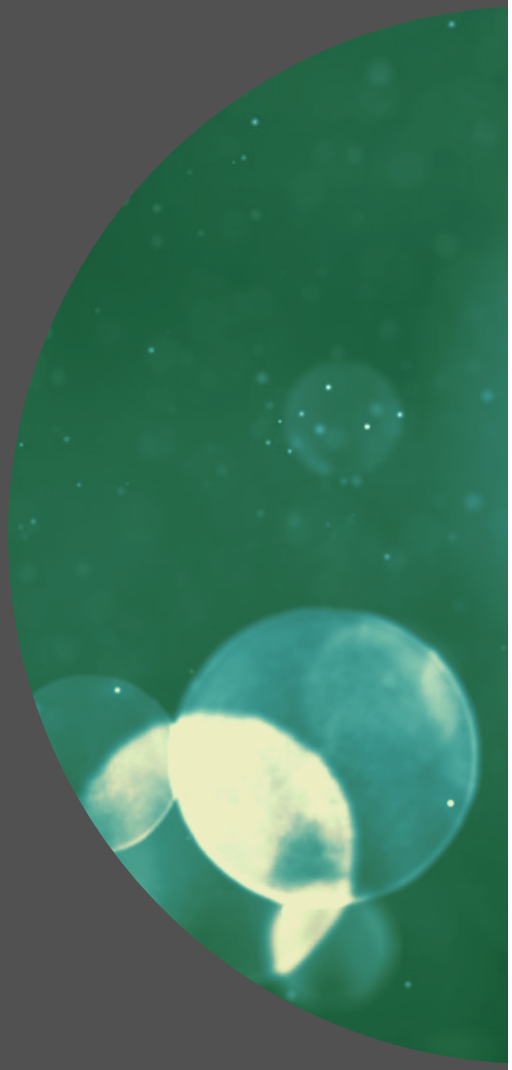
PROGNOZY CYBERBEZPIECZEŃSTWA NA 2018 ROK

NET COMPLEX
Bezpieczeństwo IT



SPIS TREŚCI

WSTĘP

Cyberbezpieczeństwo przykuwa coraz większą uwagę coraz szerszego grona użytkowników. Dzieje się tak z dwóch powodów: spektakularne, perfidne i często udane ataki hakerów są coraz częściej nagłaśniane przed media, ukazując pejzaż rozbudzających wyobraźnię zniszczeń, jakich dokonały w przedsiębiorstwach. Zagrożenie atakiem hakerskim przestało dotyczyć korporacji i rozbudowanych przedsiębiorstw, przemysł ransomware'owy spędza dzisiaj sen z powiek również małym i średnim firmom. Druga kwestia to czekające nas zaostrzenie przepisów w obrębie Unii Europejskiej, z jednej strony wymagające solidniejszej ochrony danych, podnosząc poprzeczkę cyberprzestępcom, z drugiej stawiając, często mało konkretne, wymagania przedsiębiorcom, którzy teraz będą musieli poważnie przysiąść nad kwestią bezpieczeństwa danych przechowywanych i przetwarzanych w ich firmach.

Bezpieczeństwo IT stało się kwestią ważną dla firm każdej wielkości. Przez jakie ataki przebrnęliśmy w 2017 roku? Jakim zagrożeniom stawiliśmy czoła, a jakie mogą czaić się przed polskim i europejskim użytkownikiem sieci, informatykiem, administratorem, kierownikiem IT w 2018 roku? Przygotowaliśmy dla Was kompilację raportów i prognoz, kompas wspomagający orientację na mapie cyberbezpieczeństwa.

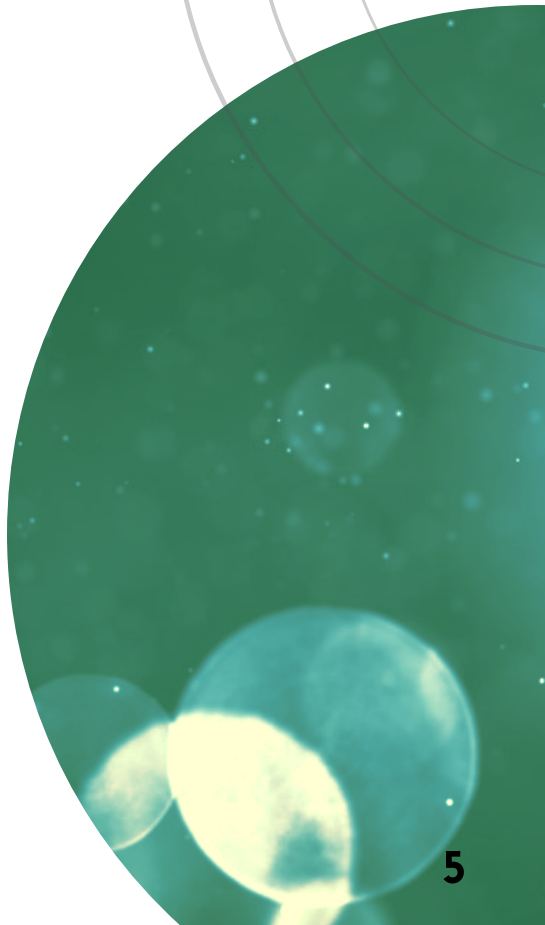
PODSUMOWANIE CYBERZAGROŻEŃ Z 2017 ROKU

Nie dajmy się zastraszyć, atakujący nie może złamać zabezpieczeń, a nawet wykonywać wyrafinowanych ataków bez dostrzeżenia słabych punktów w systemie. Zwielokrotnione ataki złośliwego oprogramowania, ataki z wykorzystaniem poczty e-mail, zhakowane urządzenia i zakłócenia w działaniu - wszystkie te elementy wymagają luki w zabezpieczeniach sieci, zarówno w postaci technologii, jak i ludzi. Trzeba po prostu znaleźć słabe ogniwa i zmienić je w filary ochrony.

