DLACZEGO CYBERATAKI NABSILAJĄ SIĘ? - EWOLUCJA CYBERATAKÓW

Cyberatak ma miejsce, gdy zagrożenie skutecznie naruszy mechanizmy bezpieczeństwa. Dowody pokazują, że cyberataki stają się coraz bardziej wyrafinowane. Cyberataki nie mogą już być postrzegane jako pojawiające się zagrożenie, ponieważ dziś są one dobrze zakorzenione w przestępczych przedsiębiorstwach, mają znaczący wpływ na codzienną przestępczość i są zawsze obecne. Organizacje są coraz bardziej podatne na zagrożenia bezpieczeństwa cybernetycznego z nowych kierunków i przeciwników. Ataki w formie haktywizmu, szpiegostwa korporacyjnego, zagrożeń wewnętrznych i państw narodowych oraz działalności przestępczej mogą kosztować organizację czasu, zasobów i nieodwracalne szkody dla jej reputacji. Technologia cyfrowa nadal przekształca i zakłóca świat biznesu, odsłaniając organizacji zarówno na szanse, jak i zagrożenia. Dzisiaj problemem nie jest to, czy organizacja zostanie złamana, ale raczej, jak skuteczny będzie atak. Nawet czołowe firmy technologiczne nie są już na nie odporne. Ta lista ofiar obejmuje firmy ochroniarskie, wykonawców obrony i jedne z najjaśniejszych świateł w technologii. Na przykład zgłoszone ofiary cyberataków to Google, Sony, Lockheed Martin i Citibank. Do organizacji można dostać się na wiele sposobów, a cyberprzestępcy mogą znaleźć najbardziej wrażliwe punkty wejścia. Organizacje powinny przyjąć proaktywne podejście, wdrażając dodatkowe bariery i monitory w nie tak oczywistych miejscach, takich jak publiczne strony internetowe, systemy stron trzecich, które łączą się z organizacjami, łączą systemy przemysłowe i chmurę. Zaawansowane technologie prowadzą do powstawania nowych rodzin złośliwego oprogramowania, rosnącej liczby urządzeń, luk w zabezpieczeniach i coraz większych wyzwań związanych z ochroną informacji. Nic dziwnego, że cyberprzestępczość nadal eskaluje jako drugie najczęściej zgłaszane przestępstwo gospodarcze według PwC Global Economic Crime Survey. Około jedna trzecia organizacji (32%) doświadczyła cyberprzestępczości, jak podało ponad 6000 respondentów w globalnej ankiecie PwC. Podczas gdy przywłaszczenie aktywów, przekupstwo i korupcja, oszustwa związane z zakupami i oszustwa księgowe są tradycyjnymi liderami w tej kategorii, cyberprzestępczość stale rośnie od 2011 roku. mieć plan reagowania na incydenty cybernetyczne.

ROZWÓJ CYBERPRZESTĘPCZOŚCI

DEFINICJA I CHARAKTERYSTYKA

Według Biura Narodów Zjednoczonych ds. Narkotyków i Przestępczości (UNODC), z prawie 200 pozycji ustawodawstwa krajowego przytoczonych przez kraje w odpowiedzi na kwestionariusz UNODC Study, mniej niż pięć procent używało słowa „cyberprzestępczość" w tytule lub zakresie przepisów prawnych . Przeciwnie, ustawodawstwo częściej odnosi się do „przestępstw komputerowych", „komunikacji elektronicznej", „technologii informacyjnych" lub „przestępczości high-tech". W praktyce wiele z tych przepisów stworzyło przestępstwa objęte pojęciem cyberprzestępczości, takie jak nieuprawniony dostęp do systemu komputerowego lub ingerencja w system komputerowy lub dane. Większości cyberprzestępczości nie można zaliczyć do jednej kategorii przestępstw. Innymi słowy, sam termin „cyberprzestępczość" niekoniecznie podlega jednej definicji i prawdopodobnie najlepiej można go opisać jako zbiór czynów lub zachowań. Niemniej jednak amerykański Departament Sprawiedliwości-Narodowa Rada ds. Zapobiegania Przestępczości określił podstawowe treści cyberprzestępczości jako:

Wszelka działalność przestępcza z udziałem komputerów i sieci. Może to być oszustwo lub niechciane wiadomości e-mail (spam). Może obejmować odległą kradzież tajemnic rządowych lub korporacyjnych poprzez wtargnięcie przestępcze do zdalnych systemów na całym świecie. Cyberprzestępczość obejmuje wszystko, od pobierania nielegalnych plików muzycznych po kradzież milionów dolarów z internetowych kont bankowych. Cyberprzestępczość obejmuje również przestępstwa niepieniężne, takie jak tworzenie wirusów na innych komputerach lub umieszczanie w Internecie poufnych informacji biznesowych.

Łatwość dostępu i szybki przepływ informacji odróżnia cyberprzestępczość od przestępstw w świecie rzeczywistym. Transformacja przestępczości wraz z wprowadzeniem technologii komputerowych i sieciowych prowadzi do przesunięcia celu z bardziej namacalnych do mniej namacalnych form wartości bogactwa; od rzeczy do pomysłów wyrażonych w źródłach informacji. Cyberprzestrzeń, w której wszystko jest przechowywane i przesyłane cyfrowo, usuwa fizyczne ograniczenia świata rzeczywistego, które rządzą zarówno legalnymi, jak i nielegalnymi działaniami jednostek. To, co wyróżnia cyberprzestępczość, można omówić w trzech głównych kategoriach, takich jak cel, miejsce i anonimowość.

Charakterystyka cyberprzestępczości

Cel cyberprzestępczości:

• Informacje przechowywane i przesyłane cyfrowo, które są niematerialne i łatwe do odtworzenia, zmiany, usunięcia znacznie łatwiejsze, szybsze i bezkosztowe

• Każdy obiekt może jednocześnie istnieć w wielu lokalizacjach. Dzięki temu informacje przechowywane na komputerze w sieci są bardziej podatne na ataki

Miejsce cyberprzestępczości:

• Nie ma państw ani międzynarodowych granic geograficznych. W ciągu sekundy można dotrzeć do dowolnego punktu w cyberprzestrzeni, a pojęcie odległości i fizycznej bliskości traci sens

• Nieodłączne cechy Internetu, które umożliwiają osobom komunikowanie się z tysiącami innych osób jednocześnie

• Może być zautomatyzowany poprzez pomnożenie liczby dyskretnych wykroczeń; łatwo jest dotrzeć do tysięcy ofiar w odległych lokalizacjach w różnych ramach czasowych

Anonimowość : używaj różnych narzędzi i technologii, aby ukryć swoją tożsamość, np. zaszyfrowanej komunikacji, anonimowych wiadomości e-mail lub komputerów zombie.

Poniżej wymieniono 14 czynów, które mogą stanowić cyberprzestępczość, podzielonych na trzy szerokie kategorie: czyny przeciwko poufności, integralności i dostępności danych lub systemów komputerowych, czyny związane z komputerami w celu osiągnięcia korzyści lub szkody osobistej lub finansowej oraz czyny związane z treściami komputerowymi.

Działa przeciwko poufności, integralności i dostępności danych lub systemów komputerowych

• Nielegalny dostęp do systemu komputerowego

• Nielegalny dostęp, przechwytywanie lub pozyskiwanie danych komputerowych

• Nielegalna ingerencja w system komputerowy lub dane komputerowe

• Produkcja, dystrybucja lub posiadanie narzędzi do nadużyć komputerowych

• Naruszenie prywatności lub środków ochrony danych

Działania związane z komputerem w celu osiągnięcia osobistych lub finansowych korzyści lub szkód

• Oszustwa lub fałszerstwa związane z komputerem

• Komputerowe przestępstwa tożsamościowe

• Naruszenia praw autorskich lub znaków towarowych związanych z komputerem

• Wysyłanie lub kontrolowanie wysyłania spamu

• Czyny związane z komputerem powodujące szkodę osobistą

• Związane z komputerem nagabywanie lub „pielęgnowanie" dzieci

Akty dotyczące treści komputerowych

• Czyny związane z komputerem związane z mową nienawiści

• Produkcja, dystrybucja lub posiadanie pornografii dziecięcej związane z komputerem

• Czyny komputerowe wspierające przestępstwa terrorystyczne

POSTĘP OD PRZESTĘPSTW KOMPUTEROWYCH DO CYBERPRZESTĘPCZOŚCI

Technologia komputerowa i internet, podobnie jak inne środki zwiększające możliwości interakcji międzyludzkich, mogą być wykorzystywane do działalności przestępczej. Kryminalne nadużycia technologii informacyjnej i reakcja prawna to kwestie, które były omawiane od czasu wprowadzenia technologii. Czyny przestępcze związane z komputerami, w tym fizyczne uszkodzenie systemów komputerowych i przechowywanych danych; nieuprawnione korzystanie z systemów komputerowych i manipulacja danymi elektronicznymi; oszustwa komputerowe; piractwo komputerowe jest uznawane za przestępstwa kryminalne od lat 60. XX wieku. Chociaż przestępczość komputerowa jest zjawiskiem od dawna znanym w historii, istotną zmianą we współczesnych czasach jest wzrost mocy obliczeniowej komputerów osobistych w zglobalizowanej sieci komunikacyjnej. Rozwój globalnej łączności jest zdecydowanie powiązany z rozwojem współczesnej cyberprzestępczości. Technologia sieciowa stała się czymś więcej niż tylko mnożnikiem siły. Pomysły popełnienia przestępstwa są nie tylko udostępniane na skalę globalną, ale także szybko wdrażane w życie w globalnej sieci. Nowoczesne systemy komputerowe, które teraz wchodzą na rynek, potężne i używane do rozszerzenia działalności przestępczej. Istnieją różne terminy odnoszące się do wiktymizacji komputerowej i internetowej, takich jak cyberprzestępczość, przestępstwa komputerowe i przestępstwa informatyczne. Chociaż terminy „cyberprzestępczość" lub „przestępczość komputerowa" stały się terminami powszechnie używanymi, słowa te można stosować zamiennie w odniesieniu do przestępstw popełnianych przy użyciu komputerów, sieci i innych narzędzi technologicznych. „Przestępczość komputerowa" była powszechnie stosowana na wczesnym etapie technologii komputerowej i sieciowej, zanim powstał internet. Termin „cyberprzestępczość" jest obecnie najpopularniejszym terminem odnoszącym się do przestępstw, które dotyczą nie tylko komputerów, ale także sieci komputerowej (ogólnie Internetu). Cyberprzestrzeń, globalnie połączona cyfrowa infrastruktura informacyjno-komunikacyjna, wspiera niemal każdy aspekt współczesnego społeczeństwa i zapewnia kluczowe wsparcie dla gospodarki, infrastruktury cywilnej, bezpieczeństwa publicznego i bezpieczeństwa narodowego. Ewolucja technologii przekształciła światową gospodarkę i połączyli ludzi w niewyobrażalny sposób. Tymczasem zagrożenia związane z cyberbezpieczeństwem stanowią jedne z najpoważniejszych wyzwań gospodarczych i bezpieczeństwa narodowego XXI wieku. Architektura infrastruktury cyfrowej opierała się bardziej na interoperacyjności i wydajności niż na bezpieczeństwie. Cyberataki i związane z nimi incydenty wkraczają w światowy krajobraz zagrożeń jako jedno z najbardziej prawdopodobnych i potencjalnie najbardziej znaczących zagrożeń. Według Międzynarodowego Związku Telekomunikacyjnego (ITU) w ciągu ostatnich 50 lat różne rozwiązania zostały wdrożone na poziomie krajowym i regionalnym. Jednak temat nadal pozostaje trudny ze względu na ciągły rozwój techniczny, a także zmieniające się metody i sposoby popełniania wykroczeń. Poniższa tabela przedstawia postęp od przestępczości komputerowej do cyberprzestępczości opisany przez ITU.

Rozwój przestępczości komputerowej i cyberprzestępczości

Lata 60.:

* Wprowadzenie systemów komputerowych opartych na tranzystorach, które były mniejsze i tańsze niż maszyny oparte na lampach próżniowych, spowodowało wzrost wykorzystania technologii komputerowej.

* Przestępstwa skoncentrowane na fizycznym uszkodzeniu systemów komputerowych i przechowywanych danych. Takie incydenty zostały zgłoszone na przykład w Kanadzie, gdzie w 1969 r. zamieszki studenckie spowodowały pożar, który zniszczył dane komputerowe przechowywane na uczelni.

* W połowie lat 60. Stany Zjednoczone rozpoczęły debatę na temat utworzenia centralnego organu przechowującego dane dla wszystkich ministerstw. W tym kontekście omówiono możliwe nadużycia baz danych w celach przestępczych i związane z tym zagrożenia dla prywatności.

Lata 70.:

* Przy spadających cenach technologia komputerowa była coraz szerzej wykorzystywana w administracji i biznesie oraz przez społeczeństwo.

* Nastąpiło przejście od tradycyjnych przestępstw przeciwko mieniu przeciwko systemom komputerowym, które zdominowały lata 60., do nowych form przestępczości.

* Rozpoznano nowe formy przestępczości komputerowej, w tym nielegalne korzystanie z systemów komputerowych i manipulację danymi elektronicznymi.

* Przejście od transakcji ręcznych do obsługiwanych komputerowo doprowadziło do kolejnej nowej formy przestępczości, oszustw komputerowych.

* Wielomilionowe straty zostały spowodowane oszustwami komputerowymi.

* Prawdziwym wyzwaniem były w szczególności oszustwa komputerowe, a prawo

organy ścigania badały coraz więcej spraw. Ponieważ stosowanie istniejących przepisów w sprawach o przestępstwa komputerowe prowadziło do trudności.

Lata 80.:

* Komputery osobiste stawały się coraz bardziej popularne.

* Liczba systemów komputerowych, a tym samym liczba potencjalnych celów dla przestępców, ponownie wzrosła.

* Po raz pierwszy cele obejmowały szeroki zakres infrastruktury krytycznej.

* Rosnące zainteresowanie oprogramowaniem spowodowało pojawienie się pierwszych form piractwa komputerowego i przestępstw związanych z patentami.

* Połączenie systemów komputerowych przyniosło nowe rodzaje przestępstw.

* Sieci umożliwiły przestępcom wejście do systemu komputerowego bez obecności na miejscu przestępstwa.

* Możliwość rozpowszechniania oprogramowania za pośrednictwem sieci umożliwiła przestępcom rozpowszechnianie złośliwego oprogramowania i wykrywano coraz więcej wirusów komputerowych.

* Kraje rozpoczęły proces aktualizacji swojego ustawodawstwa, aby sprostać wymaganiom zmieniającego się środowiska przestępczego.

Lata 90. :

* Wprowadzenie interfejsu graficznego („World Wide Web”), po którym nastąpił gwałtowny wzrost liczby internautów, postawił przed sobą nowe wyzwania.

* Informacje legalnie udostępniane w jednym kraju były dostępne na całym świecie, nawet w krajach, w których publikacja takich informacji była kryminalna.

* Dystrybucja pornografii dziecięcej przeszła od fizycznej wymiany książek i taśm do dystrybucji online za pośrednictwem stron internetowych i usług internetowych.

* Internet zamienił przestępstwa elektroniczne w przestępczość międzynarodową. Jak w rezultacie społeczność międzynarodowa bardziej intensywnie zajęła się tym problemem

XXI wiek:

* Pierwsza dekada nowego tysiąclecia była zdominowana przez nowe, wysoce wyrafinowane metody popełniania przestępstw, takie jak „phishing” i „ataki botnetowe”.

* Pojawiające się zastosowania technologii, które są trudniejsze do obsługi i zbadania przez organy ścigania, takie jak „komunikacja Voice-over-IP (VoIP)” i „przetwarzanie w chmurze”.

* Gdy przestępcy mogli zautomatyzować ataki, wzrosła liczba wykroczeń.

* Kraje oraz organizacje regionalne i międzynarodowe zareagowały na rosnące wyzwania i nadały odpowiedzi na cyberprzestępczość wysoki priorytet.

RODZAJE CYBERPRZESTĘPCZOŚCI

Cyberprzestępczość można podzielić na dwie kategorie; brutalne i pokojowe cyberprzestępstwa. Większość cyberprzestępstw to przestępstwa bez użycia przemocy, ponieważ interakcja przebiega bez kontaktu fizycznego. Brutalne cyberprzestępstwa stanowią fizyczne zagrożenie dla jakiejś osoby lub osób, w tym terroryzm, prześladowanie, zastraszanie i pornografia dziecięca. Cyberprzestępstwa bez użycia przemocy, takie jak szpiegostwo korporacyjne i kradzież tożsamości, nie powodują żadnych fizycznych szkód u osób, ale powodują straty finansowe, zaburzenia psychiczne i szkody społeczne. Poniższa tabela przedstawia rodzaje cyberprzestępczości wraz z różnymi formami.

Cyberprzestępstwa

Brutalna cyberprzestępczość:

- Cyberterroryzm

- Pornografia dziecięca

- Cyberprześladowanie

- Cyberprzemoc

Cyberprzestępczość bez użycia przemocy

Cyberkradzież

- Złamanie biznesowej poczty e-mail

- Narażenie konta e-mail

- Tożsamość

- Defraudacja

- Bezprawne przywłaszczenie

- Szpiegostwo korporacyjne

- Plagiat

- Piractwo

Cyberoszustwo

- Oprogramowanie ransomware

- Wyłudzanie informacji

- Spamowanie

Hacking

Niszcząca cyberprzestępczość

- Cyber wandalizm

- Wirusy

Inne cyberprzestępstwa bez użycia przemocy

- Cyber prostytucja

- Hazard online

- Handel online

- Internetowa sprzedaż leków

BRUTALNE CYBERPRZESTĘPCZOŚCI

CYBERTERRORYZM/CYBERWOJNA

Gwałtowny wzrost aktywności w Internecie doprowadził do cyberterroryzmu; konwergencja cyberprzestrzeni i terroryzmu. Według ITU w latach 90. wykorzystanie sieci przez organizacje terrorystyczne koncentrowało się na atakach sieciowych na infrastrukturę krytyczną, taką jak transport i zaopatrzenie w energię („cyberterroryzm") oraz wykorzystanie technologii informatycznych w konfliktach zbrojnych („cyberwarfare") . Stopień wzajemnych połączeń był niewielki w porównaniu do dzisiejszych czasów. Udane ataki terrorystyczne z wykorzystaniem internetu były możliwe, ale trudno jest ocenić wagę zagrożeń. Sytuacja ta uległa zmianie po atakach z 11 września z powodu wykorzystywania przez terrorystów technologii informacyjno-komunikacyjnych (ICT). Chociaż atak z 11 września nie był atakiem internetowym, internet odegrał rolę w przygotowaniu przestępstwa, ponieważ odkryto różne sposoby wykorzystywania Internetu przez organizacje terrorystyczne. Według ITU terroryści wykorzystują ICT i internet do:

* Propaganda

* Zbieranie informacji

* Przygotowanie ataków w świecie rzeczywistym

* Publikacja materiałów szkoleniowych

* Komunikacja

* Finansowanie terroryzmu

* Ataki na infrastrukturę krytyczną

Po atakach na systemy komputerowe w Estonii w 2007 r. i Gruzji w 2008 r. oraz po odkryciu wirusa komputerowego „Stuxnet", do opisu sytuacji często używano terminu cyberwojna. Cyberwojnę definiuje się jako:

Działania państwa narodowego mające na celu penetrację komputerów lub sieci innego narodu w celu spowodowania szkód lub zakłóceń. Działania obejmują również podmioty niepaństwowe, takie jak grupy terrorystyczne, firmy, polityczne lub ideologiczne grupy ekstremistyczne, haktywiści i międzynarodowe organizacje przestępcze.

Przykłady cyberwojny napędzanej motywacjami politycznymi można znaleźć na całym świecie, w tym:

• W 2009 roku Izrael rozpoczął atak o nazwie Operacja „Płynny ołów" przeciwko Autonomii Palestyńskiej. Walki między izraelskimi siłami obronnymi a Hamasem obejmowały cyberataki na rządowe strony internetowe i media oraz angażowały zarówno podmioty państwowe, jak i niepaństwowe.

• W latach 2010-2011 Stuxnet został uruchomiony z zamiarem zniszczenia firm energetycznych i obiektów jądrowych w Iranie i innych krajach. Program podobno zniszczył jedną piątą irańskich wirówek jądrowych.

• W 2011 r. jaśminowa rewolucja w Tunezji, która doprowadziła do obalenia skorumpowanego rządu, obejmowała brutalne zabezpieczenia oraz hakowanie nazw użytkowników i haseł dla całej populacji online Tunezji przez AMMAR, rządowego dostawcę usług internetowych (ISP).

