Cyberbezpieczeństwo w Twojej firmie

Koszt cyberprzestępstw i sposoby ochrony danych

Dostarczone przez

Spis treści

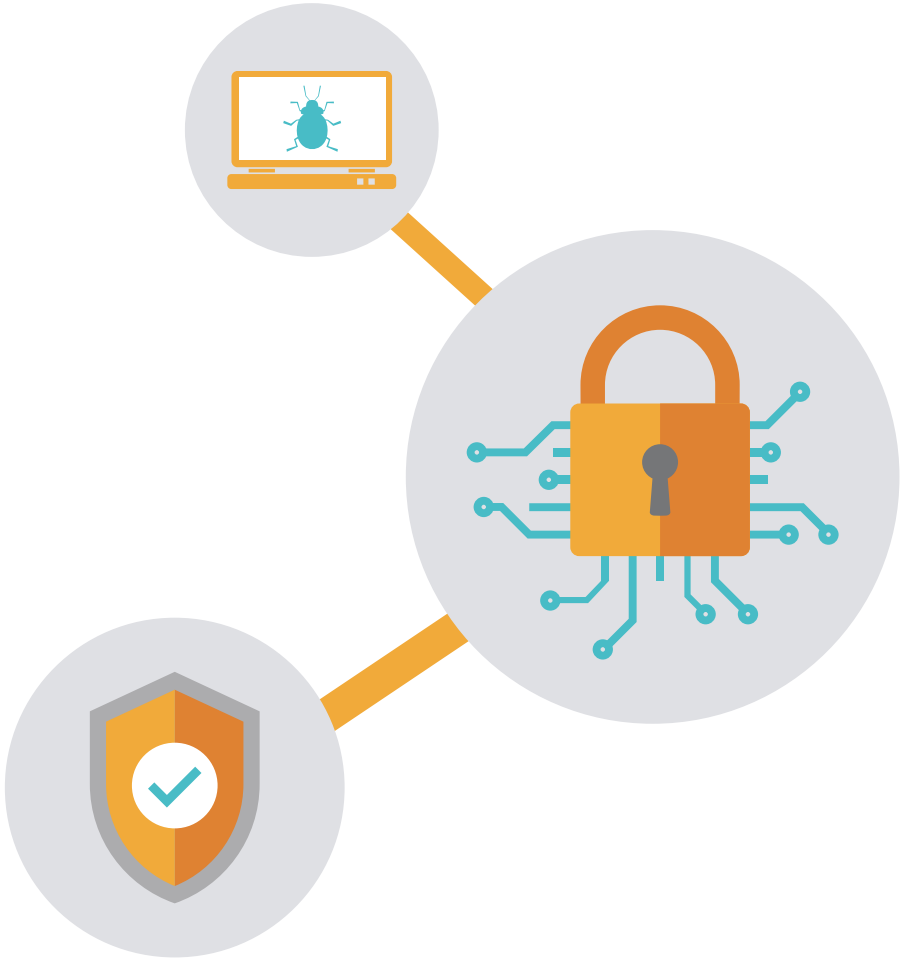
Wprowadzenie

„Wielu menedżerów wyższego szczebla uważa, że cyberprzestępczość to ryzyko, które będzie w przyszłości definiować naszą generację” — Dennis Chesley, Global Risk Consulting Leading, PwC[1]

Cyberprzestępczość nie jest nowym zagrożeniem. Ale ciągle wzrasta. Hakerzy są coraz lepsi. I jest coraz więcej punktów, za pomocą których mogą dostać się do sieci. Internet rzeczy zwielokrotnił liczbę urządzeń końcowych i często są one najłatwiejszym punktem wejścia do sieci. Liczba celów rośnie, podobnie jak czas przestojów.

21 października 2016 roku dostawca DNS z siedzibą w USA, firma Dyn, była obiektem największego w historii rozproszonego ataku polegającego na spowodowaniu odmowy usługi (distributed denial-of-service, DDoS). Niektóre największe serwisy internetowe — w tym Netflix,[2] Amazon i Twitter — przestały działać na kilka godzin.