Jeśli chodzi o globalny krajobraz cybernetyczny, ten rok zaczął się tam, gdzie zakończył poprzedni. W 2016 r. co miesiąc pojawiały się nowe, wyrafinowane, szkodliwe programy, ujawniające nowe możliwości, metody dystrybucji oraz pomysłowe usługi ataków, oferowane do sprzedaży za pośrednictwem wielu platform, takich jak niesławny program Cerber-ransomware-as-service czy zestaw Angler Exploit Kit. Rok 2017 rzuca światło na nowy trend - proste, ale bardzo skuteczne rodziny malware'u powodują szybkie zniszczenia na całym świecie. Próbki są dystrybuowane przez nieznanych graczy zagrożeń, ale posługują się zaawansowanymi narzędziami ataku i technikami opracowanymi stosownie dla konkretnego kraju.

Ponadto masowe operacje kradzieży, takie jak niesławny wyciek narzędzi od Shadow Brokers, ponoć opracowanych przez hackerów amerykańskiej Agencji Bezpieczeństwa Narodowego (NSA), doprowadziły do tego, że niektóre z najbardziej wyrafinowanych złośliwych programów na świecie trafiły w ręce niewykwalifikowanych napastników. Akcja cieszyła się tak dużym zainteresowaniem, że w czerwcu została udostepniona możliwość zapisania się do płatnej, comiesięcznej subskrybcji usługi „TheShadowBrokers Data Dump of the Month".

Po raz pierwszy byliśmy świadkami zjawiska takiego jak ransomware typu „WannaCry", wpływającego na infrastrukturę publiczną, a także placówki medyczne na całym świecie. Ataki WannaCry czy NotPetya wykorzystywały znane warianty szkodliwego oprogramowania, które mogły zostać zablokowane, gdyby wdrożono odpowiednie zabezpieczenia. Trzeba zauważyć, że cyberprzestępcy uciekają się do wyrafinowanych metod perswazji i używania przekonujących danych, „przekonujących" ofiary do płacenia okupu. Z ransomware-as-a-service (RaaS) wciąż oferowanym na podziemnych forach, wraz z bitcoinem jako bezpieczną metodą zbierania okupu, cyberprzestępcy są tym bardziej przywiązani do tego rentownego modelu biznesowego.



NAJWAŻNIEJSZE ATAKI HAKERSKIE W 2017 ROKU

MARZEC: ukazały się tysiące dokumentów opisujących wysiłki CIA i metodologie włamywania się na iPhone'y, urządzenia z Androidem i inteligentne TV. W pierwszej połowie 2017 roku byliśmy również świadkami ciągłego wzrostu rozpowszechniania i technicznych możliwości botnetów mobilnych typu adware - HummingWhale, Judy - automatycznie wyświetlających lub pobierających materiały reklamowe na zainfekowanej maszynie i, w nowym wydaniu, wykonujących dowolny kod na komputerze ofiary.

KWIECIEŃ: Grupa przestępcza Shadow Brokers wydała repozytorium zawierające exploity NSA i narzędzia hakerskie, uważane za najbardziej szkodliwe wersje, ze względu na liczbę udostępnionych exploitów, a także zaawansowanie i różnorodność exploitów. Paczka zawierająca prawie 300 megabajtów materiału, zawierała narzędzia przeznaczone dla większości wersji systemu operacyjnego Windows, a także kod do włamywania się do EastNets, największego dostawcy usług SWIFT na Bliskim Wschodzie.

MAJ: oprogramowanie WannaCry było słabo napisane, nie było zapakowane, nie miało zaciemnionego kodu i zawierało swoisty "Kill Switch". A jednak ten złośliwy program posiadał nadzwyczajne możliwości ruchu bocznego, oparte w dużej mierze na wycieku z Shadow Brokers, a dokładniej na Eternal Blue. Ujawniony kod posłużył do uaktualnienia prostego oprogramowania ransomware do jednego z najbardziej wpływowych globalnych narzędzi ataku zaobserwowanych w ostatnich latach, wpływających na dużą część obiektów publicznych i cywilnych.

CZERWIEC: Te same zdolności NSA, które były widoczne w ataku WannaCry, zostały ponownie użyte w NotPetya - szerokim ataku skoncentrowanym na ukraińskich organizacjach, który zajęły całe sieci. Incydent ten pokazał, że podczas o ile cyberprzestępcy uczą się dzięki każdej udanej fali ataku, organizacje i osoby fizyczne nadal ignorują te lekcje i odmawiają wdrożenia łatwo dostępnych i skutecznych środków bezpieczeństwa.

LIPIEC: Oprogramowanie adware ewoluuje, pojawia się kilka nowych metod wykorzystywania plików Microsoft Office, które nie wymagają już od ofiary otwarcia drzwi dla atakujących, poprzez samo włączenie, makr.

SIERPIEŃ: Wzrost liczby ataków DDoS na środowisko Linux - w dużej mierze skierowanych na urządzenia IoT oparte na systemie Linux. W drugim kwartale zauważalny wzrost oprogramowania sieciowego wykorzystującego systemy linuksowe. Odnotowanie wielu ataków typu DDoS, które opierały się na ogromnej liczbie niezabezpieczonych urządzeń, takich jak kamery internetowe, cyfrowe rejestratory wideo i inteligentne żarówki. Wiele ataków atakujących systemy oparte na systemie Linux, podobne do botnetu Mirai IoT, za pomocą którego w 2016 roku dokonano największego ataku hakerskiego przy użyciu DDoS w historii.