• W 2013 r. BND zaobserwowało do pięciu ataków dziennie na władze rządowe, jednak głównie z Chin. Skradzione informacje mogą posłużyć jako podstawa przyszłych ataków sabotażowych na producentów broni, firmy telekomunikacyjne oraz agencje rządowe i wojskowe.

• W 2015 r. na Ukrainie miał miejsce pierwszy znany udany cyberatak na sieć energetyczną, który spowodował tymczasowe przerwy w dostawie prądu. Cyberatak jest przypisywany rosyjskiej grupie zaawansowanych trwałych zagrożeń o nazwie „Sandworm". Dokonano go podczas trwającej konfrontacji wojskowej.

PRZYKŁAD Z PRAWDZIWEGO ŚWIATA

<u>Spisek w celu przygotowania aktu terrorystycznego</u>

W maju 2012 roku zachodnioeuropejski sąd skazał jednego ze swoich obywateli na pięć lat więzienia za udział w spisku kryminalnym mającym na celu przygotowanie aktu terrorystycznego. Na rozprawie prokuratura przedstawiła dziesiątki odszyfrowanych wiadomości e-mail zawierających treści dżihadystyczne, które zostały między innymi wysłane na stronę internetową prezydenta kraju i śledzone przez członka działającej na całym świecie grupy ekstremistycznej. Nakaz ochrony umożliwił władzom zidentyfikowanie komunikacji między członkami grupy ekstremistycznej a stronami internetowymi ekstremistów, w tym stroną internetową, której celem jest przechowywanie i rozpowszechnianie dokumentów grupy ekstremistycznej, nagrań audio i wideo, oświadczeń watażków

i napastników-samobójców oraz materiałów innych grupy ekstremistyczne. Wskazywało to, że pozwany aktywnie wykonywał między innymi tłumaczenie, szyfrowanie, kompresję i ochronę hasłem materiałów prodżihadystycznych, które następnie umieszczał i rozpowszechniał za pośrednictwem Internetu; oraz podejmowanie konkretnych kroków w celu zapewnienia wsparcia finansowego grupie ekstremistycznej, w tym poprzez próby korzystania z PayPal i innych wirtualnych systemów płatności. Sąd uznał wymagane wystarczające dowody, aby wykazać, że oskarżony udzielił nie tylko wsparcia intelektualnego, ale również bezpośredniego wsparcia logistycznego jasno określonemu planowi terrorystycznemu.

PORNOGRAFIA DZIECIĘCA

Internet stał się głównym kanałem dystrybucji pornografii dziecięcej. Według ITU pornografia dziecięca była głównie transportowana za pośrednictwem usług pocztowych, a udane śledztwa doprowadziły do wykrycia znacznej liczby przestępców do połowy lat 90. XX wieku. Od połowy lat 90. przestępcy coraz częściej korzystają z usług sieciowych do dystrybucji takich materiałów. Uznano wynikające z tego trudności w zakresie wykrywania, badania i ścigania przypadków pornografii dziecięcej. Na przykład stosowanie wyrafinowanych środków anonimowej komunikacji może utrudnić identyfikację sprawcy. Liczba potencjalnych klientów wzrosła dzięki łatwemu dostępowi do Internetu. Ponadto, wraz z przejściem z mediów analogowych na cyfrowe, zgłoszono rosnącą liczbę obrazów z pornografią dziecięcą odkrytych w trakcie śledztw. Organizacje międzynarodowe angażują się w walkę z pornografią dziecięcą w Internecie, podejmując kilka międzynarodowych inicjatyw prawnych, takich jak:

* Konwencja Narodów Zjednoczonych o prawach dziecka z 1989 r.

* Protokół fakultatywny ONZ do Konwencji o prawach dziecka z 2000 r. dotyczący handlu dziećmi, dziecięcej prostytucji i dziecięcej pornografii

* Decyzja ramowa Rady Unii Europejskiej z 2003 r. w sprawie zwalczania seksualnego wykorzystywania dzieci i pornografii dziecięcej

* Konwencja Rady Europy z 2007 r. o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych

* Unia Europejska Parlamentu Europejskiego i Rady z 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej

Niestety, te inicjatywy mające na celu kontrolowanie sieciowej dystrybucji pornografii okazały się mało odstraszające dla sprawców. Internet jest głównym kanałem handlu regularną pornografią, a także pornografią dziecięcą. Dwa kluczowe czynniki w wykorzystywaniu technologii informacyjno-komunikacyjnych do wymiany pornografii dziecięcej stanowią przeszkody w prowadzeniu dochodzeń w sprawie tych przestępstw:

1) Korzystanie z wirtualnych walut i anonimowa płatność

2) Wykorzystanie technologii szyfrowania

CYBERPRZEMOC

Inne brutalne cyberprzestępstwa obejmują wykorzystywanie komunikacji elektronicznej do nękania, zawstydzania, poniżania, grożenia lub wywoływania strachu lub zastraszania jednostki. Na przykład sprawca wysyła obraźliwe, groźne, obraźliwe lub obraźliwe wiadomości lub obrazy lub w inny sposób monitoruje lub ingeruje w samopoczucie emocjonalne lub fizyczne danej osoby. Cyberprzemoc,

rozszerzenie fizycznego dokuczania, wykorzystuje technologię elektroniczną, taką jak telefony komórkowe i komputery, a także narzędzia komunikacyjne, w tym witryny mediów społecznościowych, wiadomości tekstowe, czat i strony internetowe. Przykłady cyberprzemocy obejmują złośliwe wiadomości tekstowe lub e-maile, plotki wysyłane pocztą elektroniczną lub publikowane w serwisach społecznościowych oraz zawstydzające zdjęcia, filmy lub fałszywe profile. Dzieciom, które są ofiarami cybernękania, trudniej jest uciec od tego zachowania, ponieważ:

• Cyberprzemoc może mieć miejsce 24 godziny na dobę, 7 dni w tygodniu

• Wiadomości lub wyobrażenia dotyczące cybernękania można publikować anonimowo i szybko rozpowszechniać wśród szerokiego grona odbiorców

• Usuwanie nieodpowiednich lub nękających wiadomości, tekstów i wyobrażeń może być bardzo trudne po ich opublikowaniu lub wysłaniu

W USA prawie wszystkie stany mają przepisy dotyczące nękania, wiele z nich zawiera przepisy dotyczące cyberprzemocy lub nękania elektronicznego. Chociaż w niektórych stanach pojawiły się przepisy, ich egzekwowanie często pozostawia się w rękach urzędników szkolnych. Dlatego cyberprzemoc często może być traktowana jako sprawa cywilna, a nie karna. Jednak prokuratorzy wykorzystali istniejące przepisy do ścigania osób podejrzanych o cyberprzemoc. Ustawy dotyczące nękania karnego często mogą stanowić podstawę do wniesienia oskarżenia w ciężkich przypadkach. Poważniejsze zarzuty karne zostały wniesione w sprawach, w których przestępstwo spowodowało samobójstwo lub inne tragiczne konsekwencje. Ogólnokrajowy trend zmierza w kierunku większej odpowiedzialności za zastraszanie w ogóle.

CYBERPRZESTĘPSTWA BEZ PRZEMOCY

ZŁAMANIE POCZTY BIZNESOWEJ/WŁAMANIE NA KONCIE E-MAIL

Ewoluujący charakter cyberprzestępczości stanowi wyjątkowy zestaw wyzwań, ponieważ przestępstwa często pokrywają się z granicami jurysdykcji, a sprawcy mogą atakować z dowolnego miejsca na świecie. Na przykład kompromitacja biznesowej poczty e-mail (BEC) jest definiowana jako wyrafinowane oszustwo wymierzone w firmy współpracujące z zagranicznymi dostawcami i/lub firmy, które regularnie wykonują płatności przelewem. Oszustwo polega na kompromitowaniu legalnych firmowych kont e-mail za pomocą socjotechniki lub technik włamań komputerowych w celu przeprowadzenia nieautoryzowanych transferów środków. Oszukańcze przelewy przeszły przez konta w wielu krajach, przy czym znaczna większość podróżuje przez Azję. Oszustwo zaczęło ewoluować w 2013 r., kiedy ofiary wskazały, że konta e-mail dyrektorów generalnych lub dyrektorów finansowych docelowych firm zostały zhakowane lub sfałszowane, a płatności przelewem zostały wysłane do fałszywych lokalizacji. BEC nadal ewoluował, a w 2014 r. firmy będące ofiarami informowały o skompromitowaniu osobistych wiadomości e-mail i wielu fałszywych żądaniach płatności wysyłanych do dostawców zidentyfikowanych na ich liście kontaktów. W 2015 r. ofiary zgłosiły, że kontaktowały się z nimi osoby podające się za prawników lub firmy prawnicze, instruujące je, by dokonywały tajnych lub wrażliwych na czas przelewów. Według FBI, programy BEC spowodowały co najmniej 3,1 mld USD łącznych strat około 22 000 przedsiębiorstw na całym świecie w latach 2014–2016. Od stycznia 2015 r. odnotowano 1300% wzrost zidentyfikowanych strat w wysokości 140 000 USD za oszustwo. FBI zmusiło do wydania ogłoszenia o służbie publicznej, w którym szczegółowo opisano, w jaki sposób działają oszustwa BEC ze względu na potencjalne szkody i skuteczność tych kampanii. Pomimo ogromnego wpływu, jaki wywarły schematy BEC, analiza przepływu ataków jest dość łatwa. Na przykład tematy wiadomości e-mail używane w schematach BEC są proste i niejasne, czasami składające się tylko z jednego słowa, takiego jak:

* Request For

* Transfer

* Request

* Urgent

* Transfer Request

Narażenie konta e-mail (EAC) to siostrzane oszustwo BEC. EAC różni się od BEC tym, że jest skierowany do osób fizycznych lub indywidualnych profesjonalistów, a nie do firm. EAC jest definiowany jako wyrafinowane oszustwo skierowane do ogółu społeczeństwa i profesjonalistów związanych między innymi z instytucjami finansowymi i pożyczkowymi, firmami z branży nieruchomości oraz kancelariami prawnymi.

PRZYKŁAD Z PRAWDZIWEGO ŚWIATA

Naruszenie w zakresie biznesowej poczty e-mail: Infront Consulting Group Inc.

W 2015 r. dyrektor finansowy Infront Consulting Group Inc. z siedzibą w Toronto i Las Vegas otrzymał e-mail, który wydawał się pochodzić od dyrektora generalnego firmy, instruujący ją, aby „przetworzyła płatność w wysokości 169 705 USD". Załączone instrukcje dotyczące przelewu nakazywały dokonanie płatności do domu maklerskiego w Neapolu na Florydzie. Program nie powiódł się tylko dlatego, że dyrektor generalna Infront, przez przypadek, zadzwoniła do dyrektora finansowego, gdy analizowała wniosek. Kiedy zapytała, na co są te pieniądze, prezes powiedział, że nic o tym nie wie. Dalsza analiza wykazała, że e-mail został wysłany z adresu podobnego do adresu firmy, ale brakowało litery „l" w „konsultingu".

KRADZIEŻ TOŻSAMOŚCI

Kradzież tożsamości to jeden z najczęstszych rodzajów cyberprzestępczości. Termin ten jest używany, gdy osoba podaje się za inną osobę w celu stworzenia oszustwa w celu uzyskania korzyści finansowych. Według Centrum zasobów identyfikacji kradzieży istnieją cztery główne typy kradzieży tożsamości przedstawione w poniższej tabeli.

Rodzaje kradzieży tożsamości

Kradzież tożsamości przestępcy : osoba przyłapana na zarzutach kryminalnych będzie podszywać się pod inną osobę, której dane zabezpieczyła poprzez naruszenie danych, phishing lub socjotechnikę.

Kradzież dowodu osobistego : Jest to związane głównie z deklaracjami podatku dochodowego. Przestępca może pracować gdzieś pod nazwiskiem i identyfikacją ofiary. W takim przypadku nie może składać deklaracji podatkowych.

Kradzież tożsamości finansowej: Jest to związane ze złodziejami tożsamości, którzy zaciągają pożyczki na dane ofiary. Ofiara może otrzymać pismo pożyczkodawcy, aby stwierdzić, że nie spłaciła pożyczki, której nie zaciągnęła.

Kradzież legitymacji medycznej : odnosi się do złodziei legitymacji, którzy korzystają ze świadczeń medycznych ofiary w szpitalach i aptekach.

Najczęstszym źródłem kradzieży informacji identyfikacyjnych innych osób są naruszenia danych dotyczące rządowych lub federalnych witryn internetowych. Mogą to być również naruszenia bezpieczeństwa danych lub prywatne witryny internetowe, które zawierają ważne informacje, takie

jak dane karty kredytowej, adres i identyfikatory e-mail itp. Drugą najczęściej stosowaną techniką kradzieży informacji identyfikacyjnych jest phishing. Chociaż większość z nas nie zwraca uwagi na wiadomości e-mail z prośbą o podanie naszych danych osobowych, niektóre ataki phishingowe, takie jak ten określany jako nigeryjskie oszustwa phishingowe, często udaje się wydobyć dane od niczego niepodejrzewających osób, które wpadają w pułapkę przestępców . Następnie istnieje socjotechnika, w ramach której przestępcy zaprzyjaźniają się z ofiarami osobiście lub przez telefon, e-mail lub media społecznościowe. Gdy przestępcy staną się „przyjaciółmi", mogą łatwo uzyskać informacje wykorzystywane do podszywania się pod ofiary. Techniki socjotechniki są najczęściej używane przez indywidualnych napastników, ponieważ brakuje im zasobów lub doświadczenia profesjonalnych zespołów hakerskich, organizacji lub agencji szpiegowskich. Chociaż rodzaje danych, na które kierują się przestępcy, są różne, najistotniejszymi danymi są numery ubezpieczenia społecznego i paszportów, data urodzenia, adresy i numery telefonów oraz hasła. W Stanach Zjednoczonych numer ubezpieczenia społecznego (SSN) jest pojedynczym elementem danych związanych z tożsamością, na który celują przestępcy, ponieważ mogą używać numeru SSN i informacji paszportowych do otwierania kont finansowych, przejmowania istniejących kont finansowych i uzyskiwania kredytu lub zwiększania zadłużenia. Data urodzenia, adres i numer telefonu mogą zostać użyte do popełnienia kradzieży tożsamości tylko wtedy, gdy zostaną połączone z innymi informacjami, takimi jak SSN. Przestępcy mogą łatwo obejść procesy weryfikacji, mając dostęp do dodatkowych informacji (np. data urodzenia, adres). Niepokojące jest to, że takie informacje są dostępne na dużą skalę w Internecie – albo publikowane dobrowolnie w jednym z różnych ustawień związanych z tożsamością, albo w oparciu o wymogi prawne, takie jak nadruk na stronach internetowych. Posiadanie dostępu do haseł do kont pozwala przestępcom wykorzystywać je do własnych celów. Na przykład mogą przejąć konto e-mail, aby wysyłać wiadomości zawierające nielegalne treści. Kradzież tożsamości była poważnym problemem i wciąż narasta. Straty mogą być nie tylko finansowe, ale mogą również obejmować utratę reputacji. Rzeczywista częstość występowania kradzieży tożsamości prawdopodobnie znacznie przekroczy liczbę zgłoszonych przypadków, ponieważ wiele ofiar nie zgłasza takich przestępstw, a instytucje finansowe często nie chcą nagłaśniać złych doświadczeń klientów. Federalna Komisja Handlu ujawnia, że każdego roku tożsamość 9 milionów Amerykanów zostaje skradziona, a od 2005 roku w wyniku ataków na bazy danych firm, organów rządowych, instytucji i organizacji skonfiskowano co najmniej 534 miliony danych osobowych. Gdyby te naruszenia rozprzestrzeniły się równomiernie na 310 milionów mieszkańców USA, tożsamość każdego z nich zostałaby skradziona raz i dwie trzecie razy. Webroot sugeruje następujące siedem kroków, aby zapobiec identyfikacji kradzieży w Internecie:

1) Chroń komputer i smartfon za pomocą silnego, aktualnego oprogramowania zabezpieczającego

2) Naucz się rozpoznawać spam i oszustwa

3) Używaj silnych haseł

4) Monitoruj ocenę kredytową

5) Sprawdź ocenę kredytową

6) Zablokuj zabezpieczenie kredytu

7) Dokonując zakupów korzystaj wyłącznie z renomowanych stron internetowych

PRZYKŁAD Z PRAWDZIWEGO ŚWIATA

Naruszenie danych: Biuro Zarządzania Personelem

W czerwcu 2015 r. amerykańskie Biuro Zarządzania Personelem (OPM) ogłosiło, że było celem naruszenia danych, które dotyczyło rekordów aż czterech milionów osób. Później FBI podało liczbę 18 milionów. Naruszenie danych, które rozpoczęło się w marcu 2014 r., a być może rozpoczęło się wcześniej, zostało zauważone przez OPM w kwietniu 2015 r. Urzędnicy federalni określili je jako jedno z największych naruszeń danych rządowych w historii USA. OPM był wielokrotnie ostrzegany o lukach w zabezpieczeniach i błędach. Raport półroczny Biura Generalnego Inspektora OPM z marca 2015 r. dla Kongresu ostrzegał przed „utrzymującymi się niedociągnięciami w programie bezpieczeństwa systemów informatycznych OPM", w tym „niekompletnymi pakietami autoryzacji bezpieczeństwa, słabościami w testowaniu mechanizmów kontroli bezpieczeństwa informacji oraz niedokładnymi planami działania i kamieniami milowymi ". Informacje, których dotyczy naruszenie, obejmowały informacje umożliwiające identyfikację, takie jak numery ubezpieczenia społecznego, a także nazwiska, daty i miejsca urodzenia oraz adresy. Włamanie sięgnęło głębiej, niż początkowo sądzono i prawdopodobnie polegało na kradzieży szczegółowych informacji związanych z poświadczeniem bezpieczeństwa. 9 lipca 2015 r. szacunkowa liczba skradzionych płyt wzrosła do 21,5 mln. Obejmowały one rejestry osób, które przeszły kontrolę przeszłości, ale które niekoniecznie były obecnymi lub byłymi pracownikami rządowymi. Skradzione dane obejmowały 5,6 miliona zestawów odcisków palców. Niedługo potem zrezygnowała Katherine Archuleta, dyrektor OPM i była krajowa dyrektor ds. politycznych kampanii reelekcyjnej Baracka Obamy w 2012 roku. Notatka z 22 lipca 2015 r. sporządzona przez inspektora generalnego Patricka McFarlanda mówi, że dyrektor ds. informacji w OPM, Donna Seymour, spowalnia śledztwo w sprawie naruszenia, co skłoniło go do zastanowienia się, czy działała w dobrej wierze. W lutym 2016 r. Donna Seymour zrezygnowała, zaledwie dwa dni przed wyznaczonym terminem składania zeznań przed panelem Izby, który kontynuuje śledztwo w sprawie naruszenia danych.