W styczniu 2017 r. Lloyds Bank doświadczył poważnych problemów związanych z wyłączeniami bankowości online. Klienci nie mogli sprawdzać stanów swoich kont ani dokonywać płatności online. Również dostęp do aplikacji na urządzeniach mobilnych był wyłączony. Lloyds niczego nie potwierdził, ale atak DDoS był najbardziej prawdopodobną przyczyną tej sytuacji.[3]



Źródła: [1] PwC: Wyniki badania globalnego stanu zabezpieczenia informacji, Global State of Information Security Survey 2016 [2] http://thehackernews.com/2016/10/dyn-dns-ddos.html
[3] https://www.theguardian.com/business/2017/jan/23/lloyds-bank-accounts-targeted-cybercrime-attack

Wprowadzenie

Naruszenia tego rodzaju to coś więcej niż zła prasa. To konkretne koszty.

W raporcie 2016 Printer Security Survey Report przygotowanym przez Spiceworks 34% organizacji stwierdziło, że naruszenie powoduje zwiększenie liczby telefonów do stanowisk pomocy/wydłużenie czasu udzielania wsparcia, 29% zgłosiło zmniejszenie wydajności, a 26% — problem z wydłużeniem czasu wyłączenia systemu.[4]

Niemal 60% liderów rynku w zakresie zabezpieczeń w ankiecie dla IBM CSO Assessment stwierdziło, że ataki hakerów są bardziej wyrafinowane i skomplikowane niż sposoby obrony organizacji.[5]

Zaniepokojeni dyrektorzy IT podają cyberbezpieczeństwo jako jedno z 10 największych wyzwań tej dekady, teraz jest to numer 2 w corocznym opracowaniu SIM Trends.[6]

Wielu szkodom można było zapobiec. Na kolejnych stronach omówimy najczęstsze nieporozumienia dotyczące cyberbezpieczeństwa, a także przyjrzymy się dokładniej wpływowi cyberprzestępstw na działalność gospodarczą i pokażemy, jak można lepiej bronić się przed atakami. Na koniec spojrzymy w przyszłość: opowiemy o tym, co nas czeka i i jak się do tego przygotować.

Źródła: [4] HP Printer Security Research 2016, Spiceworks [5] IBM CSO Assessment 2014 [6] SIM IT Trends Survey 2015

Obalone mity dotyczące cyberbezpieczeństwa

Pięć najczęstszych nieporozumień dotyczących cyberbezpieczeństwa,

które mogą narazić firmę na ryzyko ataku

Znane marki są najbardziej narażone na naruszenie danych, ale ryzyko to występuje we wszystkich typach organizacji. Oto pięć mitów o cyberbezpieczeństwie, które sprawiają, że firmy narażają się na ataki hakerskie.

Naruszenie zabezpieczeń

Wycieki danych

Praktyki dotyczące zabezpieczeń

Oprogramowanie antywirusowe

Cyber ataki

1 Firmy potrafią szybko usuwać skutki naruszeń.

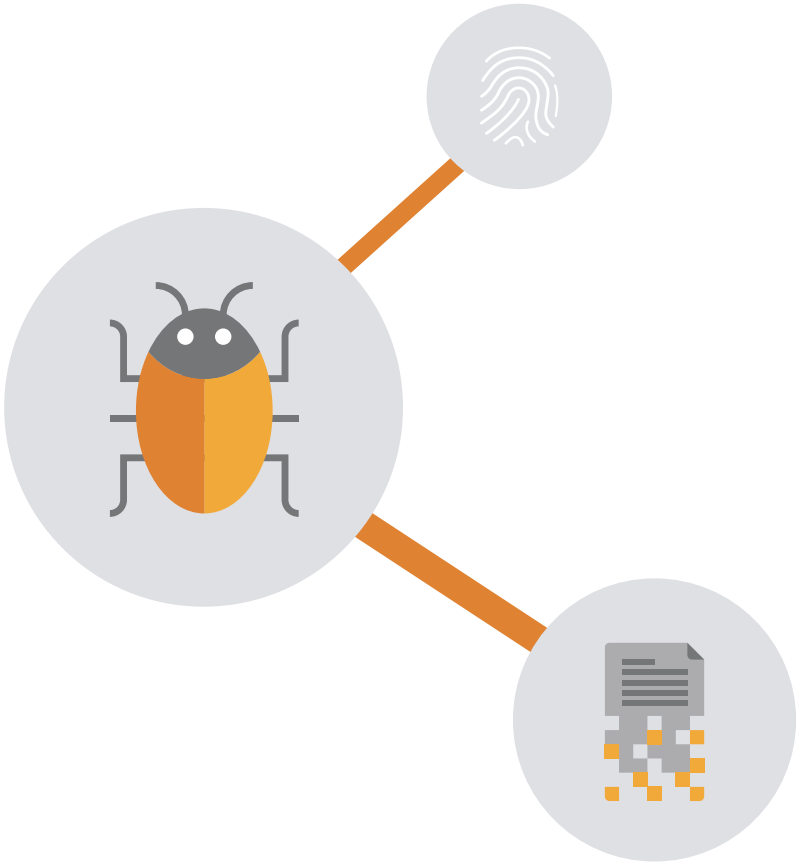
W wielu firmach bardzo trudno zmierzyć koszt naruszeń bezpieczeństwa. Łatwo natomiast zauważyć, że każde naruszenie powoduje spadek cen akcji.