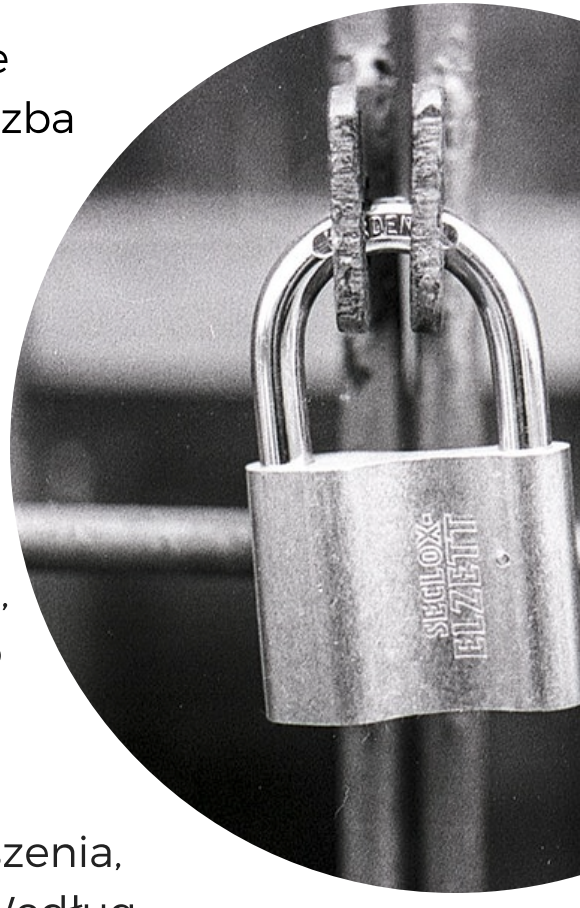
PAŹDZIERNIK: Google podaje, że manipulacje wynikiem wyborów w USA mogły mieć o wiele szerszy zasięg, niż do tej pory sądzono. W rosyjskiej kampanii dezinformacyjnej zostały wykorzystane głównie social media, Facebook i Twitter, a propagandowe filmiki lądowały na Youtube i na platformie Google.

LISTOPAD: Wysyp złośliwych aplikacji dedykowanych urządzeniom mobilnym dostępnych w sklepie Google Play. Fałszywe aplikacje nakłaniają użytkownika do przyznania jej specjalnych uprawnień, a następnie pobierają i uruchamiają na smartfonie swojej ofiary np.: wirusy szpiegujące czy fałszywe aplikacje bankowości mobilnej. Wśród nich znalazło się między innymi kilka popularnych rozwiązań do czyszczenia pamięci telefonu: Clear Android, Cleaner for Android, ale także World News, WORLD NEWS, World News PRO, MEX Tools.

GRUDZIEŃ: Spam przeżywa swój renesans! Skrzynki pocztowe zalewa fala spamu wykorzystująca spoofing czyli podszywanie się pod istniejącą firmę. Takie wiadomości e-mail zawierają w załącznikach ransomware i inne szkodniki: trojany bankowe czy keyloggery. Pozornie oferują sprzedaż autentycznych produktów, jednak w rzeczywistości ich celem jest gromadzenie danych kart kredytowych i danych osobowych. W 2017 roku spamerzy podszywali się m.in. pod: Apple, Amazon, Microsoft, przedsiębiorstwa z branży randek internetowych, a przed świętami, koniecznie: firmy kurierskie. W Polsce hakerzy podszyli się w grudniu pod firmę Polkurier.

KONKRETNE NARUSZENIA BEZPIECZEŃSTWA W EUROPIE I NA BLISKIM WSCHODZIE W 2017 ROKU

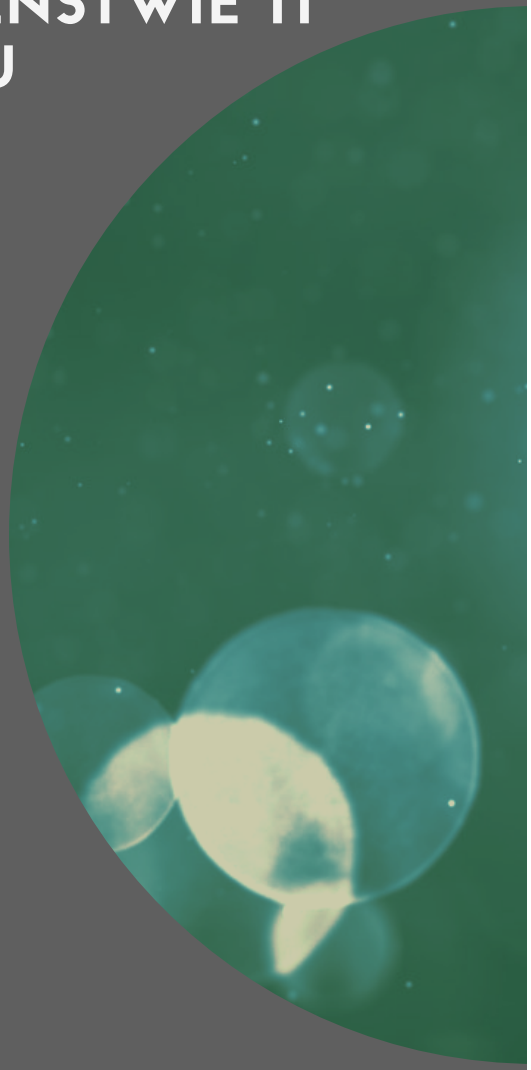
7 stycznia 2017 r.: E-Sports Entertainment Association League, popularna społeczność gier wideo należąca do niemieckiej firmy Tursport Entertainment GmbH z e-sportu, doznała naruszenia, ujawniając dane serwerów gier i dane osobowe użytkowników. Według naukowców liczba użytkowników dotkniętych naruszeniem może osiągnąć 1,5 miliona