RANSOMWARE

Oprogramowanie ransomware stało się na przestrzeni lat jedną z głównych przyczyn incydentów związanych z bezpieczeństwem. Ransomware, stosunkowo nowy rodzaj cyberprzestępczości, jest formą złośliwego oprogramowania, które atakuje zarówno ludzkie, jak i techniczne słabości organizacji i poszczególnych sieci, aby uniemożliwić dostęp do krytycznych danych i/lub systemów. Oprogramowanie ransomware jest często dostarczane użytkownikom końcowym za pośrednictwem wiadomości e-mail typu spear phishing, co skutkuje szybkim szyfrowaniem poufnych plików w sieci firmowej. Kiedy organizacja ofiary stwierdzi, że nie ma już dostępu do swoich danych, cyberprzestępca żąda zapłaty okupu, zazwyczaj w wirtualnej walucie, takiej jak BitCoin, w którym to momencie przestępca rzekomo zapewni ofierze możliwość odzyskania dostępu do ich dane. Ostatnio przypadki oprogramowania ransomware zyskały na znaczeniu w dziedzinie cyberbezpieczeństwa ze względu na wzrost liczby ofiar, co z kolei wynika ze znacznych zysków, jakie cyberprzestępcy mogą uzyskać dzięki tego typu złośliwej kampanii. Nastąpił znaczny wzrost ransomware, które koncentruje się na sprzęcie związanym z Internetem Rzeczy (IoT). Jak wynika z badań IBM Security, liczba zdarzeń związanych z oprogramowaniem ransomware wzrosła czterokrotnie w 2016 r., a każdego dnia dochodziło do średnio 4000 ataków. Digital Guardians sugeruje, aby organizacje podjęły następujące działania w celu obrony przed atakami ransomware:

* Miej solidną strategię tworzenia kopii zapasowych

* Promuj świadomość bezpieczeństwa i zapewniaj szkolenia wszystkim pracownikom

* Zainstaluj program antywirusowy i upewnij się, że jest aktualny we wszystkich punktach końcowych w organizacji

* Ustanowienie kontroli nad wykonywaniem plików (ograniczenia GPO)

* Łatanie powszechnie wykorzystywanego oprogramowania innych firm, takiego jak Java, Flash i Adobe

* Ogranicz prawa administracyjne

* Skanuj, aby zidentyfikować możliwe do wykorzystania luki

* Zapoznaj się z polityką bezpieczeństwa dostawcy usług

PRZYKŁAD Z PRAWDZIWEGO ŚWIATA

Ransomware: Mahone Bay i Bridgewater

Mahone Bay i Bridgewater, małe miasteczka w Nowej Szkocji, zgłosiły infekcje na miejskich komputerach, które miały miejsce w czerwcu 2015 roku. Wirus, znany jako CryptoWall 3.0, zaatakował katalogi niepodłączone do sieci za pośrednictwem wiadomości e-mail typu spear-phishing wysłanej do użytkownika systemu lub być może zainfekowanego strona internetowa odwiedzana przez pracownika miasta. Po kliknięciu łącza systemy zostały zainfekowane CryptoWall 3.0 i drugim wirusem o nazwie CryptoLocker, którego zadaniem było szyfrowanie plików w docelowym systemie. Po aktywacji wirusy wysyłały automatyczną wiadomość do użytkownika, żądając zapłaty w wysokości około 900 USD w zamian za odblokowanie zainfekowanych plików – odszyfrowanie plików jest praktycznie niemożliwe, dopóki nie zostanie zapłacony okup. Uważa się, że wirus pochodzi z grup przestępczych w Rosji. Stosowanie technik CryptoLocker jest szeroko rozpowszechnione. Departament Sprawiedliwości USA oszacował, że ataki CryptoLocker zainfekowały ponad 234 000 komputerów – co dało 27 milionów dolarów w postaci płatności okupu – w ciągu zaledwie dwóch pierwszych miesięcy.

SPAMOWANIE/PHISHING

Spamowanie i phishing to dwie bardzo powszechne formy cyberoszustw. Chociaż niewiele możemy zrobić, aby kontrolować te działania, możemy stać się bardziej świadomi takich schematów. Nazwa „Spam" pochodzi od mielonki ze spamu w postaci szkicu Monty Pythona, że spam jest niepożądany, ale nieunikniony. Następnie spamowi nadaje się znaczenie jako emisja niechcianych wiadomości masowych. E-mail to najczęstsza forma spamu. Chociaż wiele wiadomości e-mail ze spamem ma charakter komercyjny, mogą one również zawierać ukryte łącza, które wydają się prowadzić do znanych witryn internetowych prowadzących do witryn phishingowych lub witryn zawierających złośliwe oprogramowanie. Wiadomości Spam mogą również zawierać złośliwe oprogramowanie w postaci skryptów lub innych plików wykonywalnych. Wiadomości spamowe są bardzo opłacalne, ponieważ są opłacalne ekonomicznie, ponieważ reklamodawcy nie ponoszą kosztów operacyjnych poza zarządzaniem listami mailingowymi, serwerami, zakresami adresów IP i nazwami domen. Na przykład holenderski spamer odnotował zysk w wysokości około 50 000 USD, wysyłając co najmniej 9 miliardów wiadomości spamowych. Według Cisco, 2015 Annual Security Report, ilość spamu wzrosła o 250% od stycznia 2014 do listopada 2014. Większość dostawców poczty zareagowała na rosnący poziom wiadomości spamowych, instalując technologię filtrów antyspamowych. Ta technologia identyfikuje spam za pomocą filtrów słów kluczowych lub czarnych list adresów IP spamerów. Aby zapewnić, że spam dotrze do zamierzonych odbiorców, spamerzy coraz częściej stosują te taktyki, aby uniknąć wykrycia przez technologie reputacji oparte na protokole IP. Według Cisco Security Research spam w rakietach śnieżnych to niechciana, masowa poczta e-mail wysyłana przy użyciu dużej liczby adresów IP i małej ilości wiadomości na adres IP, zapobiegając w ten sposób zatopieniu spamu przez niektóre systemy spamowe. Phishing to metoda polegająca na tym, że cyberprzestępcy oferują przynętę, aby ofiara ją zabrała i podała żądane informacje. Przynęta może mieć formę propozycji biznesowej, ogłoszenia loterii, w której ofiara nigdy się nie zapisała, oraz wszystkiego, co obiecuje ofierze pieniądze za nic lub małą przysługę. Jak zauważył Verizon w swoim raporcie z dochodzenia w

sprawie naruszenia danych z 2016 r., wzrost liczby ataków phishingowych zarówno pod względem częstotliwości, jak i zaawansowania. Amerykańskie Centrum ds. Cyberprzestępczości mówi - nie zawieraj żadnych umów, które obiecują coś zbyt pięknego, aby mogło być prawdziwe. W większości przypadków są to fałszywe oferty mające na celu uzyskanie informacji o ofierze. Jednak wielu użytkowników nie może lub nie zastosuje się do porad dotyczących bezpieczeństwa, które są znacznie większym obciążeniem niż prawdopodobne indywidualne konsekwencje awarii zabezpieczeń. Badacze bezpieczeństwa zauważają na przykład, że „jeśli użytkownicy spędziliby nawet minutę dziennie na czytaniu adresów URL, aby uniknąć phishingu, koszt (pod względem czasu użytkownika) byłby o dwa rzędy wielkości większy niż wszystkie straty związane z phishingiem". UNODC sugeruje, że w organizacjach i korporacjach sektora prywatnego procesy organizacyjne promujące zachowania świadome bezpieczeństwa przez pracowników i klientów mają kluczowe znaczenie. Na przykład, pomagając użytkownikom wybrać bezpieczne, ale zapadające w pamięć hasła jednokrotnego logowania w dogodnym czasie, a także zapewniając, że hasła nigdy nie będą wymagane w rozmowie telefonicznej lub e-mailowej lub po kliknięciu łącza w wiadomości e-mail. Ponadto kultura społeczna i organizacyjna powinna unikać propagowania poglądu, że zachowanie „mądre pod względem bezpieczeństwa" jest „paranoidalne" lub „pedantyczne" i zakłóca produktywność. Kultura organizacyjna powinna raczej pomagać w promowaniu i nagradzaniu bezpiecznych zachowań.

PRZYKŁAD Z PRAWDZIWEGO ŚWIATA

Oszustwa socjotechniczne: Mega Metals, Inc.

Mega Metals Inc., 30-letni przetwórca złomu, został oszukany w 2015 roku, kiedy włamano się na konto e-mail używane przez zewnętrznego brokera z siedzibą we Włoszech. Firma Mega Metals przekazała 100 000 USD niemieckiemu dostawcy, aby zapłacić 40 000 funtów za kontener zawierający wióry tytanowe. Po transakcji sprzedawca skarżył się, że nie otrzymał zapłaty. Dochodzenie ujawniło, że złośliwe oprogramowanie wszczepione do systemów komputerowych brokera strony trzeciej umożliwiało przestępcom zbieranie haseł, które zapewniały dostęp do systemu poczty elektronicznej brokera, a następnie fałszowanie instrukcji przelewu w celu dokonania legalnego zakupu.

DALSZE ROZWAŻANIE

Najczęstsze sposoby kradzieży poświadczeń tożsamości i logowania

Złośliwe oprogramowanie: za pomocą złośliwego oprogramowania przestępcy uzyskują dostęp do systemów komputerowych i zbierają poufne dane osobowe, takie jak numery ubezpieczenia społecznego, numery kont, hasła i inne.

Phishing: w tym podstępie przestępcy próbują zdobyć poufne dane osobowe za pośrednictwem poczty elektronicznej. Phishing to jedna z najczęstszych taktyk obserwowanych w branży usług finansowych.

Inżynieria społeczna: za pośrednictwem mediów społecznościowych i innych mediów elektronicznych przestępcy z czasem zdobywają zaufanie ofiar, manipulując nimi w celu ujawnienia poufnych informacji.

Aktywnie przygotuj się na atak

• Naruszenie bezpieczeństwa może nastąpić pomimo najlepszych wysiłków wszystkich zaangażowanych stron. Rozważ podjęcie tych proaktywnych środków w celu przygotowania firmy na potencjalny problem – ze strony zewnętrznych przestępców lub pracowników firmy:

• Stwórz szczegółowy zestaw pisemnych procedur reagowania na oszustwa. Obejmuje to kroki, które należy podjąć wewnętrznie, a także wszelką komunikację z klientem.

• Określ osobę odpowiedzialną za wykonanie procedur. Osoba ta powinna być dobrze zorientowana w procedurach i być w stanie eskalować je w odpowiednim czasie w przypadku wystąpienia oszustwa. Terminowe eskalacje mają kluczowe znaczenie dla sukcesu w odzyskiwaniu nieuczciwie wypłaconych środków.

• Trenuj swój zespół. Przeprowadź szkolenie wewnętrzne, aby upewnić się, że wszyscy specjaliści w Twojej organizacji rozumieją, co musi się stać w przypadku wystąpienia incydentu.

• Zapoznaj się ze wszystkimi dostępnymi zasobami. Zrób listę rodzajów zasobów dostępnych za pośrednictwem instytucji finansowych i dostawców zewnętrznych, z którymi współpracujesz, aby chronić swoją firmę i klientów przed oszustwami cybernetycznymi.

HAKERSTWO

Hakowanie, jedno z najstarszych przestępstw komputerowych, dotyczy bezprawnego dostępu do systemu komputerowego. W USA hakowanie jest klasyfikowane jako przestępstwo i jako takie podlega karze. Przestępczość ta stała się zjawiskiem masowym wraz z rozwojem sieci komputerowych, zwłaszcza Internetu. Wszystkie organizacje są podatne na ataki, a żaden system bezpieczeństwa nie jest niezawodny. Według ITU do słynnych celów ataków hakerskich należą Narodowa Agencja Aeronautyki i Przestrzeni Kosmicznej (NASA), Siły Powietrzne Stanów Zjednoczonych, Pentagon, Yahoo, Google, eBay i rząd Niemiec. Trzy główne czynniki wspierają rosnącą liczbę ataków hakerskich, w tym nieodpowiednią i niepełną ochronę systemów komputerowych, rozwój narzędzi programowych automatyzujących ataki oraz rosnącą rolę komputerów prywatnych jako celu ataków hakerskich. Szczegóły omówiono poniżej.

Czynniki wspierały wzrost ataków hakerskich

Nieodpowiednie i niekompletne

Ochrona systemów komputerowych

- Analiza przeprowadzona przez University of Maryland sugeruje, że niezabezpieczony system komputerowy podłączony do Internetu prawdopodobnie zostanie zaatakowany w ciągu mniej niż minuty.

- Instalacja środków ochronnych może obniżyć ryzyko, ale udane ataki na dobrze chronione systemy komputerowe dowodzą, że techniczne środki ochrony nigdy nie mogą całkowicie powstrzymać ataków.

Rozwój narzędzi programowych

Automatyzacja ataków

- Za pomocą oprogramowania i preinstalowanych ataków jeden przestępca może zaatakować tysiące systemów komputerowych w ciągu jednego dnia przy użyciu jednego komputera.

- Jeżeli sprawca ma dostęp do większej liczby komputerów, m.in. za pośrednictwem botnetu może dalej zwiększać skalę.

Dorastanie

Rola prywatnych komputerów jako celu

- Przestępcy coraz częściej skupiają swoje ataki na prywatnych komputerach, ponieważ wiele prywatnych komputerów jest nieodpowiednio chronionych.

- Komputery prywatne często zawierają poufne informacje (np. dane karty kredytowej i konta bankowego).

- Przestępcy atakują również komputery prywatne, ponieważ po udanym ataku przestępcy mogą włączyć komputer do swojego botnetu i wykorzystać go do dalszych działań przestępczych.

Hakerzy nadal wykorzystują podstawowe luki w zabezpieczeniach systemów komputerowych oraz słabości organizacji. Luki i słabości pozwalają intruzowi wykonywać polecenia, uzyskiwać dostęp do nieautoryzowanych danych i przeprowadzać ataki typu „odmowa usługi". Przykłady luk w zabezpieczeniach i słabości obejmują niezałatane oprogramowanie (np. Adobe, Microsoft i Oracle), niechronione porty, słabe hasła, słabą politykę bezpieczeństwa, przestarzałą infrastrukturę i brak edukacji użytkowników końcowych. Według EY słabości, które narażają organizacje na zwiększone ryzyko, dzielą się na szerokie kategorie:

• Cyberbezpieczeństwo nie jest zgodne z priorytetami organizacji.

• Ramy reagowania są przestarzałe lub niekompletne i pozostają zbyt skoncentrowane na IT.

• Rozwiązania tradycyjnie opierały się na „wkręcanych" uaktualnieniach i wielu heterogenicznych produktach zabezpieczających.

• Linie odpowiedzialności w organizacjach są niejasne.

• Analityka nie jest w pełni wykorzystywana.

Poziom podatności organizacji zależy od wielu czynników, takich jak branża i położenie geograficzne, charakter działalności, adekwatność technologii i systemów bezpieczeństwa, procesów i procedur, zgodność wewnętrzna z ustalonymi procesami, a także jej publiczny profil i łańcuch dostaw. Ogólnie rzecz biorąc, organizacje, które nie skanują pod kątem luk w zabezpieczeniach i aktywnie usuwają słabe punkty systemów informatycznych, mają zwiększone prawdopodobieństwo narażenia ich systemów na szwank. Organizacje powinny uwzględniać oceny podatności jako element swoich programów cyberbezpieczeństwa w celu ochrony przed rosnącymi zagrożeniami cyberataków. Poniżej znajdują się zalecenia dotyczące oceny zagrożeń i podatności.

Zalecenia dotyczące oceny zagrożeń i podatności

• Regularnie uruchamiaj zautomatyzowane narzędzie oceny podatności na wszystkie systemy w sieci. Dostarcz uporządkowane listy najważniejszych luk w zabezpieczeniach każdemu odpowiedzialnemu administratorowi systemu.

• Subskrybuj usługi analizy luk w zabezpieczeniach, aby być świadomym pojawiających się zagrożeń i ekspozycji.

• Upewnij się, że używane narzędzia do skanowania luk w zabezpieczeniach są regularnie aktualizowane i zawierają najnowsze informacje o lukach w zabezpieczeniach.

• Upewnij się, że oprogramowanie/aplikacje komputerowe są regularnie aktualizowane za pomocą poprawek bezpieczeństwa.

• Oceń krytyczne poprawki w środowisku testowym przed wprowadzeniem ich do systemów produkcyjnych

CZYNNIKI ZWIĄZANE Z WZROSTEM CYBERPRZESTĘPCZOŚCI

NIEWŁAŚCIWE UŻYCIE URZĄDZEŃ I ŁATWY DOSTĘP

Cyberprzestępczość wciąż dojrzewa, staje się uprzemysłowiona i profesjonalna, ponieważ generuje wysokie zwroty przy niskim ryzyku przy stosunkowo niskich kosztach i powszechnej dostępności łatwych w użyciu narzędzi programowych. Narzędzia potrzebne do popełnienia skomplikowanych przestępstw są szeroko dostępne w Internecie. Narzędzia programowe upraszczają ataki, pozwalając mniej doświadczonym użytkownikom komputerów na popełnianie cyberprzestępczości. Jedna z najczęstszych technik eksploatacji, wykorzystywanie luk w zabezpieczeniach, w której przestępcy wykorzystują słaby system zabezpieczeń, aby uzyskać dostęp, jest zaskakująco tania. Dostępne są zestawy narzędzi spamowych, które umożliwiają praktycznie każdemu wysyłanie wiadomości spamowych. Takie zachęty zachęcają do ataku i często zniechęcają do obrony. Wraz z większą dostępnością specjalnie zaprojektowanych narzędzi programowych liczba potencjalnych przestępców dramatycznie wzrosła. Popełnianie cyberprzestępczości jest łatwiejsze dzięki specjalistycznym narzędziom programowym. Na przykład przestępcy mogą pobierać narzędzia programowe przeznaczone do łamania ochrony hasłem. Zestawy narzędzi do złośliwego oprogramowania są dostępne jako produkty do zwalczania cyberprzestępczości z obsługą posprzedażną, a funkcje, takie jak rozproszona odmowa usługi (DDoS), są dostępne jako usługi chmurowe wycenione zbiorczo. Coraz częściej tego typu produkty i usługi można otrzymać bezpłatnie. Trudno jest ograniczyć powszechną dostępność takich urządzeń ze względu na techniki dublowania i wymianę peer-to-peer. Na przykład dostępne są narzędzia programowe, których można używać do przesyłania i pobierania plików z systemów udostępniania plików. Rosnąca komercjalizacja narzędzi do nadużyć komputerowych prowadzi do wzrostu poziomu cyberprzestępczości. Dostęp do Internetu jest istotnym elementem popełniania przestępstwa. Liczba internautów szybko rośnie na całym świecie dzięki niedrogim komputerom osobistym i łatwemu dostępowi do Internetu. Internet zapewnia środki do łączenia wielu i różnorodnych sieci, które już istnieją. Internet stale się rozwija. Na przykład stworzenie graficznego interfejsu użytkownika (World Wide Web) zapoczątkowało jego dramatyczny rozwój, ponieważ poprzednie usługi oparte na poleceniach były mniej przyjazne dla użytkownika. Stworzenie World Wide Web umożliwiło nowe aplikacje, a także nowe przestępstwa. Wszędzie tam, gdzie występuje handel, istnieje również ryzyko cyberprzestępczości. Cyberprzestępcy nieustannie poszukują słabych punktów w urządzeniach ochrony sieci, które mają dostęp do Internetu (np. zapory). Chociaż łączność bezprzewodowa ma tę zaletę, że zwiększa mobilność i produktywność, wiąże się również z szeregiem krytycznych zagrożeń i wyzwań związanych z bezpieczeństwem. W wielu głośnych przypadkach kradzieże własności intelektualnej i poufnych informacji zostały zainicjowane przez napastników, którzy uzyskali bezprzewodowy dostęp do organizacji spoza fizycznego budynku. Ponieważ sygnały bezprzewodowe zwykle są nadawane poza fizyczną infrastrukturą budynku, omijają tradycyjne przewodowe zabezpieczenia obwodowe, takie jak zapory ogniowe i systemy ochrony przed włamaniami. W niektórych przypadkach cyberprzestępcy uzyskali nieograniczony dostęp do wewnętrznej sieci organizacji, instalując w sieci ukryte, nieautoryzowane punkty dostępu bezprzewodowego. Niezadowoleni pracownicy lub inny personel o złych zamiarach, pod przykrywką personelu sprzątającego lub ochroniarza, są zazwyczaj odpowiedzialni za podłożenie tych urządzeń. Sieci bezprzewodowe znacznie ułatwiły cyberprzestępcom penetrację organizacji bez fizycznego wchodzenia do budynku. W rezultacie bardzo ważne jest wdrożenie silnych zabezpieczeń w celu złagodzenia tych zagrożeń.

PRZYKŁAD Z PRAWDZIWEGO ŚWIATA

Zaatakowana bezprzewodowa sieć lokalna: TJX Companies Inc.

Hakerzy, którzy ukradli 45 milionów rekordów klientów, w tym miliony numerów kart kredytowych z firmy TJX Companies Inc., zrobili to, włamując się do bezprzewodowej sieci LAN firmy detalicznej. TJX zabezpieczył swoją sieć bezprzewodową za pomocą Wired Equivalent Privacy (WEP) - jednej z

najsłabszych form zabezpieczeń bezprzewodowych sieci LAN. Według The Wall Street Journal hakerzy złamali protokół szyfrowania WEP używany do przesyłania danych między urządzeniami do sprawdzania cen, kasami fiskalnymi i komputerami w sklepie w Minnesocie. Intruzi zbierali następnie informacje przekazywane przez pracowników logujących się do centralnej bazy danych firmy w Massachusetts, kradnąc nazwy użytkowników i hasła. Dzięki tym informacjom hakerzy zakładają własne konta w systemie TJX. Przez 18 miesięcy ich oprogramowanie gromadziło dane transakcyjne, w tym numery kart kredytowych, do około 100 dużych plików. Analitycy oszacowali, że naruszenie kosztowałoby firmę około 1 miliarda dolarów, nie licząc kosztów postępowania sądowego.

Od urządzeń mobilnych po routery, hakerzy zawsze szukają platformy innej niż PC (prawdopodobnie mniej chronionej) w celu złamania zabezpieczeń. Według różnych badań:

- Do 2018 roku 70% mobilnych profesjonalistów wykonywało całą swoją pracę na osobistych inteligentnych urządzeniach.