Jednak ceny akcji to tylko część tej historii — pierwsza część. Ceny mogą po kilku tygodniach wrócić do poprzedniego poziomu, ale w dłuższym okresie koszty się kumulują. Nowe programy zabezpieczające, wymiana pracowników, koszty ochrony prawnej.

Wszystkie te czynniki mogą znacznie zaburzyć działanie firm na dłuższy czas po wystąpieniu naruszenia.
Rosną również koszty.
Ostatnie badania przeprowadzone przez Ponemon pokazują, jak średnie roczne koszty naruszeń wzrosły z **7,7 mln USD** w 2015 roku do **9,5 mln USD** w 2016 roku.[7]

Źródła: [7] Ponemon Institute Cost of Cyber Crime Study 2016

2 Wycieki danych występują rzadko, nie trzeba się przed nimi poważnie zabezpieczać



IDC podało[8], że w 2016 roku aż 99% firm doświadczyło naruszenia danych. Dodatkowo liczba firm, w których naruszenie danych miało miejsce 6–10 razy w ciągu roku, wzrosła z 9% w roku 2014 do 18,9% w roku 2016.[9]

Te wartości mogą być zaniżone. Naruszenia często nie są zgłaszane, bo firmy starają się unikać związanej z tym utraty reputacji.

Drugi element mitu wymagający wyjaśnienia to ocena osłabienia, jakie może spowodować naruszenie danych. Być może w firmie miał miejsce tylko jeden wyciek. Jednak nawet pojedynczy incydent może spowodować znaczne problemy.

Źródła: [8] IDC [9] Ponemon Institute Cost of Cyber Crime Study 2016

3 Zleciliśmy specjaliście IT zajęcie się zabezpieczeniami i nie musimy robić nic więcej

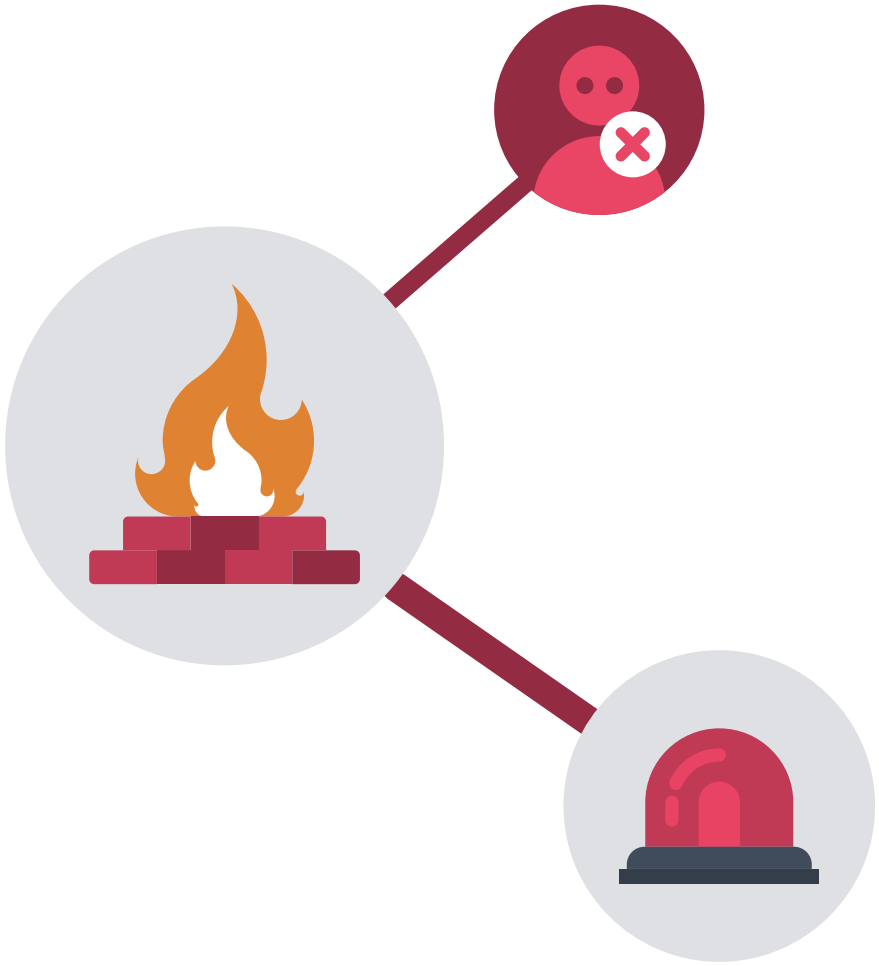
Zlecenie zadania specjaliście IT to dobry pomysł, ale każdy pracownik w firmie powinien zostać przeszkolony w zakresie bezpieczeństwa oraz poznać i stosować sprawdzone praktyki zapewniające cyberbezpieczeństwo.