12 stycznia 2017 r.: Cellebrite, izraelska firma znana z opracowywania mobilnych narzędzi kryminalistycznych i hakerskich, doznała poważnego naruszenia, co doprowadziło do kradzieży 900 GB danych klientów. Zgodnie z zapowiedziami, naruszony serwer sieciowy zawierał podstawowe informacje o klientach zarejestrowanych dla alertów i powiadomień o produktach Cellebrite, a także zawierał hasła klientów, którzy nie przeszli jeszcze migracji do nowego systemu zarządzania licencjami użytkownika końcowego Cellebrite.

9 kwietnia 2017 r.: Wonga, brytyjska firma pożyczkowa, doznała naruszenia, które dotyczyło 270 000 klientów, w większości w Wielkiej Brytanii. Według Wonga wyciek danych może obejmować adresy e-mail, adresy domowe, numery telefonów, częściowe numery kart kredytowych i numery kont bankowych.

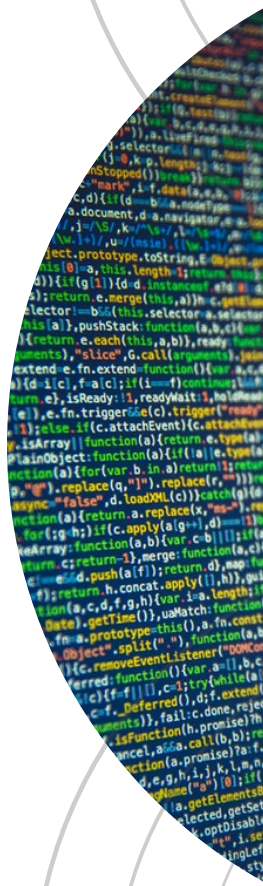
PRZEWIDYWANE TRENDY W BEZPIECZEŃSTWIE IT W 2018 ROKU



Aby przedstawić przewidywane trendy w bezpieczeństwie IT, zarówno w obrębie pojawiających się zagrożeń, jak i strategii odwetowej, która może być obrana w 2018 roku przez specjalistów bezpieczeństwa, skompilowaliśmy prognozy płynące z najważniejszych ośrodków badawczych: WatchGuard Threat Lab, Trend Micro TrendLabs, Check Point Research, SophosLabs oraz analiz ekspertów Lastline, ESET i Kaspersky.

RANSOMWARE NADAL ULUBIONĄ ZABAWKĄ CYBERPRZESTĘPCÓW

Eksperci są zgodni: ransomware nie popuści. Sukcesy WannaCry i Petya oraz rozprzestrzenianie się spamu Locky'ego i FakeGlobe nie pozostawia złudzeń, można spodziewać się podobnych rund w 2018 r. Zapewne poszerzy się również rynek ransomware-as-a-service (RaaS) z ransomware oferowanym na podziemnych forach, wraz z bitcoinem jako bezpieczną metodą zbierania okupu. Jesteśmy pewni, że cyberprzestępcy są przywiązani do tego modelu biznesowego i z niego nie zrezygnują.



Obecny sukces kampanii ransomware - zwłaszcza elementów wymuszających okup - spowoduje, że cyberprzestępcy będą poszukiwać jeszcze większych zysków od grup docelowych. Atakujący będą nadal polegać na masowych kampaniach phishingowych, gdzie odpowiednia wiadomość e-mail z ładunkiem oprogramowania ransomware, zapewni intratny odsetek użytkowników, którzy „klikną". Hakerzy będą również dążyć do większego zysku, celując w pojedynczą organizację, być może w środowiska Industrial Internet of Things (IIoT), gdzie zaszyfrowanie jej przez ransomware zakłóci działanie i wpłynie na zatrzymanie linii produkcyjnej. Widzieliśmy już to w działaniu WannaCry i Petya.

RODO spowoduje wzrost liczby prób naruszenia i żądań okupu. Cyberprzestępcy mogliby pozyskiwać od firm dane, które w świetle nowego prawa powinny być skrzętnie chronione i prosić o zapłacenie okupu, co w tym momencie opłacałoby się bardziej niż zapłacenie kary za wyciek, w wysokości do 4 procent rocznego obrotu firmy (RODO). Ponadto spodziewamy się, że GDPR (RODO) będzie wykorzystane w taktyce inżynierii społecznej w taki sam sposób, jak naruszenia praw autorskich i ostrzeżenia policyjne były wykorzystywane w poprzednich kampaniach FAKEAV i ransomware.

Przedsiębiorcy i przedsiębiorstwa mogą być odporni na te próby wymuszeń cyfrowych dzięki zastosowaniu skutecznej bramki internetowej i poczty e-mail jako pierwszej linii obrony. Rozwiązania z uczeniem maszynowym o wysokiej niezawodności, monitorowaniem zachowania i ochroną przed zagrożeniami zapobiegają przedostawaniu się zagrożeń w głąb sieci. Możliwości te są szczególnie korzystne
w przypadku wariantów oprogramowania typu "ransomware", które są postrzegane jako czyste i przepuszczane do użytkowników końcowych.