- Szacuje się, że do 2021 roku 80% dorosłych na Ziemi będzie miało smartfona.

- Urządzenia mobilne wpłynęły na ponad 1 bilion USD w całkowitych zakupach w 2015 r. między transakcjami online i offline.

- Przewiduje się, że przychody ze sprzedaży mobilnego e-commerce wyniosą 516 mld USD.

Ponieważ transakcje mobilne szybko rosną, oszustwa wyprzedzają je, ponieważ cyberprzestępcy przenoszą się na mniej chronione urządzenia. W miarę jak organizacje w dalszym ciągu zapewniają klientom coraz więcej usług mobilnych, a pracownicy zaczynają od nich polegać w celu prowadzenia działalności w ich imieniu, kanał mobilny stał się pełen cyberprzestępczości. Ostatnie badania pokazują, że wiele firm przyjęło systemy płatności mobilnych. Chociaż płatności mobilne są już w głównym nurcie, ekosystem nadal szybko ewoluuje w miarę tworzenia nowych partnerstw w konstelacji sektorów technologii, finansów, handlu detalicznego i telekomunikacji. To ciągle zmieniające się środowisko prawdopodobnie przyniesie nieoczekiwane zagrożenia cyberbezpieczeństwa i rozszerzy wektor cyberataków. Według PwC organizacje zajmują się następującymi najważniejszymi problemami, aby poprawić bezpieczeństwo płatności mobilnych:

- Zagrożenia związane ze złośliwym oprogramowaniem/złośliwymi aplikacjami

- Zagrożenia związane z platformami sprzętowymi/urządzeniami

- Procesy weryfikacji/zaopatrywania w celu ograniczenia oszustw

- Ochrona danych osobowych klientów

- Zagrożenia i luki w zabezpieczeniach użytkowników końcowych

Według RSA, w miarę jak organizacje zmieniają sposób interakcji z klientami, wzrost liczby prób oszustw pochodzących z kanału mobilnego wzrósł o 173% w latach 2013-2015 w porównaniu do zaledwie jednego procenta w kanale internetowym. Należy również wiedzieć, że oprogramowanie ransomware, jedna z najbardziej dochodowych aktywności w świecie cyberprzestępczości, dominuje nad infekcjami platform mobilnych dzięki nowym technikom blokowania urządzeń.

Koncepcja Bring Your Own Device (BYOD) to rosnący trend w biznesie. Odnosi się do polityki, która umożliwia pracownikom przynoszenie do miejsca pracy urządzeń osobistych, w tym laptopów, smartfonów i tabletów, oraz korzystanie z tych urządzeń w celu uzyskania dostępu do aplikacji i danych firmy. Według EY, chociaż realne korzyści biznesowe można czerpać z BYOD w miejscu pracy, niesie to ze sobą znaczne ryzyko. Na przykład:

• Pracownik może stracić urządzenie osobiste zawierające informacje biznesowe.

• Pracownik może nieumyślnie zainstalować aplikacje o złośliwym charakterze.

• Pracownik może nieumyślnie ujawnić informacje biznesowe, na przykład pozwalając członkom rodziny lub znajomym korzystać z laptopa zawierającego poufne informacje biznesowe.

• Sama implementacja BYOD może stanowić naruszenie obowiązujących praw i przepisów, przy czym niewłaściwa implementacja BYOD może naruszać przepisy i regulacje dotyczące prywatności danych.

DALSZE ROZWAŻANIE

Korzystanie z uwierzytelniania bez hasła

Korzystanie z uwierzytelniania i aplikacji bez haseł będzie wymagało od organizacji ponownego przemyślenia swojego podejścia do zarządzania tożsamością i dostosowania poziomu uwierzytelniania do ryzyka związanego z dostępem. Przede wszystkim uwierzytelnianie musi być bezproblemowe i intuicyjne dla użytkowników końcowych. Wystarczy wziąć pod uwagę techniki zarządzania tożsamością i dostępem oraz uwierzytelniania stosowane przez usługi „gospodarki współdzielenia", aby zrozumieć potencjalny wpływ bezproblemowego dostępu na rozwój firmy. Technologie uwierzytelniania nie tylko pomagają przyspieszyć tempo wprowadzania produktu, ale także zwiększają ogólne bezpieczeństwo danych. W rzeczywistości 46% organizacji, które stosują zaawansowane uwierzytelnianie, twierdzi, że technologia ta zwiększyła bezpieczeństwo transakcji online, zgodnie z tegorocznymi wynikami ankiety. Respondenci informują również, że technologie uwierzytelniania zwiększają zaufanie konsumentów do ich funkcji bezpieczeństwa i prywatności, a także poprawiają wrażenia klientów i chronią reputację marki. Inny trend dotyczy uwierzytelniania adaptacyjnego. Ponieważ systemy informatyczne przechwytują coraz więcej informacji, firmy zaczynają wykorzystywać dodatkowe punkty danych do identyfikowania podejrzanych zachowań i wzorców. Uwierzytelnianie adaptacyjne wykorzystuje dane, takie jak czas i lokalizacja logowania użytkownika, wzorce dostępu i typ urządzenia, aby podjąć decyzję o dostępie opartą na ryzyku. Jeśli aplikacja wykryje nieprawidłową aktywność podczas próby logowania, może wymagać dalszych kroków uwierzytelniania lub całkowicie zatrzymać proces. Firmy naprawdę myślące przyszłościowo zaczynają łączyć techniki uwierzytelniania adaptacyjnego ze sztuczną inteligencją (AI) i uczeniem maszynowym, aby budować mechanizmy predykcyjnego uwierzytelniania. Zastosowanie zmiennych predykcyjnych może sprawić, że uwierzytelnianie będzie ciągłym zdarzeniem, powiązanym z ryzykiem związanym z określonymi próbami dostępu. Może to znacznie poprawić wrażenia użytkownika końcowego, jednocześnie zwiększając poziom bezpieczeństwa i zaufania.

AUTOMATYZACJA

Możliwość automatyzacji niektórych procesów to jedna z największych zalet technologii informacyjno-komunikacyjnych. Ważne jest zrozumienie konsekwencji automatyzacji, w tym zwiększenia szybkości procesów oraz skali i wpływu procesów, a także zmniejszenia zaangażowania człowieka. Cyberprzestępczość jest łatwiejsza dzięki automatyzacji, gdy przestępcy mogą wykorzystać automatyzację do zwiększenia skali swoich działań. Na przykład miliony niechcianych, masowych wiadomości spamowych mogą zostać wysłane automatycznie. Według ostatnich badań ataki hakerskie często można zautomatyzować, przy czym każdego dnia dochodzi do 80 milionów ataków hakerskich dzięki użyciu narzędzi programowych, które mogą zaatakować tysiące systemów komputerowych w ciągu godzin. Przestępcy mogą czerpać duże zyski, projektując oszustwa oparte na dużej liczbie przestępstw, przy stosunkowo niskiej stracie dla każdej ofiary dzięki automatyzacji procesów. Im niższa pojedyncza strata, tym większa szansa, że ofiara nie zgłosi przestępstwa. Ponadto stopa zwrotu na

ofiarę cyberprzestępczości może być bardzo niska, ale ponieważ koszty i ryzyko zaangażowania się w nią są jeszcze niższe, cyberprzestępczość pozostaje działalnością przestępczą, której nie można się oprzeć.

ANONIMOWOŚĆ

Rosnący poziom cyberprzestępczości przypisuje się rosnącym możliwościom w zakresie technik anonimowości podczas korzystania z ICT. Anonimowość była jednym z największych wyzwań, jakie cyberprzestępczość stawia przed organami ścigania. Przestępcy zazwyczaj nie subskrybują usług internetowych, aby zmniejszyć swoje szanse na zidentyfikowanie i preferują usługi, z których mogą korzystać bez rejestracji. Najczęstszymi metodami używanymi przez przestępców w celu uzyskania dostępu do sieci są publiczne terminale internetowe, sieci otwarte (bezprzewodowe), sieci zhakowane i usługi przedpłacone bez wymogu rejestracji. Ponadto wielu dostawców oferuje bezpłatne adresy e-mail. Tam, gdzie trzeba wprowadzić dane osobowe, mogą nie zostać zweryfikowane, więc użytkownicy mogą zarejestrować adresy e-mail bez ujawniania ich tożsamości. W rezultacie częste korzystanie z technologii anonimizacji szybko poszerza grono przestępców za pośrednictwem internetowych rynków przestępczych. Anonimowa komunikacja może prowadzić do zachowań antyspołecznych. W warunkach całkowitej anonimowości ludzie stają się bardziej wydziedziczeni niż zwykle lub mogą eksperymentować z różnymi tożsamościami. Według UNODC stan zagrożenia cyberprzestrzeni tworzy nowe zjawiska, które są wyraźnie różne od (zwykłego) istnienia samych systemów komputerowych i bezpośrednich możliwości popełniania przestępstw, jakie stwarzają komputery. W cyberprzestrzeni osoby mogą wykazywać różnice między swoim zachowaniem zgodnym (legalnym) i niezgodnym (nielegalnym) w porównaniu z zachowaniem w świecie fizycznym. Osoby mogą na przykład popełniać przestępstwa w cyberprzestrzeni, których inaczej nie popełniłyby w przestrzeni fizycznej ze względu na swój status i pozycję. Ponadto elastyczność tożsamości, dysocjacyjna anonimowość i brak czynników odstraszających mogą stanowić zachęty do zachowań przestępczych w cyberprzestrzeni.

ŁATWY DOSTĘP DO OFIAR

Zgodnie z teorią czynności rutynowych Cohena i Felsona, przestępczość występuje ze zbieżnością trzech elementów; zmotywowany sprawca, odpowiedni cel i brak odpowiedniej opieki. Gdy umotywowany przestępca wejdzie w kontakt z odpowiednim celem przy braku zdolnego opiekuna, który mógłby potencjalnie zapobiec popełnieniu przestępstwa przez przestępcę, dochodzi do przestępstwa. Innymi słowy, zbieżność tych trzech elementów stwarza możliwości dla działań przestępczych i dewiacyjnych oraz zwiększa prawdopodobieństwo wiktymizacji przestępczej. Brak któregokolwiek z tych trzech elementów w równaniu zapobiega występowaniu działań przestępczych i dewiacyjnych. Hindelang, M.J. twierdzi, że ryzyko wiktymizacji zależy od różnych stylów życia jednostek, które definiuje się jako „rutynowe codzienne czynności, zarówno zawodowe (praca, szkoła, prowadzenie domu itp.), jak i zajęcia rekreacyjne". Teorie rutynowej aktywności i ekspozycji na styl życia można zastosować do cyberprzestrzeni stworzonej przez postęp w technologiach komputerowych i sieciowych, w którym codzienne, rutynowe czynności i styl życia ludzi zmieniły się radykalnie. Rutynowe czynności jednostek i ekspozycja na styl życia stwarzają sprawcom możliwość popełnienia przestępstwa. Na przykład duża liczba odpowiednich celów może wyłonić się dzięki wydłużeniu czasu spędzanego w Internecie oraz korzystaniu z usług internetowych, takich jak bankowość, zakupy i udostępnianie plików, co sprawia, że użytkownicy są podatni na ataki typu phishing lub oszustwa. Nic dziwnego, że phishing jest jedną z najczęstszych taktyk obserwowanych w branży usług finansowych. Niezależnie od tego, czy jest to instytucja finansowa, sklep internetowy, który prowadzi interesy z kupującymi online, a teraz nawet szpitale w obliczu rosnącej fali oprogramowania ransomware, cyberprzestępczość nie ma granic. Każdy, kto ma adres e-mail, skrzynkę odbiorczą lub konto w mediach społecznościowych, jest celem. UNODC zauważa, że pojawienie się

internetowych sieci społecznościowych, w tym Twittera i Facebooka, zapewnia również dostęp do milionów potencjalnych ofiar oszustw lub oszustw. Tam, gdzie użytkownicy nie ograniczyli ustawień komunikacji, aby umożliwić tylko interakcję z ich prywatną siecią „przyjaciół", takie sieci mogą zapewnić dostęp do dużej liczby potencjalnych ofiar jednocześnie. Osoby mają również tendencję do organizowania swoich profili w sieciach społecznościowych zgodnie ze swoimi zainteresowaniami i lokalizacją, co umożliwia przestępcom namierzenie ofiar z określonymi trybami zachowania lub pochodzeniem. Takie „opiekuńcze" środki, które istnieją, takie jak programy antywirusowe i (stosunkowo niewielkie) ryzyko działań organów ścigania, mogą być niewystarczające, aby odstraszyć sprawcę motywowanego pokusą znacznego zysku.

NAUKI SPOŁECZNE

Według Bandury A, kluczowego uczestnika teorii społecznego uczenia się, większość ludzkich zachowań uczy się obserwacyjnie, a ta informacja służy jako wskazówka do działania w przyszłości. Jednostka poznaje normy społeczne poprzez proces socjalizacji. Na przykład osoba z mniejszym doświadczeniem postrzega bardziej doświadczoną osobę jako mentora. Teoria ta może mieć szczególne zastosowanie w przypadku cyberprzestępczości, ponieważ przestępcy często muszą nauczyć się określonych technik i procedur komputerowych. Na przykład aktu hakowania uczy się w interakcji grupowej. Ponadto osoby narażone w Internecie na modele cyberprzestępcze i ich rówieśnicy mogą postrzegać siebie jako bardziej skłonne do angażowania się w cyberprzestępczość. Badania podkreślają również, że ogólna teoria przestępczości dotycząca ograniczonej samokontroli i gotowości do podejmowania ryzyka krótkoterminowych korzyści może mieć zastosowanie do działań ułatwianych lub usprawnianych przez komunikację elektroniczną i Internet. Ludzie o mniejszej samokontroli są impulsywni, niewrażliwi i podejmują ryzyko, że nie są w stanie oprzeć się okazji do urazy. Mniejsza samokontrola wiąże się z różnymi formami cyberprzestępczości, w tym nielegalnym pobieraniem muzyki, piractwem filmów i piractwem oprogramowania. Teoria społecznego uczenia się i ogólna teoria przestępczości wchodzą w interakcję, w której osoby o obniżonej samokontroli mogą aktywnie poszukiwać podobnych osób i łączyć się w środowiskach wirtualnych w taki sam sposób, jak w świecie rzeczywistym. W cyberprzestrzeni proces ten może zachodzić w znacznie skróconym czasie i o znacznie szerszym zasięgu geograficznym.

DALSZE ROZWAŻANIE

Zaawansowane uwierzytelnianie w celu wyłapania phisherów

W ciągu ostatniego roku phishing stał się poważnym zagrożeniem dla firm każdej wielkości i z różnych branż. Technika ta reprezentuje ponowne pojawienie się tradycyjnych taktyk socjotechnicznych, chociaż phishing jest bardziej skoncentrowany i skuteczny. Cyberprzestępcy nabrali biegłości w wykorzystywaniu schematów phishingowych w celu uzyskania danych uwierzytelniających użytkownika, a następnie uzyskania dostępu do informacji w systemie i dane. W tym roku 38% respondentów ankiety zgłosiło oszustwa phishingowe, co czyni je głównym wektorem incydentów cyberbezpieczeństwa. Wzrost liczby incydentów phishingowych sugeruje, że cyberprzestępcy w mniejszym stopniu polegają na wyrafinowanym złośliwym oprogramowaniu do przeprowadzania ataków, a zamiast tego „żyją na lądzie", wykorzystując istniejące narzędzia i funkcje administracyjne. W celu zwalczania kradzieży poświadczeń użytkowników wiele firm stosuje zaawansowane uwierzytelnianie, które zastępuje wszystkie, ale bezużyteczne hasła. Ten rodzaj zapobiegania stał się krytycznym wymogiem biznesowym, ponieważ wykładniczo więcej informacji konsumenckich i korporacyjnych jest generowanych i udostępnianych, a konsumenci oczekują, że ich dane osobowe będą zabezpieczone. Obecnie najczęściej używanymi technologiami zaawansowanego uwierzytelniania są tokeny sprzętowe i programowe, a następnie biometria, taka jak skanery linii

papilarnych i tęczówki oka. Jednak w nadchodzącym roku respondenci ankiety twierdzą, że ich priorytetem w zakresie wydatków na uwierzytelnianie będą tokeny smartfonów. W tym roku 28% respondentów ankiety zgłosiło naruszenia bezpieczeństwa urządzeń mobilnych, a zabezpieczenie smartfonów i tabletów jest zdecydowanie najważniejsze.

ŹRÓDŁA CYBER ZAGROŻEŃ

PROFILE PODMIOTÓW ZAGROŻEŃ

Ponieważ cyberprzestępcy nieustannie zmieniają taktyki, zwiększając swoją wytrwałość i rozszerzając swoje możliwości, charakter cyberzagrożeń ewoluował od prostych atakujących do ataków sponsorowanych przez państwo. Szybko ewoluujące i wielowymiarowe zagrożenia występują we wszystkich branżach, ponieważ przestępczość zorganizowana staje się coraz bardziej wyrafinowana w wykorzystywaniu technologii do popełniania oszustw. Poniższa tabela przedstawia ciągłą ewolucję zagrożeń bezpieczeństwa cybernetycznego od skryptowych dzieciaków do ataków sponsorowanych.

Niewyrafinowani napastnicy (Script Kiddies) -> Wyrafinowani napastnicy (hakerzy) -> Szpiegostwo korporacyjne (Insiders) -> Ataki sponsorowane przez państwo (hacktywizm, kradzieże tożsamości)

Eksperyment: Jesteś atakowany, ponieważ jesteś w Internecie i masz podatność na ataki -> Monetyzacja: Jesteś atakowany, ponieważ jesteś w Internecie i posiadasz wartościowe informacje -> Twój obecny lub były pracownik dąży do uzyskania korzyści finansowych ze sprzedaży Twojej własności intelektualnej -> Jesteś kierowany ze względu na to, kim jesteś, co robisz lub wartość Twojej własności intelektualnej. -Cyberataki promujące cele polityczne, takie haktywistowskie. Kradzież informacji umożliwiających identyfikację osób (PII) rośnie

Zagrożenia dla cyberbezpieczeństwa przybierają różne formy i są popełniane przez różne grupy o różnych celach, motywacjach i środkach. Na przykład cyberprzestępcy o charakterze korporacyjnym starają się uzyskać informacje o kontach finansowych i inne dane klientów, na których mogliby zarabiać. Ci cyberprzestępcy mogą atakować systemy punktów sprzedaży (PoS) lub bazy danych klientów w celu gromadzenia danych uwierzytelniających użytkownika, przechowywanych danych finansowych i przechowywanych informacji umożliwiających identyfikację osób (PII). Aktorzy państwowi zazwyczaj biorą na cel wysoce wrażliwą własność intelektualną, wrażliwą komunikację lub inne strategiczne aktywa i informacje. Podmioty zaawansowanego trwałego zagrożenia (APT), najbardziej znaczące i wymagające zagrożenia, mają na celu wspieranie krajowych firm poprzez dostarczanie im innowacyjnych technologii lub przewagi konkurencyjnej nad konkurencją. McAfee opisuje APT jako:

„Bardziej podstępne i występują w dużej mierze bez publicznego ujawnienia. Stanowią one znacznie większe zagrożenie dla firm i rządów, ponieważ przeciwnik wytrwale dąży do osiągnięcia swoich celów. Kluczem do tych włamań jest to, że przeciwnik jest motywowany ogromnym głodem tajemnic i własności intelektualnej; różni się to od natychmiastowej gratyfikacji finansowej, która napędza większość cyberprzestępczości, innego poważnego, ale łatwiejszego do opanowania zagrożenia”

APT obejmują działalność w dużej mierze wspieraną, bezpośrednio lub pośrednio, przez państwo narodowe. APT są ukierunkowane na starannie wyselekcjonowane, wartościowe dane w każdej branży, od przemysłu lotniczego po hurtowników, od edukacji po finanse. Ci aktorzy zagrożeń mogą dalej starać się zrozumieć łańcuchy dostaw, procesy produkcyjne i programistyczne szczegóły biznesowe w celu powielenia tych procesów lub zidentyfikowania słabych punktów. Według przewodnika ITU National Cybersecurity Strategy Guide, świadomość ataku nie stanowi problemu, jeśli sprawcami są grupy haktywistyczne, takie jak Anonymous i Lulzsec, które szukają rozgłosu. Jednak

stratedzy ds. cyberbezpieczeństwa i bezpieczeństwa narodowego są bardzo zaniepokojeni celowymi włamaniami lub atakami APT. Niezależnie od rodzaju cyberprzestępców, ich działania mogą poważnie zaszkodzić organizacjom. W poniższej tabeli wymieniono profile cyberprzestępców, w tym ich motywy, cel i wpływ.