Pomyśl o koledze, który niczego nie podejrzewając, pobiera złośliwy załącznik do poczty elektronicznej lub odwiedza niebezpieczną witrynę internetową, infekując przy tym sieć firmową oprogramowaniem typu malware, które powoduje spowolnienie komputerów lub wysyła poufne informacje do cyberprzestępców.

Według raportu Cyber Threat Report przygotowanego w 2016 roku przez CyberEdge, organizacje z „niską świadomością bezpieczeństwa wśród pracowników" uważają, że jest to główny problem utrudniający obronę przed zagrożeniami bezpieczeństwa. Są w rankingu wyżej niż organizacje, w których „brak budżetu" lub „brak wykwalifikowanego personelu".[10]

Źródła: [10] Ponemon Institute Cost of Cyber Crime Study 2016

4 W naszych systemach działają zaawansowane programy antywirusowe, jesteśmy dobrze zabezpieczeni



Oprogramowanie antywirusowe skanuje systemy w poszukiwaniu oprogramowania typu malware pobranego z pocztą elektroniczną lub ze stron internetowych. Hakerzy mają sposoby na ominięcie tego zabezpieczenia.

Cyberataki, których nie blokuje oprogramowanie antywirusowe, to między innymi rozproszone ataki odmowy usługi (DDoS) polegające na tym, że stronę internetową spowalnia lub blokuje sztucznie generowany ruch. Inny przykład to ataki internetowe, w których hakerzy umieszczają złośliwy kod w kodzie strony i kradną dane lub zdalnie szpiegują. Hakerzy uzyskują dostęp do danych również za pośrednictwem skradzionych urządzeń.