UBEZPIECZENIA CYBERNETYCZNE, KTÓRE MOGĄ STAĆ SIĘ POPULARNE W KONTEKŚCIE RODO, POSZERZĄ RYNEK RANSOMWARE

W krajach, które już wymagają obowiązkowego ujawnienia naruszenia, ubezpieczenie cybernetyczne pomaga pokryć koszty, a czasem także sprawy sądowe, wynikające z tych naruszeń. Niedawno ubezpieczyciele promowali opcjonalne pakiety ubezpieczeń „w wypadku okupu", które pokrywają koszty oprogramowania ransomware i innych wymuszeń cybernetycznych. W niektórych przypadkach ubezpieczyciele płacą nawet okup, aby pomóc ofierze odzyskać dane.

Prognozuje się, że małe i średnie firmy będą nadal korzystać z cyber-ubezpieczenia, w tym opcjonalnych pakietów „od ryzyka okupu". Ubezpieczenie może pomóc obniżyć koszty incydentów związanych z bezpieczeństwem i pomóc firmom w odzyskaniu potencjału po ataku, w szczególności MŚP, które w przeciwnym razie musiałyby zamknąć działalność. To jednak nie znaczy, że ubezpieczenie zastąpi stosowanie rozwiązań bezpieczeństwa i trzymanie się odpowiednich praktyk - powinno je jedynie uzupełniać. Przewidujemy, że firmy ubezpieczeniowe będą wdrażać bardziej rygorystyczne wytyczne, które wymagają od firm posiadania silnych mechanizmów kontroli bezpieczeństwa jako warunku do wstępnego ubezpieczenia. W połączeniu z innymi warstwami bezpieczeństwa, ubezpieczenie internetowe jest doskonałym dodatkiem do strategii bezpieczeństwa cybernetycznego.

Istnieje jednak ryzyko, że niektóre rodzaje ubezpieczeń będą wręcz zachęcać do ataku ransomware. Ubezpieczyciele czasami płacą okup, aby odzyskać dane swoich klientów. Rozumiemy decyzję biznesową, koszt okupu może wydawać się dużo mniejszy niż koszt odzyskiwania dla ofiar, które nie mają kopii zapasowych. Jednak ubezpieczyciele nie mają długoterminowych danych dotyczących incydentów cybernetycznych i oprogramowania ransomware. Czy raz zapłacony okup zachęca do kolejnych ataków? Czy płacenie okupu promuje przestępczy model biznesowy? Czy płacenie okupu powoduje wzrost liczby incydentów, z którymi ubezpieczyciele muszą sobie radzić lub podniesienie kwoty okupu? Trudno powiedzieć bez większej ilości danych.

Większość badań wykazuje, że przynajmniej jedna trzecia ofiar ransomware - płaci. To spowodowało, że ceny okupu wzrosły, co spowodowało mniej ofiar płatniczych (jak pokazała WannaCry). Aby zwiększyć nielegalne zyski, przestępcy ransomware będą atakować organizacje, o których wiedzą, że są bardziej skłonne zapłacić. Ponieważ ubezpieczyciele często płacą, jeśli sytuacja tego wymaga, twórcy inteligentnych ransomware będą kraść dane klientów ubezpieczycieli, aby znaleźć organizacje, które mają ubezpieczenie od wymuszeń, a następnie kierować je bezpośrednio na oprogramowanie ransomware.

BOTNETY IoT ZMUSZĄ RZĄDY DO WPROWADZENIA REGULACJI I TRZYMANIE SIĘ ICH PRZEZ PRODUCENTÓW URZĄDZEŃ

Hakerzy już zaczęli ulepszać kod źródłowy Mirai, co oznacza większe i silniejsze botnety w 2018 roku. Użytkowanie rzeczy korzystających z internetu wciąż rośnie, co roku dodając miliardy nowych punktów końcowych sieci. Ponieważ ataków na takie urządzenia będzie coraz więcej, szkody, które powodują, będą rosnąć, dopóki branża wytwarzania Internetu Rzeczy nie zostanie zmotywowana lub zmuszona do zwiększenia bezpieczeństwa swoich produktów.

Bądź gotowy na poważny atak botnetowy IoT w 2018 r., który ostatecznie doprowadzi rządy do rozwiązania kwestii bezpieczeństwa Internetu rzeczy. Przepisy te najprawdopodobniej będą odzwierciedlać podobne regulacje dotyczące odpowiedzialności w innych branżach, w których producent jest co najmniej częściowo odpowiedzialny za wady swoich produktów.

Trend Micro w swoim raporcie dzieli się wizją setek lub tysięcy przejętych przez hakerów dronów, wchodzących samotnie w przestrzeń powietrzną USA. Podobnie może stać się z urządzeniami domowymi, np. głośnikami bezprzewodowymi czy asystentem głosowym, które mogą umożliwić hakerom określenie lokalizacji domu i włamanie. Spodziewamy się również, że przypadki biohackingu za pośrednictwem urządzeń do noszenia typu ubrania oraz akcesoria zawierające w sobie komputer i urządzeń medycznych zmaterializują się w 2018 r. Biometryczne urządzenia śledzące aktywność, takie jak monitory mierzące tętno czy taśmy fitness, mogą być przechwytywane w celu zbierania informacji o użytkownikach. Stwierdzono już, że podtrzymujące życie rozruszniki serca mają luki w zabezpieczeniach, które można wykorzystać do potencjalnie śmiertelnych ataków. Urządzenia tego typu są obecnie narażone na atak, najwyższa pora, aby producenci zaczęli przeprowadzać regularne oceny ryzyka oraz audyty bezpieczeństwa. Użytkownicy również są odpowiedzialni. Powinni pamiętać o konfigurowaniu swoich urządzeń pod kątem bezpieczeństwa, co opiera się na prostych zabiegach: zmianie domyślnych haseł i regularnym instalowaniu aktualizacji firmware.