Profile aktorów zagrożeń

Aktorzy : Motywy : Cel : Wpływ

Państwa narodowe: Przewaga gospodarcza, polityczna i/lub militarna:

- Tajemnice handlowe

- Wrażliwe informacje biznesowe

- Nowe technologie

- Infrastruktura krytyczna :

• Utrata przewagi konkurencyjnej

• Zakłócenie infrastruktury krytycznej

Przestępczość zorganizowana :

- Natychmiastowy zysk finansowy

- Zbieraj informacje dotyczące przyszłych zysków finansowych:

- Systemy finansowe/płatnicze

- Dane osobowe

- Informacje o karcie płatniczej

- Chronione informacje zdrowotne :

• Kosztowne zapytania regulacyjne i kary

• Sprawy konsumenckie i wspólników

• Utrata zaufania konsumentów

Haktywiści:

- Wpływaj na zmiany polityczne i/lub społeczne

- wywieranie nacisku na firmy, aby zmieniły swoje praktyki:

- tajemnice korporacyjne

- Wrażliwe informacje biznesowe

- Informacje dotyczące kluczowej kadry kierowniczej, pracowników, klientów i partnerów biznesowych:

• Zakłócenie działalności biznesowej

• Marka i reputacja

• Utrata zaufania konsumentów

Insiders :

- Korzyść osobista, zysk pieniężny

- Profesjonalna zemsta

- Patriotyzm :

- Sprzedaż, transakcje, strategie rynkowe

- Tajemnice korporacyjne, IP, R&D

- Operacje biznesowe

- Informacja personelu :

• Ujawnienie tajemnicy handlowej

• Zakłócenia operacyjne

• Marka i reputacja

• Wpływ na bezpieczeństwo narodowe

Aby skupić jak najwięcej uwagi, zapobiegać i skutecznie przeciwdziałać obszarom o największej wartości i największym ryzyku, organizacje powinny najpierw zidentyfikować najbardziej prawdopodobne źródło ataku; wewnętrzny i zewnętrzny. Szczegóły omówiono w kolejnych sekcjach.

ZAGROŻENIA WEWNĘTRZNE

Zagrożenia wewnętrzne dla bezpieczeństwa informacji przebiegają od nieumyślnych błędów (zwykły błąd użytkownika, utrata urządzeń mobilnych) po złośliwe działania (oszustwa wewnętrzne, kradzież danych). Ogólnie rzecz biorąc, intruzi wewnętrzni to użytkownicy z uprawnieniami lub autoryzowanym dostępem do systemu z kontem na serwerze lub fizycznym dostępem do sieci. Glosariusz zabezpieczeń internetowych opisuje „atak wewnętrzny" jako atak zainicjowany przez podmiot znajdujący się w strefie bezpieczeństwa („insider"). Zagrożenie wewnętrzne może pochodzić od obecnego lub byłego pracownika, kontrahenta lub innego partnera biznesowego, który ma lub upoważnił dostęp do sieci, systemu lub danych organizacji i celowo nadużył tego dostępu w sposób, który negatywnie wpłynął na poufność, integralność lub dostępność informacji lub systemów komputerowych organizacji. Obrona przed zagrożeniami wewnętrznymi może być trudna, ponieważ sprawcy nadużywają uzyskanych uprawnień dostępu do legalnych funkcji biznesowych. Ponadto pracownicy, kontrahenci, doradcy i osoby w łańcuchu dostaw często znajdują się w obrębie zapór bezpieczeństwa organizacji, z uprawnieniami dostępu do technologii oraz wykorzystywania i rozpowszechniania danych. Niemal codziennie zgłaszane są przypadki zgubienia lub kradzieży laptopów zawierających poufne dane. Najnowsze statystyki pokazują, że nadużycie uprawnień jest główną przyczyną wycieku danych wykrywaną przez złośliwych insiderów. Według Baker Botts, The Future of Cyber-Security Threats and Opportunities, łańcuch cyberbezpieczeństwa jest tak silny, jak jego najsłabsze ogniwo, a organizacje powinny być czujne, gdy ujawniają poufne dane handlowe swoim dostawcom i doradcom, w tym księgowym, prawnikom i finansistom - jak bezpieczne są ich systemy i procesy? Na przykład rząd Wielkiej Brytanii ostrzegł niedawno, że cyberprzestępcy atakują doradców, takich jak prawnicy, bankierzy inwestycyjni i księgowi, aby uzyskać dostęp do poufnych informacji dotyczących ich klientów korporacyjnych. Równie niepokojący są osoby z wewnątrz lub pracownicy, którzy przypadkowo powodują cyberszkody poprzez nieumyślne kliknięcie wiadomości e-mail phishingowej, podłączenie

zainfekowanego USB do komputera lub zignorowanie procedur bezpieczeństwa i pobranie niebezpiecznej zawartości z Internetu. Na przykład znaczna liczba utraty danych i naruszeń bezpieczeństwa nadal ma miejsce w wyniku niezamierzonych zdarzeń (np. niewinnych błędów, złej praktyki w zakresie bezpieczeństwa wewnętrznego), takich jak nieumyślne zgubienie lub naruszenie bezpieczeństwa laptopów i innych mobilnych nośników pamięci, dołączanie niewłaściwych plików do wiadomości e-mail, lub wiadomości e-mail nieumyślnie wysłane do niewłaściwych odbiorców. Według EY, nieostrożni lub nieświadomi pracownicy to najczęstsze luki, które organizacje postrzegają jako priorytetowe na podstawie wyników ankiety przeprowadzonej zarówno w 2014, jak i 2015 roku. Zwiększone wykorzystanie narzędzia Bring Your Own Device (BYOD) jest często niewspierane przez organizację pracodawców lub nie chronione w ramach architektury bezpieczeństwa sieci organizacji. Możliwość łatwego i regularnego pobierania aplikacji osobistych na urządzenia obsługujące dane wrażliwe budzi obawy dotyczące bezpieczeństwa. Ryzyko jest większe, jeśli wrażliwe lub cenne dane są pobierane na urządzenie, a nie są dostępne przez urządzenie. Według EY, ponieważ firmy wspierają produktywność poprzez szybką integrację BYOD, cloud computing i innych aspektów całkowitej mobilności, istnieje odpowiedni wzrost ryzyka, dla którego informacje znajdujące się w tych kanałach lub dostępne za ich pośrednictwem. Takie ryzyko związane z zagrożeniami wewnętrznymi może obejmować:

• Niepożądane ujawnienie poufnych danych klientów i kont — naraża na niebezpieczeństwo najcenniejsze relacje organizacji

• Oszustwo

• Utrata własności intelektualnej

• Zakłócenie infrastruktury krytycznej

• Strata pieniężna

• Reperkusje regulacyjne

• Destabilizacja, zakłócenia i niszczenie cyberaktywów instytucji finansowych

• Zakłopotanie i kwestie związane z public relations/ryzykiem reputacji

Centrum zagrożeń wewnętrznych CERT Carnegie Mellon sugeruje, że następujący pracownicy stanowią największe ryzyko zagrożenia wewnętrznego:

- niezadowoleni pracownicy, którzy czują się lekceważeni i szukają zemsty;

- pracownicy poszukujący zysku, którzy mogą wierzyć, że mogą zarobić więcej pieniędzy sprzedając skradzioną własność intelektualną;

- Pracownicy przenoszący się do konkurenta lub rozpoczynający działalność gospodarczą, którzy na przykład kradną listy klientów lub plany biznesowe, aby zapewnić sobie przewagę konkurencyjną, oraz

- Pracownicy, którzy uważają, że posiadają własność intelektualną, którą pomagają rozwijać. W rezultacie, opuszczając organizację, zabierają ze sobą własność intelektualną

Rozpoznając potencjalne szkody stwarzane przez obecnych lub odchodzących pracowników, organizacja może pomóc złagodzić szkody, które mogą wyniknąć z zagrożeń wewnętrznych. Poniżej znajdują się zalecenia dotyczące przeciwdziałania zagrożeniom wewnętrznym.

Zalecenia dotyczące postępowania z niejawnymi przysmakami

1) Zbuduj zespół multidyscyplinarny

Tam, gdzie to możliwe, organizacje muszą mieć dedykowany zespół złożony z specjalistów ds. zasobów ludzkich, bezpieczeństwa i prawników, którzy tworzą zasady, prowadzą szkolenia i monitorują pracowników zagrożonych.

2) Kwestie organizacyjne

Dowiedz się, czy Twoja organizacja jest narażona na większe ryzyko z powodu nieodłącznych czynników organizacyjnych. Czy Twoja firma ma zdalne biura, dostawców lub podwykonawców, w których różnice kulturowe, polityczne lub językowe mogą prowadzić do potencjalnych konfliktów?

3) Zbadaj procesy przesiewowe przed zatrudnieniem

Informacje zebrane w trakcie tych procesów pomogą menedżerom ds. rekrutacji podejmować świadome decyzje i zmniejszać ryzyko zatrudnienia „problematycznego" pracownika.

4) Opracuj zasady i praktyki

Jest to lista kontrolna konkretnych obszarów polityki i praktyki, które należy uwzględnić w podstawowych strukturach zarządzania organizacji.

5) Przeprowadź szkolenie i edukację

Są one niezbędne dla skuteczności polityki, ponieważ polityki i praktyki, które nie są rozpoznawane, rozumiane i przestrzegane, mogą mieć ograniczoną skuteczność.

6) Monitoruj i reaguj na podejrzane lub destrukcyjne zachowanie, począwszy od procesu rekrutacji

7) Przewiduj negatywne problemy w miejscu pracy i zarządzaj nimi

8) Egzekwuj rozdział obowiązków i najmniejszy przywilej

PRZYKŁAD Z PRAWDZIWEGO ŚWIATA

Wyciek danych wewnętrznych: Biuro kredytowe Korei Południowej

Dane osobowe co najmniej 20 milionów użytkowników banków i kart kredytowych w Korei Południowej zostały skradzione z trzech firm obsługujących karty kredytowe przez tymczasowego konsultanta współpracującego z firmą koreańskiej agencji ratingowej Korean Credit Bureau (KCB). Skradzione dane, które zostały sprzedane firmom zajmującym się marketingiem telefonicznym, obejmowały imiona i nazwiska klientów, numery ubezpieczenia społecznego, numery telefonów, numery kart kredytowych i daty ważności. W wyniku kradzieży dziesiątki dyrektorów najwyższego szczebla złożyły rezygnacje, organy regulacyjne wszczęły dochodzenia w sprawie środków bezpieczeństwa w zaatakowanych firmach, a firmy zostały pociągnięte do odpowiedzialności za pełne straty finansowe, gdyby klienci padli ofiarą oszustw związanych z kradzieżą danych.

ZAGROŻENIA ZEWNĘTRZNE

Sprawcy zewnętrzni, dobrze finansowani, wytrwali i wyrafinowani, to osoby, które nie należą do domeny sieciowej. Ludzie i procesy są w coraz większym stopniu celem, podobnie jak technologia. Ponieważ cyberprzestępcy są zmotywowani do jak najszybszej ewolucji, reakcje muszą być równie sprawne, aby dotrzymać kroku. Witryny publiczne i społecznościowe to najczęstsze miejsca, w których hakerzy mogą oszukać zwykłych użytkowników. Stała łączność organizacji z Internetem naraża ją na

wrogie środowisko szybko ewoluujących zagrożeń. Co więcej, systemy operacyjne używane na laptopach, komputerach PC i telefonach komórkowych mają wspólne i znane luki w zabezpieczeniach, które mogą wykorzystać atakujący. Ryzyko cyberataku na podmioty ze wszystkich branż stale rośnie, ponieważ nasz wysoce połączony świat stwarza więcej możliwości dla cyberprzestępców. Na przykład wzrasta presja na agencje rządowe, aby świadczyć usługi online, ponieważ obywatele coraz częściej oczekują, że usługi tradycyjnie świadczone w formie papierowej będą dostępne online. W wyniku przejścia na świadczenie usług cyfrowych agencje rządowe są odpowiedzialne za dane wrażliwe pod względem bezpieczeństwa, które z natury są bardziej narażone na publiczny dostęp. Istnienie tych informacji stwarza cyberprzestępcom możliwość uzyskania dostępu do danych i wykorzystania ich do kradzieży tożsamości i oszustw. Instytucje finansowe pozostają stałym celem cyberprzestępców, którzy chcą ukraść swoją własność intelektualną i poufne informacje, ponieważ polegają na narzędziach online, które pomagają im komunikować się z interesariuszami. Osoby, firmy, organy rządowe, instytucje i organizacje stoją w obliczu zagrożeń głównie ze strony państw narodowych, gangów przestępczych i haktywistów.

PAŃSTWA NARODOWE

Państwa narodowe, motywowane nacjonalizmem, są ustanowione i dobrze zorganizowane, aby przeprowadzać najbardziej wyrafinowane zagrożenia w cyberprzestrzeni. Ich interesy obejmują cele polityczne, gospodarcze, wojskowe i finansowe. Zwykle mają określone zadania, takie jak:

• Zdobywanie inteligencji

• Kradzież tajemnic przemysłowych i własności intelektualnej

• Sabotowanie infrastruktury krytycznej i mediów w celach politycznych i gospodarczych

• Przysłuchiwanie się dyskusjom dotyczącym polityki

• Prowadzenie propagandy

Każdy kraj ma unikalny system polityczny, historię i kulturę, ataki sponsorowane przez państwo mają również charakterystyczne cechy, które obejmują wszystko, od motywacji do celu i rodzaju ataku. FireEye opisuje unikalną charakterystykę kampanii cyberataków prowadzonych przez rządy w regionie Azji i Pacyfiku, Rosji/Europy Wschodniej, Bliskiego Wschodu i USA. Należy zauważyć, że jedno państwo narodowe rozwija i używa wyrafinowanego trojana, a później (po własnym (zabezpieczenie trojana) sprzedaje go cyberprzestępcom na czarnym rynku. Dlatego niektóre kampanie cyberataków mogą nosić znamiona zarówno podmiotów państwowych, jak i niepaństwowych, co sprawia, że pozytywna atrybucja jest prawie niemożliwa.

Charakterystyka cyberataków dokonywanych przez rządy na całym świecie

Azja i Pacyfik : siedziba dużych, biurokratycznych grup hakerów, takich jak „Comment Crew", które dążą do wielu celów i celów w atakach brutalnych o wysokiej częstotliwości.

Rosja/Europa Wschodnia: Te cyberataki są bardziej zaawansowane technicznie i wysoce skuteczne w unikaniu wykrycia.

Bliski Wschód : ci hakerzy są dynamiczni, często wykorzystują kreatywność, oszustwa i socjotechnikę, aby nakłonić użytkowników do skompromitowania własnych komputerów.

USA: Najbardziej złożone, ukierunkowane i rygorystycznie zaprojektowane kampanie cyberataków w historii.

Należy zauważyć, że jedno państwo opracowuje i wykorzystuje wyrafinowanego trojana, a później (po wdrożeniu własnych mechanizmów obrony przed trojanami) sprzedaje go cyberprzestępcom na czarnym rynku. Dlatego niektóre kampanie cyberataków mogą nosić znamiona zarówno podmiotów państwowych, jak i niepaństwowych, co sprawia, że pozytywna atrybucja jest prawie niemożliwa.

Gangi kryminalne

Grupy przestępcze napędzane zyskiem i osobistym zyskiem stanowią szybko narastający problem we współpracy międzynarodowej, tworząc globalny rynek narzędzi do cyberprzestępczości. Przestępczość zorganizowana staje się coraz bardziej wyrafinowana w wykorzystywaniu technologii do popełniania oszustw, kradzieży funduszy i cennych informacji. Według UNODC szacuje się, że ponad 80% cyberprzestępczości ma swoje źródło w jakiejś formie zorganizowanej działalności, przy czym czarne rynki cyberprzestępczości opierają się na cyklu tworzenia złośliwego oprogramowania, infekcji komputerowych, zarządzania botnetami, przechwytywania danych osobowych i finansowych, sprzedaży danych, oraz „wypłacanie" informacji finansowych. Łączność online i partnerskie uczenie się mają prawdopodobnie kluczowe znaczenie dla zaangażowania zorganizowanych grup przestępczych w cyberprzestępczość. Carding, handel kartami kredytowymi, kontami bankowymi i innymi danymi osobowymi online to jeden z takich przykładów. Nowoczesne punkty kartingowe zostały opisane jako podmioty komercyjne oferujące pełen zakres usług, takich jak dostarczanie technik prania pieniędzy. Wiele forów udostępnia również powiązane usługi związane z przestępczością komputerową, takie jak zestawy phishingowe, listy złośliwego oprogramowania i spamu.

HAKTYWIŚCI

Haktywiści zwykle odnoszą się do odmiennej grupy, która składa się z wielu różnych ideologicznie zorientowanych grup i osób o różnych motywacjach. Promują formę nieposłuszeństwa obywatelskiego w cyberprzestrzeni, taką jak Anonymous, włamując się do systemów komputerowych w celach politycznych lub społecznych, aby zwrócić uwagę na problem, a nie dla zysku osobistego lub pieniężnego. Na przykład w listopadzie 2013 r. hakerzy twierdzący, że linki do witryny Anonymous zniszczyli dziesiątki stron internetowych należących do australijskich firm i filipińskich agencji rządowych, w odpowiedzi na zarzuty szpiegowania.

PRZYKŁAD Z PRAWDZIWEGO ŚWIATA

Haktywizm: Ashley Madison

Kanadyjska firma Ashley Madison była celem hakerów w lipcu 2015 roku. Nazywając siebie Impact Team, hakerzy zakwestionowali model biznesowy firmy polegający na udostępnianiu forum ułatwiającego niewierność małżeńską. Celem hakerów było zmuszenie firmy do zaprzestania działalności. W sierpniu 2015 r. hakerzy opublikowali około 39 milionów profili klientów, w tym profile użytkowników, nazwiska i adresy e-mail. Prawnicy reprezentujący ofiary kanadyjskie wszczęli pozew zbiorowy, domagając się odszkodowania w wysokości 760 milionów dolarów. Firma macierzysta, Avid Life Media, odłożyła na czas nieokreślony nadchodzącą pierwszą ofertę publiczną Ashley Madison, z której firma miała nadzieję zebrać 200 milionów dolarów.

DALSZE ROZWAŻANIE

Problemy bezpieczeństwa systemowego - dane kart płatniczych

Najczęstszym sposobem, w jaki cyberprzestępcy uzyskują dostęp do danych kart płatniczych klientów lub „śledzenia danych" (elektronicznie zakodowanych danych na pasku magnetycznym z tyłu karty kredytowej) jest instalowanie elektronicznego oprogramowania „skimmerów" w punkcie sprzedaży

detalicznej sprzedaż terminali (POS). Odpieniacze są zaprojektowane do zbierania danych o torze na pasku magnetycznym karty, gdy klienci przesuwają kartę, aby sfinalizować transakcję zakupu. Przechwytywanie danych toru umożliwia cyberprzestępcom tworzenie fałszywych kart poprzez zakodowanie danych toru na nowej karcie z paskiem magnetycznym. Istnieją trzy kluczowe pytania kryminalistyczne dotyczące tego typu ataku: w jaki sposób złodzieje uzyskują dostęp do terminali POS i instalują skimmery na tak dużą skalę, w jaki sposób eksfiltrują zebrane dane i jak mogą to osiągnąć, unikając wykrycia przez monitorowanie bezpieczeństwa sterownica. Jeśli kradzież obejmuje współpracę z niejawnym pracownikiem, nierzetelnym i niemonitorowanym pracownikiem, wykonawcą lub sprzedawcą z autoryzowanym dostępem do infrastruktury POS detalisty, wówczas osoba ta wykorzystałaby zarówno dostęp, jak i wiedzę o systemie, aby zainstalować skimmer, ustalić zbiórkę i eksfiltrację procesu i oprogramowania, a także wyłączać, obchodzić lub w inny sposób pozostawać pod kontrolą zabezpieczeń. Jeśli złodziej jest osobą postronną bez autoryzowanego dostępu, jest prawdopodobne, że aktor zewnętrzny podejmie następujące czynności w skoordynowany, sekwencyjny sposób (na podstawie doświadczeń naszej firmy z naruszeniami danych):

1) Pierwsze wtargnięcie (uzyskanie dostępu do infrastruktury poprzez znalezienie, a następnie wykorzystanie luki w systemie lub urządzeniu, które było połączone z Internetem lub wykorzystanie błędu ludzkiego, który doprowadził do niezabezpieczonego skonfigurowania systemu);

2) Rozpoznanie (wykorzystywanie dostępu do infrastruktury do badania środowiska jako środka do zrozumienia mechanizmów kontroli bezpieczeństwa i identyfikacji docelowych aplikacji lub procesów biznesowych);

3) Atak (skup się na terminalach w punktach sprzedaży, zainstaluj narzędzia w odpowiedniej części procesu, aby umożliwić atakującemu przechwytywanie i rejestrowanie niezaszyfrowanych transakcji kartami kredytowymi i debetowymi);

4) Eksfiltracja (usuwanie przechwyconych informacji bez wykrycia); oraz

5) Pozostanie niewykrytym (wszystkie te czynności muszą być prowadzone bez złapania przez kontrole bezpieczeństwa w środowisku).