5 Jeśli intruz dostanie się do wewnątrz, łatwo go usuniemy

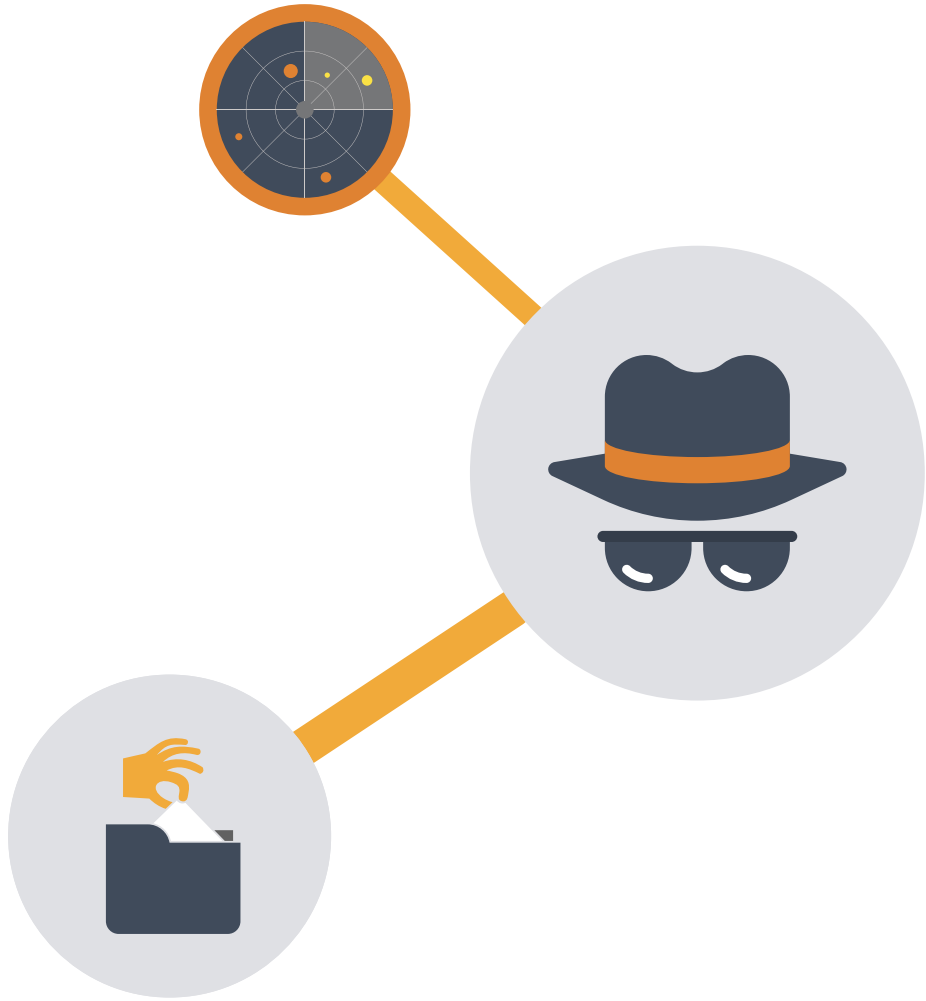
Nie jest łatwo wykryć cyberatak. Oprogramowanie typu malware, które dostanie się do systemu, nie od razu negatywnie wpływa na jego działanie. Najpierw może szpiegować — przekazywać hakerom informacje umożliwiające przygotowanie kolejnych ukierunkowanych ataków i uzyskanie dostępu do całej sieci.

Takie ataki na konkretne systemy są kwalifikowane jako zaawansowane stałe zagrożenia (APT). Cechą charakterystyczną ataków APT jest stałe monitorowanie i uzyskiwanie danych z konkretnej infrastruktury komputerów przez dłuższy czas — zwykle nie są one wykrywane.

Grupa konsultingowa IT Daisy Group szacuje, że połowa firm w Wielkiej Brytanii może zostać zhakowana w ciągu jednej godziny.

WSKAZÓWKA:
Monitorowanie danych wyjściowych pod kątem nadmiarowego ruchu może pomóc zidentyfikować kradzież danych — to może być atak APT.

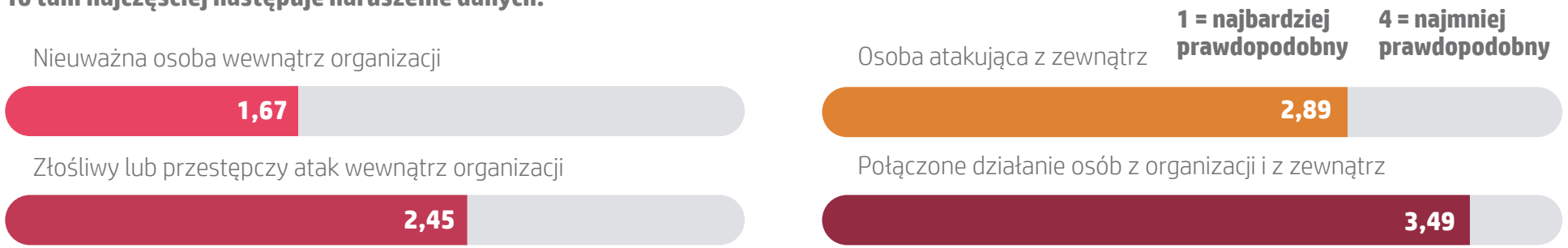
DZIAŁAJ:
Wybierz oprogramowanie zabezpieczające z ochroną danych, takie jak HP SureStart, które po wykryciu ataku oprogramowania typu malware automatycznie przywraca system BIOS komputera i wstrzymuje naruszenie danych.