ATAKI UKIERUNKOWANE NA LINUXA W 2018 ROKU PODWOJĄ SIĘ

Wzrost liczby ataków na Linuxa - w dużej mierze skierowanych na urządzenia IoT oparte na systemie Linux - był powtarzającym się trendem w 2017 roku. Malware Linuksa stanowiły 36 procent najgroźniejszego złośliwego oprogramowania w Q1 2017. W drugim kwartale zauważono wzrost oprogramowania sieciowego wykorzystującego systemy linuksowe. Na koniec, badania przeprowadzone przez honeynet laboratorium Threat Lab wykryły wiele ataków telnetowych i SSH atakujących systemy oparte na systemie Linux, podobne do botnetu Mirai IoT.

Do tej pory Linux kojarzył się z bezpieczeństwem. Zmiana już się rozpoczęła i najprawdopodobniej zobaczymy dramatyczny wzrost liczby ataków atakujących systemy linuksowe w 2018 roku. Laboratoroum WatchGuard potwierdza, że zwiększone zainteresowanie przestępców atakami na Linuxa wynika z ich chęci celowania w urządzenia IoT.

Podczas gdy urządzenia IoT są technicznie zróżnicowane, duży procent z nich to tanie urządzenia, z wbudowanymi systemami Linux i bardzo niepewnymi ustawieniami domyślnymi. Oczekujemy, że osoby atakujące będą nadal korzystać z tych niezabezpieczonych urządzeń w celu zasilania swoich botnetów. Na podstawie różnych badań nad zagrożeniami i głównych trendów w przestrzeni Internetu Rzeczy spodziewa się, że liczba ataków specyficznych dla systemu Linux podwoi się w 2018 roku.

WZROŚNIE RYZYKO CYFROWEJ DEZINFORMACJI I PROPAGANDY

Konferencja hakerska DefCon 2017 w Las Vegas pojawiła się na pierwszych stronach gazet, gdy jej uczestnicy znaleźli i wykorzystali wiele nowych luk w amerykańskich automatach do głosowania. Skłoniło to popularne serwisy informacyjne do kwestionowania integralności elektronicznych urządzeń do głosowania i zasugerowało istnienie armii bezpośrednio zmieniającej wyniki głosowania podczas przyszłych wyborów.

Dezinformacja i propaganda ze strony cyberprzestępców i podmiotów sponsorowanych przez państwo prawdopodobnie odegra większą rolę w kolejnych wyborach i referendach, niż sama zhakowana infrastruktura głosowania. Fałszywy trójkąt informacyjny składa się z: motywacji, na której opiera się propaganda, sieci społecznościowych, które służą jako platforma dla wiadomości oraz narzędzi i usług, które są wykorzystywane do dostarczania wiadomości. Widzieliśmy na to dowody w wyborach w 2016 roku, z fałszywymi kontami na Facebooku i botami na Twitterze, które rozniecały kontrowersje. Prawdopodobnie liczba organizacji krajowych i zagranicznych uzyska swoje fałszywe bliźniacze konta w mediach społecznościowych w 2018 roku.

Dezinformacja może stawiać w złym świetle całe przedsiębiorstwa, wpływając na ich wydajność i reputację. Naukowcy szukają obecnie narzędzi do manipulacji dźwiękiem i obrazem wideo, które pozwalają realistycznie wyglądającemu materiałowi filmowemu jeszcze bardziej zatrzeć granicę między autentycznym a fałszywym. Manipulowane kampanie polityczne będą kontynuowały taktykę „skażania" i celowo zmieniały opinię publiczną. Jest prawdopodobne, że zbliżające się wybory powszechne w Szwecji nie będą wolne od manipulacji.

Odróżnianie fałszywych wiadomości od prawdziwych, będzie trudne, ponieważ propagandziści opierają się na starych, sprawdzonych już technikach, tym bardziej, ze nie istnieje rozwiązanie do wykrywania lub blokowania manipulowanych treści. Co prawda serwisy społecznościowe, w szczególności Google i Facebook, zobowiązały się tłumić fałszywe historie rozpowszechniające się w kanałach i grupach - w zarodku, ale jak dotąd nie mają się tutaj czym pochwalić. Dopóki użytkownicy nie nauczą się odróżniać fałszywych fałszywych wiadomości, takie treści będą przenikać Internet i będą ze smakiem konsumowane.

OBNIŻENIE ZAUFANIA DO KRYPTO-WALUTY I SPADEK JEJ WARTOŚCI

Podczas gdy Bitcoin był pierwszą krypto-walutą i pozostaje najpopularniejszą, istnieje wiele różnych monet kryptograficznych: Ethereum, Litecoin i Monero. Każda nowa kryptowaluta wprowadza swoje innowacje do odpowiednich bloków kodu. Blokada Ethereum działa na przykład jako w pełni zdecentralizowany komputer zdolny do uruchamiania aplikacji a dodatkowe funkcje blockchain wprowadzają konkretne względy bezpieczeństwa. Tymczasem Ethereum już w 2016 roku odnotowało prawie 50-procentowy spadek wartości, gdy hakerzy wykorzystali lukę w popularnej aplikacji blockchain, aby ukraść ponad 50 milionów dolarów w krypto-walucie Ethereum. Od tego czasu publiczne przeglądy kodów stały się główną częścią rozwoju blockchain.