POŁĄCZONE ŚRODOWISKO – INTERNET RZECZY

RYZYKO WSPÓŁPRACY

Istnieje odpowiedni wzrost ryzyka, na które narażone są informacje znajdujące się w tych kanałach lub dostępne za ich pośrednictwem, ponieważ firmy wspierają produktywność poprzez szybką integrację BYOD, przetwarzania w chmurze i innych aspektów całkowitej mobilności. Według badania BYOD & Mobile Security 2016, jedna na pięć organizacji doświadczyła naruszenia bezpieczeństwa mobilnego, głównie z powodu złośliwego oprogramowania i złośliwego Wi-Fi. Ponieważ wyciek/utrata danych jest uważana za główny problem bezpieczeństwa związany z BYOD, zagrożenia bezpieczeństwa dla BYOD mogą nałożyć duże obciążenie na zasoby IT organizacji. Wzrasta również liczba ataków na podłączone urządzenia konsumenckie, takie jak elektroniczne nianie, domowe termostaty i telewizory, które składają się na Internet rzeczy (IoT), rodzący się ekosystem urządzeń łączących technologie informacyjne, operacyjne i konsumenckie. Te urządzenia połączone z Internetem są podatne na ataki, ponieważ nie mają podstawowych zabezpieczeń zweryfikowanych w niedawnym badaniu HP Security Research. Chociaż przetwarzanie w chmurze ma wiele zalet, wiąże się z ryzykiem podobnym do ryzyka związanego z outsourcingiem do dostawców zewnętrznych. Jednak w przeciwieństwie do dostawców zewnętrznych, podstawową działalnością dostawcy chmury jest przechowywanie krytycznych aplikacji i poufnych danych. W rezultacie bezpieczeństwo i prywatność danych są głównymi problemami

większości firm rozważających ich wykorzystanie. Firmy powinny wziąć pod uwagę związane z nimi ryzyko i zagrożenia, a także wielkość ryzyka, które są gotowe zaakceptować. Zagrożenia te obejmują niedostępność danych lub aplikacji, utratę danych, kradzież oraz nieautoryzowane ujawnienie poufnych informacji. Badanie EY Global Information Security Survey 2015 wykazało, że 60% organizacji dostrzega zwiększone ryzyko związane z korzystaniem w pracy z sieci społecznościowych, przetwarzania w chmurze i osobistych urządzeń mobilnych. W konsekwencji luki, w tym nieostrożni pracownicy, nieaktualne informacje, kontrole bezpieczeństwa, korzystanie z chmury, komputerów mobilnych i mediów społecznościowych oraz autoryzowany dostęp zwiększyły narażenie organizacji na ryzyko. Według badań Instytutu Ponemon organizacje powoli radzą sobie z zagrożeniami bezpieczeństwa IoT, chociaż liderzy bezpieczeństwa informacji przewidują, że IoT będzie jedną z najbardziej przełomowych technologii, ponieważ konsumenci przyjmują coraz więcej połączonych urządzeń. Poniższa tabela pokazuje, że większość respondentów nie wierzy, że jest gotowa na wpływ bezpieczeństwa IoT na ich organizacje. Według Cloud Security Alliance, Security Guidance for Early Adopters of the Internet of Things , tradycyjne rozwiązania bezpieczeństwa dla przedsiębiorstw nie rozwiązują w wystarczającym stopniu problemów związanych z bezpieczeństwem Internetu Rzeczy, ponieważ IoT wprowadził nowe wyzwania, w tym:

• Zwiększone obawy o prywatność, które często są mylące;

• Ograniczenia bezpieczeństwa platformy, które sprawiają, że podstawowe kontrole bezpieczeństwa stanowią wyzwanie;

• Wszechobecna mobilność, która sprawia, że śledzenie i zarządzanie aktywami jest wyzwaniem;

• Masowe ilości, które sprawiają, że rutynowe czynności aktualizacyjne i konserwacyjne stanowią wyzwanie, oraz

• Operacje w chmurze, które sprawiają, że ochrona granic jest mniej skuteczna

Ogólna koncepcja IoT została omówiona poniżej, a następnie kwestie związane z bezpieczeństwem wraz z kilkoma zaleceniami dotyczącymi typowych zagrożeń bezpieczeństwa.

DEFINICJA I ROZWÓJ

Termin „Internet rzeczy" stał się popularny w 1999 r., kiedy Kevin Ashton ukuł ten termin, aby zilustrować moc łączenia znaczników identyfikacji radiowej (RFID) używanych w korporacyjnych łańcuchach dostaw z Internetem w celu liczenia i śledzenia towarów bez potrzeby ludzka interwencja. Chociaż termin „Internet przedmiotów" jest stosunkowo nowy, koncepcja łączenia komputerów i sieci w celu monitorowania i kontrolowania urządzeń istnieje od dziesięcioleci. Według AFCEA International Cyber Committee, The Security Implication of the Internet of Thing, ogólny trend odchodzi od systemów, w których na urządzenie przypada wielu użytkowników (lub osób), osoby w pętli kontrolnej systemu oraz system zapewniający możliwość ludzie do interakcji z ludźmi. Przejście IoT stawia to na głowie, gdzie jest wiele urządzeń (lub setki) na użytkownika; urządzenia to rzeczy, które głównie rozmawiają z rzeczami; a interakcja dotyczy nie tylko użytkowników, ale realnych efektów fizycznych (np. zablokowanie drzwi, włączenie światła, zmiana temperatury w pomieszczeniu).

1960-1970 :

- Teleks

- Telegram

- Telefon

- Podstawowe teleprzetwarzanie

1980-1990:

- Podstawowe sieci

- Komórka

- Komputery osobiste

- System tablicy ogłoszeń

2000-teraz:

- Wszechobecny Internet

- Bezprzewodowe 2G do 4G

- IPv4 do IPv6

- GPS

Bliska przyszłość:

- Systemy autonomiczne

- Internet podłączony w domu i w samochodzie

Dzisiaj IoT stał się popularnym terminem opisującym połączenie urządzeń fizycznych, pojazdów, budynków i innych przedmiotów z elektroniką, oprogramowaniem, czujnikami i łącznością sieciową, które umożliwiają tym obiektom zbieranie i wymianę danych. Różne grupy używają różnych definicji, aby opisać lub promować określony pogląd na to, co oznacza IoT. Wszystkie poniższe definicje opisują scenariusze, w których łączność sieciowa i możliwości obliczeniowe rozciągają się na konstelację obiektów, urządzeń, czujników i przedmiotów codziennego użytku, które zwykle nie są uważane za „komputery"; pozwala to urządzeniom generować, wymieniać i konsumować dane, często przy minimalnej interwencji człowieka.

Definicja IoT

Internet. Architecture Board (IAB): Trend, w którym duża liczba urządzeń wbudowanych wykorzystuje usługi komunikacyjne oferowane przez protokoły internetowe. Wiele z tych urządzeń, często nazywanych „inteligentnymi obiektami", nie jest bezpośrednio obsługiwanych przez ludzi, ale istnieje jako komponenty w budynkach lub pojazdach lub jest rozproszonych w środowisku.

Internet Engineering Task Force (IETF): „Inteligentne sieci obiektów" są powszechnie używane w odniesieniu do Internetu Rzeczy. W tym kontekście „obiekty inteligentne" to urządzenia, które zazwyczaj mają znaczące ograniczenia, takie jak ograniczona moc, pamięć i zasoby przetwarzania lub przepustowość.

Międzynarodowy Związek Telekomunikacyjny (ITU) : Globalna infrastruktura dla społeczeństwa informacyjnego, umożliwiająca zaawansowane usługi poprzez łączenie (fizycznych i wirtualnych) rzeczy w oparciu o istniejące i rozwijające się interoperacyjne technologie informacyjne i komunikacyjne.

Słowniki oksfordzkie : Połączenie za pośrednictwem Internetu urządzeń komputerowych wbudowanych w przedmioty codziennego użytku, umożliwiające im wysyłanie i odbieranie danych.

Wdrażanie urządzeń IoT na dużą skalę obiecuje zmienić wiele aspektów naszego stylu życia. IoT obejmuje takie technologie, jak inteligentne sieci, inteligentne domy, inteligentny transport i inteligentne miasta. Od produktów konsumenckich, dóbr trwałych, samochodów osobowych i ciężarowych, komponentów przemysłowych i użytkowych po czujniki, urządzenia te są połączone z łącznością internetową. Na przykład urządzenia z dostępem do Internetu, komponenty automatyki domowej i urządzenia do zarządzania energią kierują nas w kierunku wizji „inteligentnego domu", oferującego większe bezpieczeństwo i efektywność energetyczną. Inne osobiste urządzenia IoT, takie jak ubieralne urządzenia do monitorowania kondycji i zdrowia oraz sieciowe urządzenia medyczne, zmieniają sposób świadczenia usług opieki zdrowotnej. McKinsey Global Institute opisuje szeroki zakres potencjalnych zastosowań w kategoriach „ustawień", w których oczekuje się, że IoT stworzy wartość dla przemysłu i użytkowników.

„Ustawienia" dla aplikacji IoT

Ustawienie : Opis : Przykład

Człowiek : Urządzenia przymocowane do ciała ludzkiego lub wewnątrz niego : Urządzenia (do noszenia i do spożycia) służące do monitorowania i utrzymywania zdrowia i dobrego samopoczucia człowieka; zarządzanie chorobami, zwiększona sprawność, wyższa produktywność

Home : Budynki, w których mieszkają ludzie : Kontrolery domu i systemy bezpieczeństwa

Środowisko handlu detalicznego: Przestrzenie, w których konsumenci prowadzą handel: sklepy, banki, restauracje, hale widowiskowe – wszędzie tam, gdzie konsumenci rozważają i kupują; kasa samoobsługowa, oferty sklepowe, optymalizacja stanów magazynowych

Biura: Przestrzenie, w których pracują pracownicy wiedzy: Zarządzanie energią i bezpieczeństwo w budynkach biurowych; poprawa produktywności, w tym dla pracowników mobilnych

Fabryki: Znormalizowane środowiska produkcyjne: Miejsca o powtarzalnych procedurach pracy, w tym szpitale i farmy; wydajność operacyjna, optymalizacja wykorzystania sprzętu i inwentaryzacji

Miejsca pracy: Niestandardowe środowiska produkcyjne: Górnictwo, ropa i gaz, budownictwo; wydajność operacyjna, konserwacja predykcyjna, BHP

Pojazdy: Systemy wewnątrz poruszających się pojazdów: Pojazdy, w tym samochody, ciężarówki, statki, samoloty i pociągi; konserwacja oparta na stanie, projektowanie oparte na użytkowaniu, analityka przedsprzedażowa

Miasta : Środowisko miejskie : Przestrzenie publiczne i infrastruktura w środowisku miejskim; adaptacyjna kontrola ruchu, inteligentne liczniki, ochrona środowiska, monitorowanie, zarządzanie zasobami

Na zewnątrz : Pomiędzy środowiskami miejskimi (i poza innymi ustawieniami): zastosowania zewnętrzne obejmują tory kolejowe, pojazdy autonomiczne (poza lokalizacjami miejskimi) i nawigację lotniczą; wyznaczanie tras w czasie rzeczywistym, połączona nawigacja, śledzenie przesyłek

Internet Rzeczy rozwija się obecnie na całym świecie, wykorzystując ogromną ekspansję adresów IP dzięki wdrożeniu przez operatora protokołu IPv6, który przenosi adresy internetowe z ograniczonej i starannie zarządzany zasób na nową platformę bez takich ograniczeń. Ta dramatyczna zmiana miejsca dała początek nowemu duchowi twórczemu, podobnie jak w pierwszych latach Internetu. IoT przeniknął wszystkie aspekty współczesnego życia, takie jak edukacja, opieka zdrowotna, administracja i biznes, umożliwiając przechowywanie poufnych informacji o osobach i firmach, transakcje na danych

finansowych, rozwój produktów i marketing. Urządzenia ubieralne, inteligentne urządzenia domowe, oświetlenie i inne inteligentne urządzenia stają się głównym nurtem, ponieważ oczekuje się, że popularność inteligentnych urządzeń konsumenckich będzie rosła w szalonym tempie w przyszłości. Przyjęcie IoT w sektorze biznesowym i publicznym będzie nadal rosło. Gminy na całym świecie również wdrażają IoT, starając się stać się inteligentnymi miastami, które opierają się na danych zebranych z tysięcy różnych czujników rozmieszczonych w regionie geograficznym. Z miliardami ludzi już połączonymi z Internetem, IoT reprezentuje poważną transformację w cyfrowym świecie, który ma potencjał, aby wpłynąć na wszystkich i każdą firmę. Szacuje się, że do 2020 roku będzie o 17,4 miliarda urządzeń więcej niż przewidywana liczba ludzi. Do roku 2020 7 miliardów ludzi i 30 miliardów urządzeń podłączonych do Internetu stworzy 44 zetabajty danych. Prognozy dotyczące wpływu IoT na internet i gospodarkę są imponujące, a niektórzy przewidują nawet 100 miliardów podłączonych urządzeń IoT i globalny wpływ ekonomiczny na ponad 11 bilionów dolarów do 2025 roku.

IPv6 i Internet Rzeczy

Chociaż różnią się one dokładnymi liczbami, większość technologii obserwatorzy są zgodni, że miliardy dodatkowych urządzeń – od czujników przemysłowych po sprzęt AGD i pojazdy – będą podłączone do Internetu do 2025 roku. móc polegać na protokole IPv4, protokole używanym obecnie przez większość usług internetowych. Będą potrzebować nowej technologii wspomagającej: IPv6. IPv6 to długo oczekiwana aktualizacja do pierwotnego podstawowego protokołu internetowego - protokołu internetowego (IP), który obsługuje całą komunikację w Internecie. IPv6 jest konieczne, ponieważ w Internecie kończą się oryginalne adresy IPv4. Podczas gdy IPv4 może obsługiwać 4,3 miliarda urządzeń podłączonych do Internetu, IPv6 z adresami zasilania od 2 do 128 jest praktycznie niewyczerpalny. Stanowi to około 340 bilionów, bilionów, bilionów adresów, co z nawiązką zaspokaja zapotrzebowanie szacowanych na 100 miliardów urządzeń IoT, które zostaną uruchomione w nadchodzących dziesięcioleciach. Biorąc pod uwagę przewidywaną żywotność niektórych czujników i innych urządzeń wymyślonych dla Internetu Rzeczy, decyzje projektowe będą miały wpływ na użyteczność rozwiązań za dziesięciolecia. Kluczowym wyzwaniem dla deweloperów IoT jest to, że IPv6 nie jest natywnie interoperacyjny z IPv4, a większość taniego oprogramowania, które jest łatwo dostępne do osadzania w urządzeniach IoT, implementuje tylko IPv4. Wielu ekspertów uważa jednak, że IPv6 jest najlepszą opcją łączności i pozwoli IoT osiągnąć swój potencjał.

PODATNOŚCI I ZAGROŻENIA

Ogromne rozpowszechnienie podłączonych urządzeń w IoT stworzyło ogromne zapotrzebowanie na solidne zabezpieczenia w odpowiedzi na rosnące zapotrzebowanie milionów, a być może miliardów podłączonych urządzeń i usług na całym świecie. Wszystko, od lodówek, elektronicznych niań po systemy tryskaczowe, jest okablowane i połączone ze sobą, a chociaż te urządzenia ułatwiły życie, stworzyły również nowe wektory ataków dla hakerów. Liczba zagrożeń rośnie z dnia na dzień, ponieważ liczba i złożoność ataków rośnie. Według M. Abomhara, Cybersecurity and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks, podłączone urządzenia lub maszyny są niezwykle podatne na cyberataki z następujących głównych powodów:

1) Większość urządzeń IoT działa bez nadzoru człowieka, dzięki czemu atakujący może łatwo uzyskać do nich fizyczny dostęp.

2) Większość komponentów IoT komunikuje się za pośrednictwem sieci bezprzewodowych, w których atakujący może uzyskać poufne informacje poprzez podsłuchiwanie.

3) Większość komponentów IoT nie obsługuje złożonych schematów bezpieczeństwa ze względu na niski pobór mocy i możliwości obliczeniowe.

Cyberzagrożenia mogą zostać skierowane przeciwko dowolnym zasobom i obiektom Internetu Rzeczy, powodując uszkodzenia lub uniemożliwiając działanie systemu, zagrażając ogólnej populacji lub powodując poważne szkody ekonomiczne dla właścicieli i użytkowników. Poniższa tabela zawiera przykłady nowych zagrożeń IoT i wektorów ataków zidentyfikowanych przez Cloud Security Alliance.

Przykłady nowych zagrożeń i wektorów ataków IoT

• Do systemów sterowania, pojazdów, a nawet ludzkiego ciała można uzyskać dostęp i manipulować nimi, powodując obrażenia lub gorzej, poprzez nieautoryzowany dostęp do fizycznych systemów wykrywania, uruchamiania i sterowania (w tym pojazdów, SCADA, wszczepialnych i niewszczepionych urządzeń medycznych, zakładów produkcyjnych i innych cybernetycznych -fizyczne implementacje IoT

• Świadczeniodawcy mogą niewłaściwie diagnozować i leczyć pacjentów na podstawie zmodyfikowanych informacji o stanie zdrowia lub zmanipulowanych danych z czujników

• Intruzi mogą uzyskać fizyczny dostęp do domów lub firm handlowych poprzez ataki na elektroniczne, zdalnie sterowane mechanizmy zamków drzwi

• Utrata kontroli nad pojazdem może być spowodowana przez odmowę usługi w stosunku do wewnętrznej komunikacji autobusowej

• Informacje krytyczne dla bezpieczeństwa, takie jak ostrzeżenia o zerwaniu przewodu gazowego, mogą pozostać niezauważone przez DDoS lub informacje z czujnika IoT

• Uszkodzenia infrastruktury krytycznej mogą wystąpić w wyniku obejścia funkcji krytycznych dla bezpieczeństwa lub regulacji zasilania/temperatury

• Złośliwe strony mogą kraść tożsamość i pieniądze na podstawie wycieku poufnych informacji, w tym osobistych informacji zdrowotnych (PHI)

• Nieoczekiwany wyciek danych osobowych lub poufnych może nastąpić w wyniku agregacji danych z wielu różnych systemów i czujników lub scalenia danych osobowych, które zostały zebrane zgodnie z różnymi preferencjami i oczekiwaniami dotyczącymi prywatności konsumentów

• Nieautoryzowane śledzenie lokalizacji osób może nastąpić poprzez śledzenie wzorców użytkowania na podstawie czasu i czasu użytkowania zasobów

• Nieautoryzowane śledzenie zachowań i działań ludzi może nastąpić poprzez badanie danych z detekcji opartych na lokalizacji, które ujawniają wzorce i umożliwiają analizę działań, często gromadzonych bez wyraźnego powiadomienia danej osoby

• Bezprawny nadzór dzięki możliwości trwałego zdalnego monitorowania oferowanego przez urządzenia IoT na małą skalę

• Nieodpowiednie profile i kategoryzację osób można tworzyć poprzez badanie sieci i śledzenia geograficznego oraz metadanych IoT

• Manipulowanie transakcjami finansowymi poprzez nieautoryzowany dostęp do POS i mPOS

• Strata pieniężna wynikająca z niemożności świadczenia usługi

• Wandalizm, kradzież lub zniszczenie zasobów IoT, które są rozmieszczone w odległych lokalizacjach i nie posiadają fizycznej kontroli bezpieczeństwa

• Możliwość uzyskania nieautoryzowanego dostępu do urządzeń brzegowych IoT w celu manipulowania danymi poprzez wykorzystanie wyzwań związanych z aktualizacją oprogramowania i

firmware urządzeń wbudowanych (np. wbudowanych w samochodach, domach, urządzeniach medycznych

• Możliwość uzyskania nieautoryzowanego dostępu do sieci Enterprise poprzez naruszenie urządzeń brzegowych IoT i wykorzystanie relacji zaufania

• Możliwość tworzenia botnetów poprzez narażanie na szwank dużej liczby urządzeń brzegowych IoT

• Możliwość podszywania się pod urządzenia IoT poprzez uzyskanie dostępu do materiału klucza przechowywanego w urządzeniach, które opierają się na opartych na oprogramowaniu magazynach zaufania

• Nieznane wykrywanie zhakowanych urządzeń w oparciu o kwestie bezpieczeństwa w łańcuchu dostaw IoT

Słabo zabezpieczone urządzenia i usługi IoT, które służą jako potencjalne punkty wejścia dla cyberataków, mogą narazić dane użytkownika na kradzież, pozostawiając nieodpowiednio chronione strumienie danych. Połączony charakter urządzeń IoT oznacza, że każde słabo zabezpieczone urządzenie podłączone do Internetu może potencjalnie wpłynąć na bezpieczeństwo i odporność Internetu na całym świecie. Ponieważ liczba podłączonych urządzeń IoT stale rośnie, obawy dotyczące bezpieczeństwa również rosną wykładniczo. Na przykład kilka problemów związanych z bezpieczeństwem pojedynczego urządzenia, takiego jak telefon komórkowy, może szybko przekształcić się w 10 lub 20 problemów, gdy rozważamy wiele urządzeń IoT w połączonym domu lub firmie. Ważne jest, aby zrozumieć ryzyko związane z bezpieczeństwem w świetle tego, do czego urządzenia IoT mają dostęp. Użytkownicy muszą wziąć pod uwagę następujące kluczowe czynniki podczas oceny zagrożeń bezpieczeństwa i technik łagodzenia:

* Jasne zrozumienie obecnych zagrożeń bezpieczeństwa i potencjalnych przyszłych zagrożeń

* Szacunkowe koszty ekonomiczne i inne szkody w przypadku zrealizowania ryzyka

* Szacunkowy koszt ograniczenia ryzyka

Chociaż tego rodzaju kompromisy w zakresie bezpieczeństwa są często dokonywane z perspektywy indywidualnego użytkownika lub organizacji, ważne jest rozważenie wzajemnych powiązań urządzeń IoT jako części większego ekosystemu IoT. Decyzje dotyczące bezpieczeństwa podejmowane lokalnie dotyczące urządzenia IoT mogą mieć globalny wpływ na inne urządzenia ze względu na charakter sieciowej łączności urządzeń IoT.