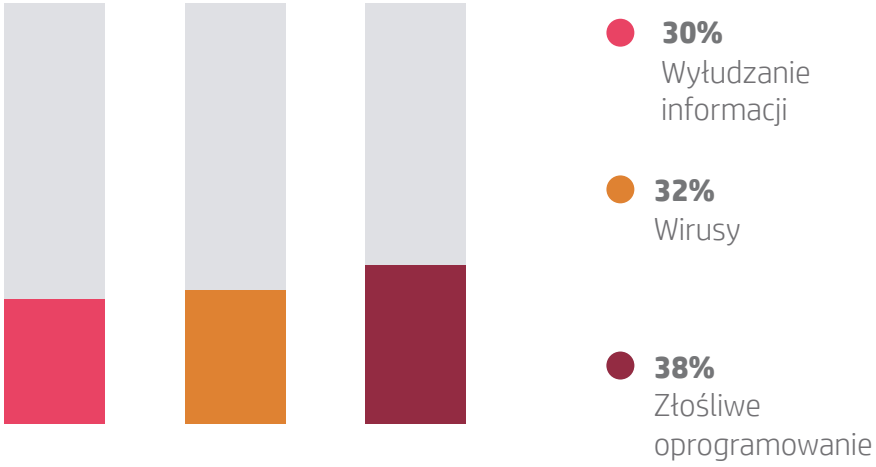
Skąd nadchodzą zagrożenia?

Zabezpieczenie sieci rozpoczyna się od znalezienia najsłabszych punktów

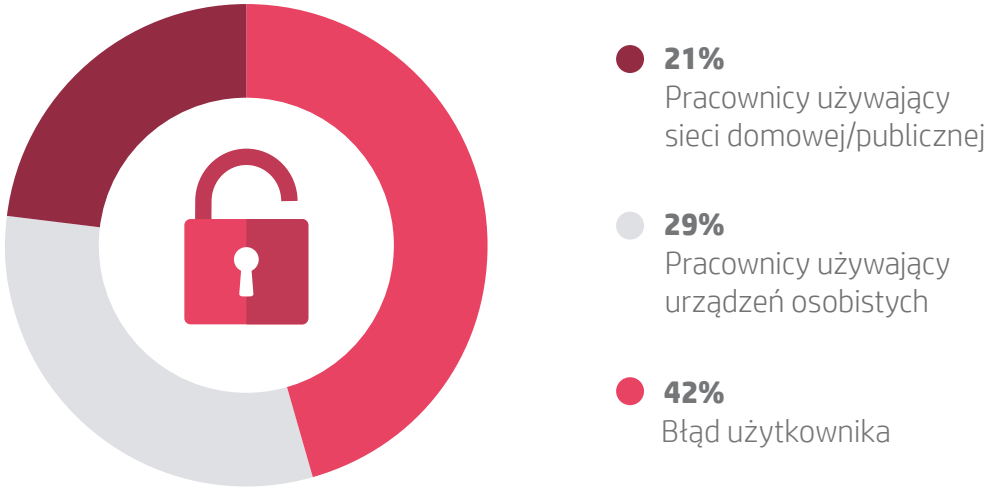
To tam najczęściej następuje naruszenie danych:[11]



Najczęstsze typy zagrożeń zewnętrznych:



Skąd się biorą naruszenia wewnętrzne: [12]



Źródła: [11] http://www.kilpatricktownsend.com/_assets/Kilpatrick%20Townsend%20Report%20Final.pdf [12] Ponemon Institute Cost of Cyber Crime Study 2015

Ile kosztuje usuwanie skutków cyberprzestępstw?

Najkosztowniejsze typy cyberataków:

25%

1 000 000 £

Złośliwy kod i oprogramowanie typu malware

Oprogramowanie, które uszkadza system, tworząc luki w zabezpieczeniach, uszkadzając pliki lub kradnąc dane (mogą to być skrypty, wirusy lub robaki).

24%

960 000 £

Rozproszona odmowa usługi

Ataki „DDoS" polegają na generowaniu ruchu w sieci który powoduje zablokowanie strony i serwerów firmy.

