstwem podejrzany intensywnie korzystał z wyszukiwarek w celu znalezienia informacji o niewykrywalnych truciznach. Ponadto rośnie liczba dokumentów cyfrowych ze względu na niskie koszty w porównaniu do

przechowywania dokumentów fizycznych. Cyfryzacja i pojawiające się zastosowanie technologii informacyjno-komunikacyjnych mają ogromny wpływ na procedury gromadzenia dowodów i wykorzystanie w sądzie, gdzie dowody cyfrowe zostały wprowadzone jako nowe źródło dowodów. Obsługa dowodów cyfrowych wymaga określonych procedur w celu zachowania integralności dowodów cyfrowych, ponieważ dane cyfrowe są bardzo delikatne i można je łatwo usunąć lub zmodyfikować. Na przykład informacje przechowywane w pamięci RAM pamięci systemowej są automatycznie usuwane po zamknięciu systemu. W tym przypadku wymagane są specjalne techniki konserwacji. W niektórych przypadkach, gdy dane są przechowywane w pamięci tymczasowej, technika zbierania dowodów może różnić się od tradycyjnego procesu zbierania dowodów cyfrowych. Autentyczność dowodów cyfrowych jest często kwestionowana w przypadku wielu użytkowników komputera lub urządzenia i braku kontroli bezpieczeństwa (np. uwierzytelnianie, szyfrowanie, oprogramowanie antywirusowe, zapora itp.). Rekordy przechowywane i generowane komputerowo mogą zostać uszkodzone, zmanipulowane lub zmienione po ich utworzeniu. Jakość procesów stosowanych w celu zachowania integralności dowodu cyfrowego, od momentu powstania do momentu wprowadzenia go w sądzie, musi być wykazana przez rzecznika dowodu, aby uzasadnić jego wiarygodność i wiarygodność. Można to osiągnąć poprzez stosowanie powszechnie akceptowanej technologii, standardów, procedur i obsługi wyłącznie przez wykwalifikowanych ekspertów, a także stosowanie specyficznych metod, takich jak suma kontrolna, algorytm mieszający i podpisy cyfrowe. Jednak metody te mogą być kosztowne i nie mogą całkowicie wyeliminować ryzyka naprzemiennego. Nowy rozwój może mieć również wpływ na zakres dowodów cyfrowych. Na przykład śledczy zwykli skupiać się na lokalach podejrzanych podczas wyszukiwania danych komputerowych. Obecnie przetwarzanie w chmurze umożliwia przechowywanie informacji cyfrowych za granicą i dostęp do nich można uzyskać tylko zdalnie. Ponadto ciągły wzrost liczby urządzeń elektronicznych i pojemności przechowywania archiwów wkrótce osiągnie punkt krytyczny w zakresie cyfrowej analizy kryminalistycznej i dochodzeń. Ilość danych przechowywanych w formacie cyfrowym stale rośnie, co podkreśla wyzwania logistyczne takich badań. Co więcej, popularność przetwarzania w chmurze stanowi wyzwanie dla transgranicznych kwestii dochodzeniowych i prywatności, ponieważ przepisy krajowe są z natury lokalne, a chmura jest z natury globalna. Na przykład, gdy dostawcy usług w chmurze prowadzą działalność obejmującą wiele krajów, dane dla poszczególnych użytkowników chmury mogą być rozproszone geograficznie i potencjalnie łączone z danymi od innych użytkowników (tj. wielodostępność) w zależności od wdrożonego modelu wdrażania chmury. Mogłoby to znacznie utrudnić badanie miejsca przestępstwa i rekonstrukcję zdarzenia. Utrzymanie ciągłości dowodów może być trudne ponieważ zarówno przechowywane, jak i przesyłane dane mogą być pobierane z różnych punktów pochodzenia w ramach infrastruktury przetwarzania w chmurze (tj. transgraniczny przepływ danych, rozproszone systemy plików, tworzenie kopii zapasowych danych oraz replikacja/synchronizacja itp.), co wpływa na przepisy prawne regulujące dostęp do danych i ujawnienie. Wiele dostępnych na rynku narzędzi kryminalistycznych jest kosztownych, niezwykle skomplikowanych w obsłudze i wymaga intensywnego szkolenia w celu ich efektywnego wykorzystania. Badacze potrzebują nowych narzędzi i procesów, które są w stanie zlokalizować i odzyskać wystarczające dowody z dużych zbiorów danych.