DALSZE ROZWAŻANIE

Internet rzeczy musi zmienić sposób, w jaki firmy prowadzą interesy

Przyjrzyj się swojej organizacji (publicznej lub prywatnej). Co możesz zrobić, czego wcześniej nie mogłeś? Zacznij to robić teraz, zanim zrobi to ktoś inny. „Działaj” zamiast „reaguj”. Rozważ te kluczowe pytania:

• Jakie możliwości IoT ma dzisiaj Twoja organizacja?

• Czy potrafisz wykorzystać uzupełniające się spostrzeżenia liderów usług i IT?

• Czy zidentyfikowałeś główne obszary możliwości IoT, które są powiązane z twoją wizją i strategią?

• Czy możesz zbudować „kulturę Internetu Rzeczy” wokół możliwości łączenia niepołączonych?

• Jak Internet Rzeczy zmieni podstawy konkurencji?

• Jak zadowolisz klientów, gdy wszystko zostanie połączone?

• Czy Twoje plany biznesowe odzwierciedlają pełny potencjał Internetu Rzeczy?

• Czy Twoje inwestycje technologiczne są dostosowane do szans i zagrożeń?

• W jaki sposób Internet Rzeczy poprawi Twoją sprawność?

• Czy masz możliwości dostarczania wartości z Internetu Rzeczy?

• Jaka jest Twoja struktura/model odpowiedzialności i zarządzania dla realizacji IoT?

• W jaki sposób rozwiązywane jest ryzyko związane z Internetem Rzeczy?

• W jaki sposób będziesz komunikować się z IoT z interesariuszami?

KWESTIE BEZPIECZEŃSTWA

Według Internet Society, The Internet of Things: An Overview, urządzenia IoT różnią się od tradycyjnych komputerów i urządzeń komputerowych pod następującymi względami, które zagrażają bezpieczeństwu:

Wiele urządzeń IoT jest zaprojektowanych do wdrażania na masową skalę. Dlatego też potencjalna ilość połączonych ze sobą połączeń pomiędzy tymi urządzeniami jest bezprecedensowa. Wiele z tych urządzeń będzie w stanie samodzielnie nawiązywać połączenia i komunikować się z innymi urządzeniami w nieprzewidywalny i dynamiczny sposób. W rezultacie istniejące narzędzia, metody i strategie związane z bezpieczeństwem IoT mogą wymagać nowego rozważenia.

Wiele wdrożeń IoT będzie składać się z kolekcji identycznych lub prawie identycznych urządzeń.

Ta jednorodność potęguje potencjalny wpływ każdej pojedynczej luki w zabezpieczeniach przez samą liczbę urządzeń, które mają te same cechy. Na przykład luka w zabezpieczeniach protokołu komunikacyjnego marki żarówek z dostępem do Internetu jednej firmy może obejmować każdą markę i model urządzenia, które korzysta z tego samego protokołu lub ma wspólne kluczowe cechy konstrukcyjne lub produkcyjne.

Wiele urządzeń IoT zostanie wdrożonych z oczekiwanym okresem eksploatacji dłuższym niż typowy sprzęt high-tech. Urządzenia te mogą być wdrażane w okolicznościach, które utrudniają lub uniemożliwiają ich ponowną konfigurację lub aktualizację; lub te urządzenia mogą przeżyć firmę, która je stworzyła, pozostawiając osierocone urządzenia bez możliwości długoterminowego wsparcia. Scenariusze te ilustrują, że mechanizmy bezpieczeństwa, które są odpowiednie podczas wdrażania, mogą nie być odpowiednie dla pełnego okresu eksploatacji urządzenia w miarę ewolucji zagrożeń bezpieczeństwa.

Wiele urządzeń IoT jest celowo zaprojektowanych bez możliwości aktualizacji lub proces aktualizacji jest uciążliwy lub niepraktyczny. Na przykład weźmy pod uwagę wycofanie 1,4 miliona pojazdów przez Fiata Chryslera w 2015 r. w celu naprawienia luki, która umożliwiała atakującemu włamanie się do pojazdu bezprzewodowo. Te samochody muszą zostać dostarczone do dealera Fiat Chrysler w celu ręcznej aktualizacji lub właściciel musi wykonać aktualizację samodzielnie za pomocą klucza USB. W rzeczywistości duży odsetek tych samochodów prawdopodobnie nie zostanie zmodernizowany, ponieważ proces modernizacji stanowi niedogodność dla właścicieli, narażając ich na nieustanną podatność na zagrożenia cyberbezpieczeństwa, zwłaszcza gdy samochód wydaje się dobrze radzić sobie w przeciwnym razie.

Wiele urządzeń IoT działa w sposób, w którym użytkownik ma niewielki lub żaden rzeczywisty wgląd w wewnętrzne działanie urządzenia lub precyzyjne strumienie danych, które wytwarza. Stwarza to lukę w zabezpieczeniach, gdy użytkownik sądzi, że urządzenie IoT wykonuje określone funkcje, podczas gdy w rzeczywistości może wykonywać niepożądane funkcje lub gromadzić więcej danych, niż zamierza użytkownik. Funkcje urządzenia mogą również ulec zmianie bez powiadomienia, gdy producent udostępni aktualizację, narażając użytkownika na wszelkie zmiany wprowadzane przez producenta.

Niektóre urządzenia IoT są zaprojektowane tak, aby były dyskretnie osadzone w środowisku, w którym użytkownik nie zauważa aktywnie urządzenia ani nie monitoruje jego stanu pracy. Co więcej, urządzenia mogą nie mieć jasnego sposobu na powiadomienie użytkownika, gdy pojawi się problem z bezpieczeństwem, co utrudnia użytkownikowi zorientowanie się, że doszło do naruszenia bezpieczeństwa urządzenia IoT. Naruszenie bezpieczeństwa może utrzymywać się przez długi czas, zanim zostanie zauważone i skorygowane, jeśli naprawa lub łagodzenie jest nawet możliwe lub praktyczne. Podobnie użytkownik może nie zdawać sobie sprawy, że w jego otoczeniu znajduje się czujnik, co potencjalnie pozwala na utrzymywanie się naruszenia bezpieczeństwa przez długi czas bez wykrycia. Open Web Application Security Project (OWASP) tworzy ogólnodostępne metodologie, dokumentację, narzędzia i technologie w dziedzinie bezpieczeństwa aplikacji internetowych i pracuje nad zapewnieniem wskazówek dotyczących bezpiecznego rozwoju dla producentów urządzeń IoT. Projekt IoT Top 10 OWASP ma na celu podniesienie świadomości na temat bezpieczeństwa aplikacji i zidentyfikowanie następujących problemów związanych z bezpieczeństwem, które należy złagodzić podczas opracowywania urządzeń IoT.

10 najważniejszych problemów bezpieczeństwa OWASP IoT

1) Niebezpieczny interfejs sieciowy

2) Niewystarczające uwierzytelnienie/autoryzacja

3) Niezabezpieczone usługi sieciowe

4) Brak szyfrowania transportu

5) Obawy dotyczące prywatności

6) Niebezpieczny interfejs chmury

7) Niepewny interfejs mobilny

8) Niewystarczająca konfiguracja zabezpieczeń

9) Ubezpiecz oprogramowanie/oprogramowanie układowe

10) Słabe bezpieczeństwo fizyczne

Niedawne badanie przeprowadzone przez HP Security Research potwierdza obawy OWASP dotyczące bezpieczeństwa IoT. Badanie internetowe HP dotyczące Internetu Rzeczy przeanalizowało 10 najczęściej używanych urządzeń w niektórych z najpopularniejszych nisz IoT, w tym producentów telewizorów, kamer internetowych, termostatów domowych, zdalnych gniazdek elektrycznych, sterowników zraszaczy, koncentratorów do sterowania wieloma urządzeniami, zamków do drzwi, alarmów domowych , wagi i otwieracze do bram garażowych. Badania ujawniają alarmująco wysoką średną liczbę luk dla każdego urządzenia. W poniższej tabeli wymieniono najczęstsze problemy z zabezpieczeniami.

Badanie HP IoT — zgłoszone wyniki

Obawy dotyczące prywatności :

• 80% przetestowanych urządzeń IoT, wraz z odpowiadającymi im komponentami chmury i aplikacji mobilnych, wzbudziło obawy dotyczące prywatności w zakresie gromadzenia danych konsumenckich, takich jak imię i nazwisko, adres e-mail, data urodzenia, dane uwierzytelniające karty kredytowej i informacje o stanie zdrowia.

• 90% przetestowanych urządzeń IoT zebrało co najmniej jedną informację osobistą za pośrednictwem samego produktu, chmury lub aplikacji mobilnej.

Niewystarczająca autoryzacja:

• 80% ocenianych urządzeń IoT wraz z komponentami chmurowymi i mobilnymi nie wymagało haseł o wystarczającej złożoności i długości, przy czym większość zezwalała na hasła, takie jak „1234" lub „123456".

• Wiele kont skonfigurowanych przez HP ze słabymi hasłami było również używanych w witrynach internetowych w chmurze oraz w aplikacji mobilnej produktu. Silna polityka haseł to Security 101 i większość rozwiązań nie powiodła się.

Brak szyfrowania transportu:

70% przeanalizowanych urządzeń IoT nie szyfrowało komunikacji z Internetem i siecią lokalną, podczas gdy połowa aplikacji mobilnych urządzeń wykonywała nieszyfrowaną komunikację z chmurą, Internetem lub siecią lokalną.

Niebezpieczny interfejs sieciowy :

• 60% urządzeń IoT oceniło zgłoszone problemy dotyczące bezpieczeństwa w interfejsie użytkownika, takie jak trwałe skrypty międzylokacyjne, słabe zarządzanie sesjami i słabe domyślne dane uwierzytelniające.

• 70% urządzeń z komponentami chmurowymi i mobilnymi umożliwiłoby potencjalnemu napastnikowi określenie ważnych kont użytkowników poprzez wyliczanie kont lub funkcje resetowania hasła.

Nieodpowiednia ochrona oprogramowania:

• 60% urządzeń nie korzystało z szyfrowania podczas pobierania aktualizacji oprogramowania, co jest liczbą alarmującą, biorąc pod uwagę, że oprogramowanie zasila funkcjonalność testowanych urządzeń.

Firma HP sugeruje następujące kluczowe działania, które producenci tych urządzeń mogą teraz podjąć w celu zabezpieczenia tych urządzeń.

* Przeprowadzenie przeglądu bezpieczeństwa urządzenia i wszystkich powiązanych komponentów

* Wdrożenie standardów bezpieczeństwa, które muszą spełniać wszystkie urządzenia przed produkcją

* Zapewnienie, że bezpieczeństwo jest brane pod uwagę w cyklu życia produktu

WZGLĘDY NA KONTROLE BEZPIECZEŃSTWA

IoT będzie w coraz większym stopniu wyposażony w narzędzia do wykrywania, analizy i wizualizacji, do których będzie można uzyskać dostęp na poziomie osobistym, społecznościowym lub krajowym. Jednak udostępnianie informacji i łatwość dostępu za pośrednictwem IoT sprawiają, że firmy są podatne na ukierunkowane cyberataki, więc ogromne korzyści należy zestawić z rosnącym ryzykiem. Organizacje muszą się dostosować i patrzeć w przyszłość i poza obecną działalność. Rozumiejąc, że

atakom nigdy nie można w pełni zapobiec, firmy powinny rozwijać swoje możliwości wykrywania cyberzagrożeń, aby móc odpowiednio i proaktywnie reagować. Aby wdrożyć skuteczne mechanizmy kontroli bezpieczeństwa IoT, organizacje powinny być świadome następujących podstawowych celów bezpieczeństwa. Cloud Security Alliance zaleca następujące kluczowe kontrole wdrażania możliwości IoT. Te mechanizmy kontrolne pozwalają organizacjom ograniczać ryzyko związane z tą nową technologią.

Podstawowe cele bezpieczeństwa IoT

* Zachowaj poufność i integralność zarówno danych biznesowych, jak i osobistych gromadzonych w ramach IoT poprzez zapewnienie szyfrowania, uwierzytelniania i ochrony integralności w całej infrastrukturze IoT;

* Zrozum i rozwiąż obawy interesariuszy dotyczące prywatności przed wdrożeniem funkcji Internetu Rzeczy, przeprowadzając ocenę wpływu na prywatność;

* Chroń infrastrukturę przed atakami, których celem jest IoT jako wektor do aktywów organizacji, dzięki wykorzystaniu kontroli cyklu życia urządzeń IoT i warstwowemu podejściu do bezpieczeństwa oraz

* Zainicjuj globalne podejście do zwalczania zagrożeń bezpieczeństwa, dzieląc się informacjami o zagrożeniach z dostawcami zabezpieczeń, partnerami z branży i Cloud Security Alliance

Kontrola: Opis

1: Przeanalizuj wpływ na prywatność interesariuszy i zastosuj podejście Privacy-by-Design do opracowywania i wdrażania IoT

2: Zastosuj bezpieczne podejście inżynieryjne do projektowania i wdrażania nowego systemu IoT.

3: Wdrożenie warstwowych zabezpieczeń w celu ochrony zasobów Internetu Rzeczy

4: Wdrożenie najlepszych praktyk w zakresie ochrony danych w celu ochrony poufnych informacji

5: Zdefiniuj kontrolki cyklu życia dla urządzeń IoT

6: Zdefiniuj i zaimplementuj ramy uwierzytelniania/autoryzacji dla wdrożeń IoT w organizacji

7 : Zdefiniuj ramy rejestrowania i audytu dla ekosystemu IoT organizacji.

1. Przeanalizuj wpływ na prywatność interesariuszy i zastosuj podejście Privacy-by-Design do opracowywania i wdrażania Internetu Rzeczy. Ważne jest, aby rozważyć potencjalne konsekwencje dla prywatności wszystkich interesariuszy przed wprowadzeniem systemu w stan operacyjny, zwłaszcza te komponenty IoT będą wszechobecne w przestrzeni publicznej, a także w domach prywatnych, a w niektórych przypadkach nawet noszone przez osoby fizyczne. Na przykład, projektując aplikacje, które śledzą połączone pojazdy, organizacje powinny zrozumieć, czy śledzenie ujawniłoby wzorce jazdy, które można by prześledzić do osoby lub grupy w połączeniu z danymi zebranymi przez inne systemy. Aby zapewnić ochronę poufnych informacji interesariuszy, organizacje powinny stosować następujące podejścia podczas projektowania systemu IoT:

* Zbierane typy danych są analizowane, aby zrozumieć, które z nich są wrażliwe i jakie przepisy mają zastosowanie do każdego typu danych.

* Przeprowadzana jest bardziej dogłębna analiza w celu zrozumienia pośrednich konsekwencji związanych z prywatnością dla różnych operacji komponentu IoT.

W 2014 r. Grupa Robocza ds. Ochrony Danych Unii Europejskiej (UE) wydała wytyczne, zgodnie z którymi wszyscy interesariusze Internetu Rzeczy powinni przyjąć zasady ochrony prywatności od samego początku wdrożeń w dowolnym regionie świata. Wytyczne UE-29 wskazują również na zalecane ramy przeprowadzania oceny wpływu na prywatność (PIA):

„Jeśli okaże się, że urządzenie gromadzi, przetwarza lub przechowuje informacje chronione prywatnością (PPI), wymagane będą bardziej rygorystyczne kontrole. Kontrole te powinny być połączeniem kontroli opartej na polityce i technicznej. Na przykład:

- Udostępnienie urządzenia może wymagać większej liczby zgód administracyjnych

- Należy przeprowadzić przegląd przez audyt wewnętrzny lub zgodność w celu ustalenia, czy możliwe jest posiadanie danych PPI na urządzeniach IoT

- Dane przechowywane na urządzeniu powinny być szyfrowane przy użyciu odpowiednio silnych algorytmów kryptograficznych

- Dane przesyłane z/do urządzenia powinny być szyfrowane przy użyciu odpowiednio silnych algorytmów kryptograficznych

- Dostęp do urządzenia, zarówno fizyczny, jak i logiczny, powinien być ograniczony do upoważnionego personelu ”

W 2014 roku przewodniczący Federalnej Komisji Handlu (FTC) zauważył, że interesariusze Internetu Rzeczy mają obowiązek:

„Włącz bezpieczeństwo w proces rozwoju produktu, aby zebrać minimalną ilość danych, a także powiadomić konsumentów o nieoczekiwanym wykorzystaniu ich danych i zapewnić uproszczone wybory dotyczące tego zastosowania”

Organizacje powinny wziąć to pod uwagę, aby upewnić się, że mają wbudowane mechanizmy kontroli prywatności w swoich systemach IoT, oprócz mechanizmów kontroli prywatności specyficznych dla urządzenia lub aplikacji zapewnianych przez dowolnego dostawcę IoT. Odpowiednie zabezpieczenia powinny być zaprojektowane w systemie IoT od samego początku, a nie po zgłoszeniu lub wykorzystaniu obaw dotyczących prywatności. Organizacje powinny również ponownie ocenić swój program powiadamiania o naruszeniu danych osobowych, aby zapewnić, że uwzględnione zostały obszary związane z Internetem Rzeczy. Ponadto, ponieważ gromadzone dane będą miały długi okres istnienia w ramach Internetu Rzeczy, organizacje powinny rozważyć pełny okres gromadzonych danych, zarówno w organizacji zbierającej, jak i wśród osób trzecich, którym są one dostarczane. Zainteresowane strony powinny zostać poinformowane o tym, kiedy dane są przekazywane stronom trzecim, jakie mechanizmy kontrolne służą do ich zabezpieczania oraz jak i kiedy usuwa się dane. Istnieją różne zalecenia dotyczące wymagań dotyczących prywatności, które należy wziąć pod uwagę w zależności od regionu, w tym:

• Ameryka Północna: Internet rzeczy, prywatność i bezpieczeństwo w połączonym świecie, raport pracowników Federalnej Komisji Handlu (FTC)

• Europa: Zalecenia dotyczące prywatności dla Internetu Rzeczy, Grupa Robocza Art. 29 UE (europejski organ doradczy ds. ochrony danych)

2. Zastosuj bezpieczne podejście inżynieryjne do projektowania i wdrażania nowego systemu IoT. Organizacje powinny zdefiniować i wprowadzić wymagania bezpieczeństwa do projektów, aby uwzględnić implementację funkcji bezpieczeństwa przed wdrożeniem. Modelowanie zagrożeń oparte

na Microsoft SDL definiuje kompleksowe podejście, wykorzystując następujące kroki w celu określenia wagi zagrożeń wprowadzonych przez nowy system.