Ponieważ wartość krypto-walut bardzo szybko rośnie, stają się one znacznie atrakcyjniejszym celem cyberprzestępców, którzy chcą zarobić miliony. Przewiduje się, że hakerzy znajdą podatność na tyle wrażliwą, aby całkowicie zniszczyć popularną krypto-walutę, niszcząc zaufanie społeczeństwa do jej bezpieczeństwa.

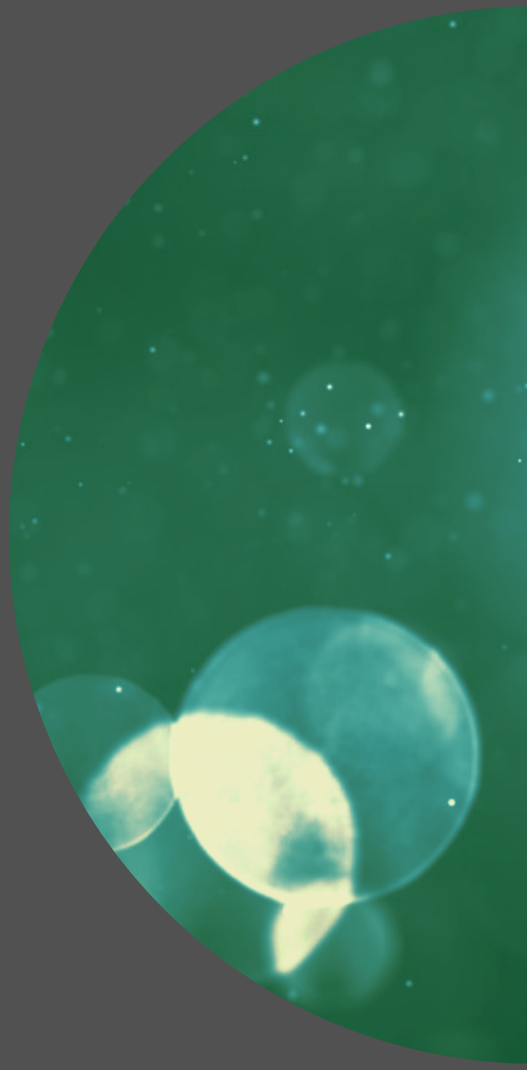
ROK 2018 JEST ROKIEM PROSTEGO I NIEDROGIEGO UWIERZYTELNIANIA WIELOSKŁADNIKOWEGO (MFA) DLA MAŁYCH I ŚREDNICH FIRM

Uwierzytelnianie jest obecnie najsłabszym ogniwem w bezpieczeństwie. Zgodnie z raportem Verizon Data Breach z 2017 roku, 81 procent naruszeń związanych z włamaniami wykorzystało skradzione i/lub słabe dane uwierzytelniające. Jeśli osoba atakująca uzyska dostęp do danych uwierzytelniających jednego z Twoich pracowników, będzie mogła szybko i sprawnie przechodzić przez kontrolę zabezpieczeń jako "uprawniony" użytkownik, nawet jeśli masz najlepsze zabezpieczenia na świecie.

Ciągłe naruszenia i kradzieże baz danych z hasłami wykazały, że właściwe metody sprawdzania haseł są zbyt trudne dla przeciętnego użytkownika. W rezultacie przemysł zmienił się w kierunku innych czynników uwierzytelniających, takich jak biometria. Chociaż te metody uwierzytelniające rozwiązują problem funkcjonalności, mają własne słabe punkty bezpieczeństwa. Większość ekspertów ds.Bezpieczeństwa zgadza się, że MFA - która wymaga co najmniej dwóch czynników do uwierzytelnienia użytkowników - jest najbezpieczniejszą opcją uwierzytelniania.

Niestety, skuteczne rozwiązania MFA znajdują się w większości poza zasięgiem przeciętnego małego i średniego biznesu. Choć wieloczynnikowa technologia dla przedsiębiorstw jest dość dojrzała, często wymaga złożonych rozwiązań lokalnych i drogich tokenów sprzętowych, na które większość małych firm nie może sobie pozwolić lub sobie z nimi poradzić. Dlatego też rozwój SaaS i smartfonów wprowadził nowe, wieloczynnikowe rozwiązania dla małych firm, niedrogie i łatwe w użyciu. W przyszłym roku wielu małych i średnich firm przyjmie te nowe rozwiązania MFA, aby zabezpieczyć bardziej uprzywilejowane konta i użytkowników. Rok 2018 będzie rokiem MSZ dla małych i średnich firm.

W JAKIE DZIAŁANIA OCHRONNE INWESTOWAĆ W 2018 ROKU?



Umiejętności i zasoby - to dwa elementy składające się na arsenał atakującego. Atakujący nie może jednak złamać zabezpieczeń, a nawet wykonywać wyrafinowanych ataków bez dostrzegania słabych punktów w systemie. Biorąc pod uwagę szeroką gamę czyhających zagrożeń - od luk w zabezpieczeniach i oprogramowania typu ransomware, po spam i ataki ukierunkowane - tym, co mogą zrobić przedsiębiorstwa i użytkownicy jest zlokalizowanie słabych punktów bezpieczeństwa i zminimalizowanie ryzyka kompromitacji na wszystkich warstwach.

Najważniejsze: lepsza widoczność i wielowarstwowa ochrona

Firmy powinny stosować rozwiązania bezpieczeństwa, które zapewniają widoczność we wszystkich sieciach, wykrywanie w czasie rzeczywistym oraz zabezpieczenie w wypadku wystąpienia luki czy ataku. Oczekiwane technologie bezpieczeństwa powinny obejmować:

Skanowanie w czasie rzeczywistym. Aktywne i automatyczne skanowanie pozwala na wysoce efektywne wykrywanie złośliwego oprogramowania i poprawę wydajności maszyny.