BADANIE UNODC

Dowody elektroniczne

Według UNODC, Comprehensive Study on Cybercrime, wiele krajów odpowiadających we wszystkich regionach odnotowuje niewystarczającą liczbę ekspertów kryminalistycznych, różnice między zdolnościami na poziomie federalnym i stanowym, brak narzędzi kryminalistycznych i zaległości z powodu przytłaczających ilości danych do analizy. Ponad 60% krajów, które udzieliły odpowiedzi, nie

dokonuje prawnego rozróżnienia między dowodami elektronicznymi a dowodami fizycznymi. Chociaż podejścia są różne, wiele krajów uważa tę dobrą praktykę, ponieważ zapewnia sprawiedliwą dopuszczalność wraz ze wszystkimi innymi rodzajami dowodów. Wiele krajów poza Europą w ogóle nie dopuszcza dowodów elektronicznych, co sprawia, że ściganie cyberprzestępczości i wszelkich innych przestępstw potwierdzonych informacjami elektronicznymi jest niewykonalne. Podczas gdy kraje na ogół nie mają odrębnych zasad dowodowych dotyczących dowodów elektronicznych, niektóre z nich odwoływały się do zasad, takich jak: zasada najlepszego dowodu, istotność dowodów, zasada zasłyszenia, autentyczność i integralność, z których wszystkie mogą mieć szczególne zastosowanie do dowodów elektronicznych

DALSZE ROZWAŻANIE

Wspólnota Wirginii ogłosiła utworzenie ISAO na poziomie stanowym w kwietniu 2015 r., co czyni ją jednym z pierwszych stanów USA, które to zrobiły. Był to również najwcześniejszy stan, w którym wdrożono US NIST Cybersecurity Framework, który w szczególności zachęca do dzielenia się informacjami o zagrożeniach cybernetycznych w celu zwiększenia bezpieczeństwa. Niedawno Virginia utworzyła publiczno-prywatną grupę roboczą z Policją Stanową Wirginii, aby zająć się potencjalnymi cyberatakami na połączone samochody. Grupa robocza składa się z interesariuszy z federalnych i stanowych agencji rządowych, środowisk akademickich i firm zajmujących się cyberbezpieczeństwem z sektora prywatnego. Grupa ma na celu pomóc urzędnikom zrozumieć, jak wykrywać i zapobiegać atakom cybernetycznym na pojazdy i inne urządzenia konsumenckie. Virginia przejęła również inicjatywę we wdrażaniu rozwiązania do analizy zagrożeń od dostawcy rozwiązań z zakresu cyberbezpieczeństwa. Wspólnota posiada ogromną skarbnicę danych osobowych (PII) mieszkańców, w tym akta urodzenia i zgonu, zeznania podatkowe i informacje zdrowotne. W ubiegłym roku urzędnicy państwowi odnotowali wzrost liczby incydentów przypisywanych atakom phishingowym i pracownikom. Aby złagodzić te zagrożenia, Virginia wdrożyła rozwiązanie do analizy zagrożeń, które umożliwia monitorowanie ruchu przychodzącego i wychodzącego pod kątem podejrzanej aktywności i złośliwego oprogramowania. Rozwiązanie pomaga również analitykom bezpieczeństwa bezpiecznie wykonywać i kontrolować zaawansowane złośliwe oprogramowanie, zagrożenia dnia zerowego i zaawansowane ataki trwałego zagrożenia (APT). Ten zjednoczony front przeciwko złośliwym przeciwnikom sprawia, że motto wspólnoty – Sic Semper Tyrannis (Tak zawsze dla tyranów) – jest bardziej odpowiednie niż kiedykolwiek.

BRAK ZAANGAŻOWANIA W PRZYWÓDZTWO

W badaniu prezesi firm z listy Fortune 500 ujawniają, że ich największymi największymi zagrożeniami są tempo zmian technologicznych i cyberbezpieczeństwo. Cyberzagrożenia generują ogromne koszty i wyczerpują zasoby. Według Gemalto Breach Level Index 2015 na całym świecie w 2014 roku skompromitowano miliard rekordów danych. McAfee szacuje, że cyberprzestępczość kosztowała światową gospodarkę ponad 400 miliardów dolarów rocznie. Ponadto szacuje się, że w ciągu pięciu lat na globalnym rynku bezpieczeństwa informacji zabraknie 1,5 miliona specjalistów. Ważne jest, aby kierownictwo przyjęło większą odpowiedzialność za zarządzanie ryzykiem cyberprzestępczości i jego łagodzenie oraz nadało odpowiedni ton na szczycie. Przy tak dużym zagrożeniu kadra kierownicza i zarządy wyższego szczebla nadal niechętnie podchodzą do kwestii cyberbezpieczeństwa. Chociaż przyczyny różnią się w zależności od organizacji, EY zidentyfikował następujące najważniejsze przeszkody. Odpowiedzialność za usuwanie luk w cyberprzestrzeni zaczyna się od góry. Prezesi i zarządy są odpowiedzialne za zapewnienie, że firma zaprojektuje i wdroży skuteczny program cyberbezpieczeństwa. Jednak wiele tablic nie jest wystarczająco proaktywnych wobec cyberzagrożeń. Według PwC, Key Findings from the US State of Cybercrime Survey z 2015 r., prawie połowa zarządów nadal postrzega cyberbezpieczeństwo jako kwestię IT, a nie problem ryzyka dla całego