Modelowanie zagrożeń

Krok 1: Zidentyfikuj zasoby

- Skataloguj różne komponenty systemu IoT, które będą rozmieszczone.

- Weź pod uwagę nie tylko urządzenia IoT, ale także magazyny danych i aplikacje, z którymi komunikują się urządzenia, oraz użytkowników, którzy wchodzą w interakcję z systemem.

Krok 2: Utwórz przegląd systemu/architektury

- Dokumentuj oczekiwaną funkcjonalność systemu IoT.

- Rozważ i udokumentuj przypadki niewłaściwego użycia systemu.

- Utwórz diagram architektoniczny, który szczegółowo opisuje nowy system IoT oraz sposób, w jaki system łączy się z innymi zasobami obliczeniowymi przedsiębiorstwa i systemami bezpieczeństwa.

- Użyj diagramu, aby zidentyfikować granice zaufania, mechanizmy uwierzytelniania i autoryzacji.

- Zidentyfikuj i zbadaj konkretne technologie, które będą się składać system Internetu Rzeczy.

Krok 3: Rozkładanie systemu IoT

- Zapoznaj się z cyklem życia danych przepływających przez system.

- Rozwiń to zrozumienie, aby zidentyfikować słabe lub słabe punkty w architekturze bezpieczeństwa, którymi należy się zająć.

- Zidentyfikuj i udokumentuj punkty wejścia danych w systemie

- Śledź przepływ danych z punktów wejścia i udokumentuj różne komponenty, które wchodzą w interakcję z tymi danymi w całym systemie.

- Zidentyfikuj cele o wysokim profilu dla atakujących — mogą to być punkty w systemie, które agregują lub przechowują dane, lub mogą to być czujniki o wysokiej wartości, które wymagają znacznych zabezpieczeń w celu utrzymania ogólnej integralności systemu.

Krok 4: Zidentyfikuj i udokumentuj zagrożenia

- Popularny model STRIDE można zastosować do wdrożeń systemów IoT.

- Korzystaj z dobrze znanych repozytoriów luk w zabezpieczeniach, aby lepiej zrozumieć środowisko, takich jak baza danych Common Vulnerabilities and Exposures firmy MITRE.

- Odkryj unikalne zagrożenia dla tworzenia instancji IoT, takie jak identyfikacja fałszowania, manipulowanie danymi, odrzucenie, ujawnienie informacji i odmowa usługi.

Krok 5: Oceń zagrożenia

- Ocena prawdopodobieństwa i wpływu każdego zagrożenia zidentyfikowanego w poprzednim kroku umożliwia przydzielenie odpowiednich poziomów inwestycji w celu złagodzenia każdego zagrożenia.

- Na tym etapie można zastosować dowolną standardową metodologię oceny zagrożeń, w tym metodę DREAD firmy Microsoft.

3. Wdrożenie warstwowych zabezpieczeń w celu ochrony zasobów Internetu Rzeczy. Warstwy bezpieczeństwa w cyfrowym świecie mają kluczowe znaczenie. Na przykład wiadomość e-mail, która przedostaje się przez firmową zaporę sieciową, zostanie zatrzymana przez program antywirusowy serwera pocztowego, a jeśli przejdzie przez to, powinna zostać zatrzymana przez program antywirusowy stacji roboczej. Dlatego na etapie projektowania należy poważnie rozważyć modelowanie zagrożeń architektury IoT, w tym aktorów/role, używane komponenty, punkty wejścia i wyjścia danych we wszystkich warstwach wymienionych poniżej, w tym w warstwie urządzenia. Należy przemyśleć różne scenariusze zagrożeń z licznymi przypadkami nadużyć, a następnie przekazać je zespołowi programistów do opracowania, stosując najlepsze praktyki w zakresie bezpieczeństwa, a następnie przeprowadzając testy bezpieczeństwa. Bezpieczeństwo musi być dokładnie przemyślane na wszystkich kolejnych warstwach, ponieważ jedna lub dwie bezpieczne warstwy nie wystarczą, aby zapewnić w pełni bezpieczną implementację.

Najważniejsze wskazówki dotyczące najlepszych praktyk w zakresie bezpieczeństwa

Warstwa sieci :

* Zapory są zaprojektowane do filtrowania ruchu na podstawie typu, portu i miejsca docelowego. Zapory ogniowe ewoluowały poprzez włączenie głębszych analiz, takich jak IPS i usługi inspekcji ruchu, umożliwiając im dokładniejsze wgląd w pakiety i lepsze wykrywanie złośliwego ruchu.

* Często skanuj w poszukiwaniu otwartych portów w firewallach i routerach. Otwarte porty to zaproszenie dla hakerów.

* Sprawdź, czy routery są podatne na źle skonfigurowane usługi NAT-Port Mapping Protocol (NAT-PMP). NAT-PMP to protokół, który nie ma wbudowanego mechanizmu uwierzytelniania i ufa wszystkim hostom należącym do sieci lokalnej routera, dzięki czemu mogą swobodnie „przebijać" dziury przez zaporę.

* Ćwicz kontrolę dostępu do sieci (NAC) w celu ujednolicenia bezpieczeństwa punktów końcowych

technologii, takich jak oprogramowanie antywirusowe i zapobieganie włamaniom do hosta. Produkty antywirusowe chronią komputery przed złośliwym oprogramowaniem, na przykład opierając się na porównaniach z sygnaturami plików.

* Okresowo przeprowadzaj oceny podatności i upewnij się, że uwierzytelnianie użytkowników i systemów w sieci jest zgodne z zasadami bezpieczeństwa organizacji.

Warstwa aplikacji :

* Sprawdź, czy nie ma luk w zabezpieczeniach cross-site scripting (XSS) lub Cross Site Request Forgery (CSRF). CSRF to rodzaj ataku złośliwej witryny internetowej, poczty e-mail, bloga, wiadomości błyskawicznej lub programu, który powoduje, że przeglądarka wykonuje niepożądane działanie na zaufanej witrynie.

* Poproś o raport z przeglądu kodu zabezpieczającego od dostawcy w przypadku jakichkolwiek luk, które zostały wykryte podczas rozwoju platformy IoT i związanej z nimi naprawy.

* Użyj szyfrowania danych w spoczynku. Zapewnij prywatność danych podczas transportu, stosując silne szyfrowanie. Dodaj sól lub losowe dane do zaszyfrowanych danych, aby utrudnić hakowanie.

Poziom urządzenia :

* Przeskanuj pliki lub sprawdź ich integralność przed zainstalowaniem ich w urządzeniu.

* Zmień domyślne hasła parowania dla urządzeń Bluetooth.

* Zmień domyślne hasło i zaimplementuj silną politykę haseł.

* Wzmocnij urządzenie, zmieniając jego domyślną konfigurację, a nie tylko hasło.

* Urządzenia i czujniki muszą być okresowo testowane, aby zapewnić prawidłowe działanie.

Warstwa fizyczna :

* Powinny istnieć zarządzanie infrastrukturą zarządzania tożsamością fizyczną i dostępem. Tylko upoważnione osoby powinny mieć dostęp do bezpiecznych obszarów, takich jak centra danych, laboratoria i obszary, w których urządzenia mają kluczowe znaczenie.

* Kamery monitorujące powinny być używane do śledzenia urządzeń rozmieszczonych na danym obszarze. Kamery powinny być w stanie obracać się w lewo i w prawo, aby skanować obszar, w którym zaimplementowano urządzenia i czujniki.

* Dokument, w którym znajdują się urządzenia. Jeśli to możliwe, opracuj graficzną mapę pokazującą, gdzie w budynku znajdują się zasoby IoT.

Warstwa ludzka :

* Wyznacz kilku przywódców, którzy są ewangelistami bezpieczeństwa. Osoby te powinny mieć osobowość i motywację, aby być w czołówce, aby inicjatywa IoT działała pomyślnie przy jak najmniejszej liczbie wyzwań związanych z bezpieczeństwem.

* Nieustannie szkol personel w kwestiach, aby uniknąć spadania na zbyt dobre, by były prawdziwe oferty, a nawet niechciane oferty, które wyglądają jak uzasadnione prośby biznesowe.

* Użytkownicy powinni być przeszkoleni w zakresie weryfikowania reputacji wszelkich pobrań z Internetu.

* Szkolenie użytkowników końcowych, w jaki sposób mogą pomóc w zabezpieczaniu urządzeń mobilnych, na przykład w przypadku wyżej wymienionych praktyk blokad i silnych haseł.

4. Wdrożenie najlepszych praktyk w zakresie ochrony danych w celu ochrony poufnych informacji. Ochrona danych w różnych ich stanach wymaga zastosowania szyfrowania. Istnieje wiele prymitywów kryptograficznych, takich jak szyfrowanie, integralność i uwierzytelnianie, dostępnych w różnych bibliotekach oprogramowania kryptograficznego i modułach sprzętowych. Poziom bezpieczeństwa i wydajność to dwa podstawowe czynniki, które należy wziąć pod uwagę przy wyborze pakietu kryptograficznego do ochrony informacji. Wydajność jest szczególnie istotna w przypadku ograniczonych, typowo wbudowanych urządzeń typowych dla IoT. Identyfikacja algorytmów kryptograficznych i rozmiarów kluczy do obsługi w urządzeniu IoT to tylko jeden z elementów kryptograficznej układanki. Algorytmy te muszą być w stanie działać w zaufanym środowisku, a klucze są przechowywane w bezpiecznych kontenerach. Ponadto potrzebne są polityki i deklaracje dotyczące własności danych w następujących obszarach:

- Bezpieczeństwo danych w spoczynku (DAR)

- Bezpieczeństwo danych w tranzycie (DIT)

- Bezpieczeństwo danych w użyciu (DIU)

- Zapobieganie utracie danych (DLP)

- Zasady integralności danych i agregacji

5. Zdefiniuj kontrole bezpieczeństwa cyklu życia dla urządzeń IoT. Kontrole cyklu życia urządzeń brzegowych IoT wymagają zarządzania zasobami i monitorowania ich w celu zapewnienia, że są one autoryzowane, bezpieczne i regularnie aktualizowane za pomocą najnowszego oprogramowania układowego, oprogramowania i poprawek. Ponadto organizacja musi posiadać udokumentowaną metodę bezpiecznej utylizacji zasobów Internetu Rzeczy pod koniec cyklu życia. Cykl życia zabezpieczeń IoT obejmuje planowanie, wdrażanie, zarządzanie, monitorowanie, wykrywanie i usuwanie. Najważniejsze z tych faz są omówione w kolejnych sekcjach.

Plan: W przypadku każdego wdrożenia IoT organizacje powinny określić odpowiednie interfejsy do istniejącego sprzętu zabezpieczającego, aktualizując architektury sieci w celu segmentacji określonych enklaw IoT. Przykłady planowania na różnych etapach, w tym:

* Planowanie komunikacji (np. lokalizacja urządzenia, podstawa IPv6 i plan przejścia)

* Planowanie bezpieczeństwa fizycznego (np. gdzie jest urządzenie; magazyn; co to jest kontrola dostępu?)

* Logiczne planowanie bezpieczeństwa (plan strefy bezpieczeństwa)

* Plan uwierzytelniania/autoryzacji (np. role, usługi i macierz kontroli dostępu dla każdego typu urządzenia)

* Plan udostępniania informacji (np. jakie dane mogą być udostępniane? Jakie dane będą udostępniane? Jaka jest kontrola prywatności tych danych?)

Wdrażanie: Proces wdrażania obejmuje następujące procedury:

• Bezpieczne konfiguracje dla systemów operacyjnych urządzeń brzegowych IoT

• Ustal tożsamość urządzenia (konta i certyfikaty); Urządzenia dokumentacyjne i inwentaryzacyjne (zarządzanie majątkiem)

• Wstępne zapewnienie kluczowych relacji materiałowych i powierniczych

• Weryfikacja i walidacja bezpieczeństwa operacyjnego (V&V):

– Czy przechwytujesz potrzebne dane audytu?

-- Czy konta są wystarczająco zablokowane itp.?

• Testy negatywne (opcjonalnie)

• Wdróż bramy w razie potrzeby

Zarządzanie: Zarządzanie urządzeniami IoT obejmuje zarządzanie samymi urządzeniami brzegowymi, oprogramowaniem i oprogramowaniem układowym ładowanym na te urządzenia brzegowe, licencjami oraz stosowaniem rutynowych aktualizacji poprawek w celu ograniczenia luk w zabezpieczeniach urządzeń. IoT to nie tylko urządzenia brzegowe, które zbierają i przesyłają dane, ale także łącza transportowe, które przenoszą te dane, systemy przetwarzające dane i systemy korzystające z danych. Śledzenie wersji oprogramowania tych aplikacji i systemów w celu zapewnienia ich aktualizacji jest ważne dla zarządzania licencjami.

Monitoruj i wykrywaj: Na tym etapie istnieją dwa kluczowe czynniki:

1) Zautomatyzuj zadania związane z bezpieczeństwem, takie jak oceny podatności i formy testów penetracyjnych

2) Rozwijanie dynamicznego i ciągłego monitorowania urządzeń w czasie rzeczywistym w celu zautomatyzowania analizy zagrożeń IoT

Specjaliści ds. bezpieczeństwa są zwykle przeciążeni zabezpieczaniem wielu aplikacji i urządzeń w danym momencie. Na przykład na każdego specjalistę ds. bezpieczeństwa przypada 50-60 programistów kodu aplikacji, którzy mogą tworzyć kod z potencjalnymi lukami w zabezpieczeniach. W rezultacie stare metody ręcznego testowania penetracji i kwartalnych przeglądów bezpieczeństwa nie są już wystarczające. Istnieje potrzeba regularnego automatyzowania ręcznego testowania bezpieczeństwa przy użyciu narzędzi do dynamicznego monitorowania. Należy również monitorować zdarzenia związane z bezpieczeństwem w infrastrukturze IoT, najlepiej 24 godziny na dobę, 7 dni w tygodniu. Planowanie przechwytywania danych istotnych z punktu widzenia bezpieczeństwa oraz ustalanie zasad identyfikowania zdarzeń lub kombinacji zdarzeń będących przedmiotem zainteresowania należy przeprowadzać na wczesnym etapie inżynieryjnego cyklu życia.

Dysponowanie:

Jest prawdopodobne, że wiele urządzeń brzegowych będzie regularnie wymienianych ze względu na ilość związaną z wieloma wdrożeniami IoT. Dlatego organizacje powinny ustanowić zasady i procedury bezpiecznej utylizacji urządzeń, w których przechowywano poufne informacje lub kluczowe materiały, które mogą zapewnić dostęp do poufnych informacji. Urządzenia, na których znajdowały się poufne informacje, należy bezpiecznie wyczyścić, aby uwzględnić usunięcie materiału klucza i certyfikatów z każdego urządzenia.

6. Zdefiniuj i zaimplementuj ramy uwierzytelniania/autoryzacji dla wdrożeń IoT organizacji. Istnieje wiele scenariuszy uwierzytelniania IoT. Na przykład komponenty IoT mogą:

* Komunikuj się ze sobą, wymagając uwierzytelniania maszyna-maszyna (m2m).

* Komunikuj się z aplikacjami w chmurze, aplikacjami mobilnymi, aplikacjami internetowymi, a nawet bezpośrednio z ludźmi.

Jednym z wyzwań związanych z uwierzytelnianiem i autoryzacją w IoT jest to, że wiele urządzeń będzie działać w ograniczonych warunkach, w których stosowane protokoły mogą ograniczać opcje uwierzytelniania lub że urządzenia nie będą w stanie korzystać z pewnych funkcji uwierzytelniania. Dostępnych jest wiele opcji uwierzytelniania IoT. Te opcje zazwyczaj obejmują:

* Wstępnie udostępniony klucz/wspólny klucz tajny

* Uwierzytelnianie oparte na certyfikatach

* Uwierzytelnianie oparte na tokenach

Według Cloud Security Alliance wybrana metoda uwierzytelniania zależy od ograniczeń urządzenia. Uwierzytelnianie współdzielonego tajnego jest uważane za mniej pożądaną alternatywę dla uwierzytelniania opartego na certyfikatach. W przypadku współdzielonych wpisów tajnych obciążenie związane z zarządzaniem wpisami tajnymi staje się znaczące wraz ze wzrostem liczby urządzeń. Uwierzytelnianie oparte na certyfikatach wprowadza obawy związane z przetwarzaniem certyfikatów i algorytmami asymetrycznymi używanymi do funkcji takich jak ustanawianie uwierzytelnienia kluczem. Struktura certyfikatu jest zoptymalizowana dla urządzeń z ograniczoną pamięcią Deweloperzy powinni rozważyć możliwość przejścia na certyfikaty IEEE 1609.3 w przypadku urządzeń

i środowisk o ograniczonej dostępności. Schematy uwierzytelniania oparte na tokenach zapewniają użyteczne alternatywy dla wspólnych sekretów i certyfikatów, pozwalając na wprowadzenie kompleksowych kontroli zasad stosowanych do wymagań dostępu IoT. Proces wyboru optymalnych mechanizmów uwierzytelniania dla wdrożenia IoT można poprowadzić, odpowiadając na następujący zestaw pytań.

Rozważania dotyczące wyboru optymalnych mechanizmów uwierzytelniania do wdrażania IOT

Czy Twoja implementacja wymaga komunikacji maszyna-maszyna? : Jeśli tak, sprawdź protokoły komunikacyjne urządzenia i określ, czy natywnie obsługują uwierzytelnianie.

Czy Twoje urządzenia IoT obsługują jeden z protokołów komunikacyjnych, który zapewnia usługi uwierzytelniania? : Jeśli nie, rozważ zabezpieczenia warstwowe, aby uwzględnić usługi uwierzytelniania wyższego poziomu, takie jak TLS lub DTLS.

Czy zasoby Twoich urządzeń IoT są ograniczone pamięcią lub mocą obliczeniową? : Jeśli tak, rozważ współpracę z dostawcami w celu obsługi certyfikatów IEEE 1609.3

Kto będzie zarządzał Twoimi urządzeniami? Czy wymagane jest zdalne zarządzanie? :

Utwórz macierz uwierzytelniania i kontroli dostępu i wybierz najsilniejszą metodę uwierzytelniania obsługiwaną przez każde urządzenie brzegowe.

Czy Twoje urządzenia IoT ujawniają funkcje zdalnego zarządzania oparte na sieci, takie jak SNMP lub SSH? : Zablokuj każde urządzenie przed uruchomieniem, aby obsługiwać tylko autoryzowane usługi zarządzania. Ustal zasady i procedury zdalnego zarządzania urządzeniami przez sieć.

Czy Twoje urządzenia IoT implementują interfejsy RESTful? : Rozważ podejście oparte na tokenach, takie jak OAUTH 2 do uwierzytelniania urządzeń brzegowych.

Czy urządzenia łączą się bezpośrednio z usługami w chmurze? : Upewnij się, że projekt uwierzytelniania zawiera klucze API, które obsługują uwierzytelnianie urządzeń i aplikacji w usłudze w chmurze.

7. Zdefiniuj ramy rejestrowania i audytu dla ekosystemu IoT organizacji. Organizacje powinny dokonać rozróżnienia między danymi operacyjnymi, które są przechwytywane i przesyłane przez urządzenie IoT, a danymi audytu bezpieczeństwa wymaganymi do utrzymania świadomości bezpieczeństwa urządzenia. Dane operacyjne, na przykład temperatura wody zbierane przez czujnik temperatury, niekoniecznie są istotne dla bezpieczeństwa i jako takie nie powinny być wykorzystywane do agregacji i analizy. Ogólnie rzecz biorąc, ważne jest rejestrowanie danych, które mogą wskazywać na wystąpienie lub wystąpienie incydentu. W miarę możliwości należy rejestrować następujące minimalne elementy danych.

Zdarzenia do rejestrowania

• Nieudane próby podwyższenia uprawnień

• Nieudane logowanie do urządzenia

• Nieudane logowanie do usługodawcy (chmura)

• Nieudane próby uwierzytelniania urządzenie-urządzenie

• Nieudane próby dostępu do bazy danych

• Zmiany w polityce

- Korzystanie z uprawnień
- Tworzenie konta
- Zmiana konta
- Nieudana negocjacja tunelu
- Stan wewnętrzny
- Wł./Wył.
- Zmiany w integralności odpowiednich systemów plików

Metadane do rejestrowania

- Czas rozpoczęcia
- Koniec czasu
- Użytkownik
- Identyfikator urządzenia równorzędnego
- Adres MAC urządzenia docelowego
- Adres IP urządzenia docelowego
- Adres IPv6 urządzenia docelowego
- Nazwa hosta urządzenia docelowego
- Protokół transportowy
- Protokół łącza danych