Reputacja stron i plików. Wykrywanie i zapobieganie złośliwym programom za pomocą usługi Web Reputation, technik antyspamowych i kontroli aplikacji chroni użytkowników przed atakami i exploitami typu ransomware.

Analiza behawioralna. Zaawansowane złośliwe oprogramowanie i techniki, które unikają tradycyjnych mechanizmów obronnych są aktywnie wykrywane i blokowane.

Uczenie maszynowe. Zachowania użytkowników wzbogacone o zebrane dane dotyczące zagrożeń umożliwiają szybkie wykrywanie i szczelną ochronę przed znanymi i nieznanymi zagrożeniami.

Ochrona punktu końcowego. Zabezpieczenie, które wykorzystuje funkcje piaskownicy, wykrywa naruszenia i podejrzane działania, zapobiega atakom oraz ruchowi bocznemu w sieci.

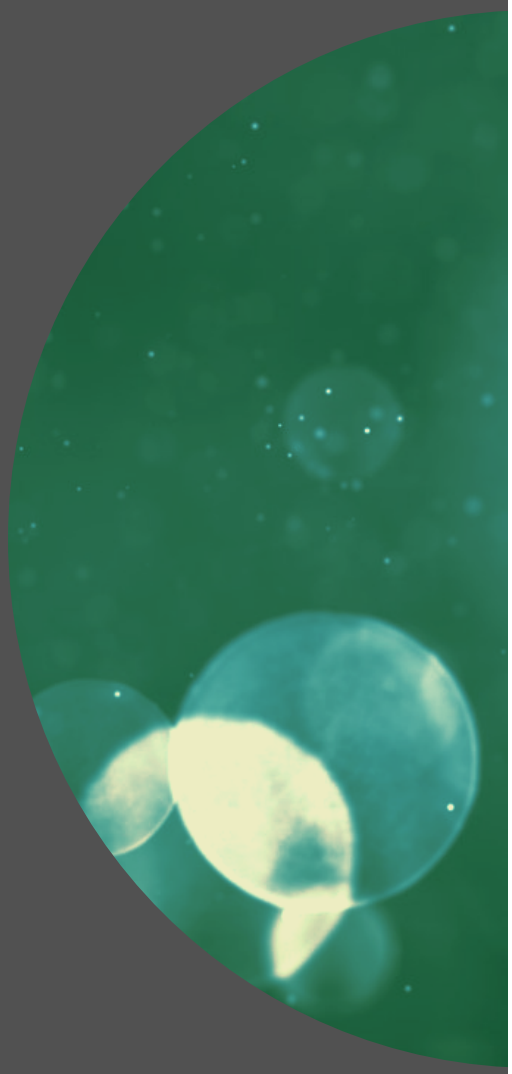
Najlepsze praktyki dla użytkowników końcowych

Bez względu na urządzenie, aplikację lub sieć, użytkownicy mogą wypełnić luki bezpieczeństwa za pomocą odpowiednich metod:

- Zmień domyślne hasła. Używaj unikatowych i złożonych haseł do inteligentnych urządzeń, szczególnie dla routerów, aby znacząco ograniczyć możliwość włamań hakerów do tych urządzeń.
- Skonfiguruj urządzenia pod kątem bezpieczeństwa. Zmodyfikuj domyślne ustawienia urządzeń, aby zachować prywatność podczas sprawdzania i zaimplementuj szyfrowanie, aby zapobiec nieautoryzowanemu monitorowaniu i korzystaniu z danych.
- Zastosuj aktualne poprawki. Zaktualizuj firmware do jego najnowszej wersji (lub włącz funkcję automatycznej aktualizacji, jeśli jest dostępna), aby uniknąć w zabezpieczeniach niezałatanych luk.
- Rozpoznawaj zabiegi socjotechniczne. Zawsze pamiętaj o otrzymywanych e-mailach i odwiedzanych witrynach, ponieważ mogą służyć do spamowania, wyłudzania informacji, złośliwego oprogramowania i ukierunkowanych ataków.

Przedsiębiorstwa i użytkownicy mają lepszą pozycję, jeżeli chodzi o ochronę, jeśli istniejące zabezpieczenia są w stanie odpowiedzieć na cały cykl życia danego zagrożenia wieloma warstwami zabezpieczeń. Posiadanie skonsolidowanej ochrony przed zagrożeniami zapewnia maksymalne bezpieczeństwo pod kątem zmieniających się zagrożeń w 2018 i później.

PODSUMOWANIE



Poza nowym prawem rzucającym potężny cień na pole bezpieczeństwa w 2018 roku, nie ma wątpliwości, że zobaczymy cyberprzestępców wykorzystujących więcej urządzeń podłączonych do Internetu, aby robić coraz większe, tragiczne w skutkach spustoszenie. Metoda, która pozwoli konsumentom i firmom być o krok przed zagrożeniami, to utrzymywanie wszechstronnej widoczności swoich sieci, aby codzienne ataki mogły być natychmiast wykrywane i blokowane. Jednak bezpieczeństwo nie jest już tylko problemem informatycznym. Spodziewamy się, że nadchodzący rok zapowiada nowe środowisko, w którym ludzie, procesy i technologie działają wspólnie.

Net Complex Sp. z o.o.

43-300 Bielsko-Biała, ul.
Cieszyńska 79
tel.: 33 472 03 18/ 33 816 04 11
fax.: 33 486 70 02
e-mail: biuro@netcomplex.pl