przedsiębiorstwa. Odpowiedzi w ankiecie pochodziły od ponad 500 dyrektorów amerykańskich firm, organów ścigania i agencji rządowych. Jeden na czterech (26%) respondentów stwierdził, że dyrektor ds. bezpieczeństwa informacji (CISO) lub dyrektor ds. bezpieczeństwa (CSO) przedstawia zarządowi prezentację dotyczącą bezpieczeństwa tylko raz w roku, podczas gdy 30% respondentów stwierdziło, że ich dyrektor ds. bezpieczeństwa przeprowadza kwartalną prezentację dotyczącą bezpieczeństwa . Jednak 28% respondentów stwierdziło, że ich liderzy ds. bezpieczeństwa w ogóle nie robią prezentacji. Krajowe Stowarzyszenie Dyrektorów Korporacyjnych zaleca, aby nadzór nad ryzykiem był funkcją całego zarządu ze względu na kluczowe powiązanie między strategią a ryzykiem w potrzebie zaangażowania całego zarządu. Dlatego trudno było dowiedzieć się, że 30% respondentów stwierdziło, że żaden członek zarządu nie jest zaangażowany w cyberzagrożenia. Tylko 15% respondentów stwierdziło, że komitet ds. audytu jest zaangażowany w cyberzagrożenia, biorąc pod uwagę, że cyberbezpieczeństwo stało się jednym z gorących tematów w programie komitetu audytu w ciągu ostatnich kilku lat. Jednym z wyjaśnień stosunkowo słabego zaangażowania członków komitetu audytu może być brak dogłębnej znajomości zagadnień technicznych. W rezultacie firmy przenoszą odpowiedzialność za nadzór nad cyberbezpieczeństwem na cały zarząd lub specjalne komisje ds. ryzyka. Na podstawie 6337 ankiet ze 115 krajów przeprowadzonych przez PwC Global Economic Crime Survey 2016, jeden na trzech (29%) respondentów stwierdził, że członkowie jego zarządu nie proszą o informacje dotyczące zdolności organizacji do radzenia sobie z incydentami cybernetycznymi. Tylko 43% respondentów stwierdziło, że omawia incydenty cybernetyczne co miesiąc, co kwartał lub co rok, biorąc pod uwagę, że cyberzagrożenia były największym wyzwaniem dla dyrektorów generalnych, o czym świadczą liczne badania i ankiety. Podobnie jak w przypadku najlepszych praktyk w zakresie bezpieczeństwa cybernetycznego, zarządy powinny uwzględniać cyberprzestępczość w swojej rutynowej ocenie ryzyka, przekazywać plan w górę, w dół i ponad podziałami organizacyjnymi oraz omówić z działem IT, w którym momencie zarząd powinien zostać ostrzeżony o naruszeniu. Podsumowując, wyniki te wskazują, że osoby najwyższego szczebla w organizacjach nie kładą wystarczającego nacisku na znaczenie zarządzania realnymi zagrożeniami, jakie oszustwa cyberprzestępcze stanowią dla ich organizacji

Przeszkody związane z cyberbezpieczeństwem dla kadry kierowniczej i zarządów

* Cyberbezpieczeństwo to tylko jedna z wielu palących kwestii wymagających zaangażowania na poziomie zarządu, szczególnie w czasach ciągłej niestabilności gospodarczej.

* Cyberbezpieczeństwo jest tradycyjnie postrzegane jako kwestia IT, która koncentruje się na ochronie systemów informatycznych przetwarzających i przechowujących informacje, a nie na strategicznej wartości samych informacji.

* Cyberbezpieczeństwo jest postrzegane jako poważny problem tylko w wybranych sektorach, takich jak wojsko czy usługi finansowe. Ale jeśli Twój sektor opiera się na danych cyfrowych, aby działać i konkurować, Twoje systemy informacyjne i informatyczne są warte odpowiedniego zarządzania ryzykiem.

* W przeciwieństwie do wielu rodzajów ryzyka organizacyjnego, zagrożenia cybernetyczne są trudne do przewidzenia, co utrudnia ocenę ryzyka i potencjalnego wpływu. Starsi liderzy mogą czuć, że brakuje im wiedzy niezbędnej do podejmowania decyzji dotyczących całego przedsiębiorstwa lub mogą obawiać się zbytniego angażowania się w procesy techniczne.

* W obliczu konkurujących żądań dotyczących ograniczonych zasobów kadrze kierowniczej może być trudno inwestować pieniądze, ludzi i czas w nieznane i nieprzewidywalne, a nie w wyniki akcjonariuszy lub bardziej oczywiste potrzeby.

* Organizacje przeinwestowały w środki zapobiegawcze kosztem zdolności wykrywania/reagowania.