16%

640 000 £

Ataki internetowe

Ataki, których celem są osoby odwiedzające stronę firmy, takie jak zaimplementowany kod, który przekierowuje przeglądarki na strony ze złośliwym kodem.

13%

520 000 £

Skradzione urządzenia

Utracone przez pracowników urządzenia z dostępem do logowania w firmie mogą doprowadzić do kradzieży danych i kradzieży tożsamości.

9%

360 000 £

Wyłudzanie informacji i inżynieria społeczna

Wiadomości e-mail lub wyskakujące okienka z prośbą o wprowadzenie danych logowania.

9%

360 000 £

Szkodliwe działania od wewnątrz

Pracownicy udostępniający poufne informacje.

4%

160 000 £

Boty sieciowe

Sieci zainfekowanych komputerów kontrolowane pod kątem szkodliwych działań, takich jak wysyłanie spamu.

Źródła: [13] Ponemon Institute Cost of Cyber Crime Study 2015

Wpływ cyberprzestępczości na firmy

Rzeczywiste koszty cyberprzestępczości to nie tylko koszty usuwania skutków ataku hakerów

Naruszenia zabezpieczeń są wyjątkowo kosztowne. Omówimy szerzej trzy rodzaje dodatkowych kosztów powodowanych przez ataki.

Zasoby firmy

Oczywiście należy wszystko uporządkować. Wymaga to znacznej liczby pracowników i dużych kosztów. Oznacza to, że trzeba będzie ograniczyć środki na inne działania, które generują przychody.

Grzywny/kary

Firma może zostać ukarana za niespełnienie wymogów prawnych. Gdy w przyszłym roku wejdzie w życie nowa regulacja Unii Europejskiej o ochronie danych osobowych (GDPR), firmy, które się do niej nie dostosują narażają się na grzywnę nawet do 4% ich całkowitych obrotów. Mogą być nawet wystawione na ryzyko procesów sądowych, jeśli wyciek spowoduje naruszenie poufnych danych, które klienci przekazywali firmie.

Utracona reputacja

To może być jeden z najbardziej szkodliwych efektów naruszenia. Klienci, media i społeczeństwo długo pamiętają o naruszeniach zabezpieczeń. Odzyskanie zaufania może trwać bardzo długo.

Analiza nieoczekiwanego ataku hakerskiego

Gdy firma Sony Pictures została zhakowana w 2014 roku, hakerzy po prostu weszli przez frontowe drzwi.[14]

Według jednego z członków grupy hakerskiej Guardians of Peace (GOP), podpisującego się pseudonimem „Lena" — który twierdzi, że ta grupa jest odpowiedzialna za atak — Sony „nigdy nie zapewni fizycznego bezpieczeństwa". Hakerzy uzyskali dostęp do sieci Sony, po prostu wchodząc do budynku i kradnąc dane uwierzytelniające administratora systemu.

Wcześniej stworzyli oprogramowanie typu malware, które kradło prywatne pliki, kod źródłowy i hasła do baz danych Oracle i SQL. Stamtąd ukradli harmonogramy produkcji filmowej, e-maile, dokumenty finansowe i wiele innych, przy czym wiele z nich opublikowali online.

Hakerzy zagrozili opublikowaniem dalszych tajnych i ściśle tajnych danych, jeśli firma nie wycofa z kin filmu „The Interview".

Firma Sony ostatecznie skapitulowała, straciła przychody kasowe i poniosła ogromne szkody wizerunkowe.

Sony Pictures popełniło dwa błędy. Nie zadbało o zablokowanie intruzom fizycznego dostępu do danych firmy oraz nie zainwestowało w wielowarstwowe zabezpieczenia, co mogłoby zapobiec dostępowi do poufnych informacji po początkowym naruszeniu.

Jak napisał po ataku Bruce Schneier, ekspert ds. zabezpieczeń: „W walce z wykwalifikowanym i zmotywowanym finansowo napastnikiem wszystkie sieci są bezbronne". Sztuczka polega na tym, aby znaleźć wrażliwy punkt w sieci. Mogą to być na przykład drzwi frontowe.

DZIAŁAJ:
Aby zminimalizować czas naprawy szkód, przygotuj plan reakcji na naruszenie dla każdego działu, od IT po dział obsługi klienta.

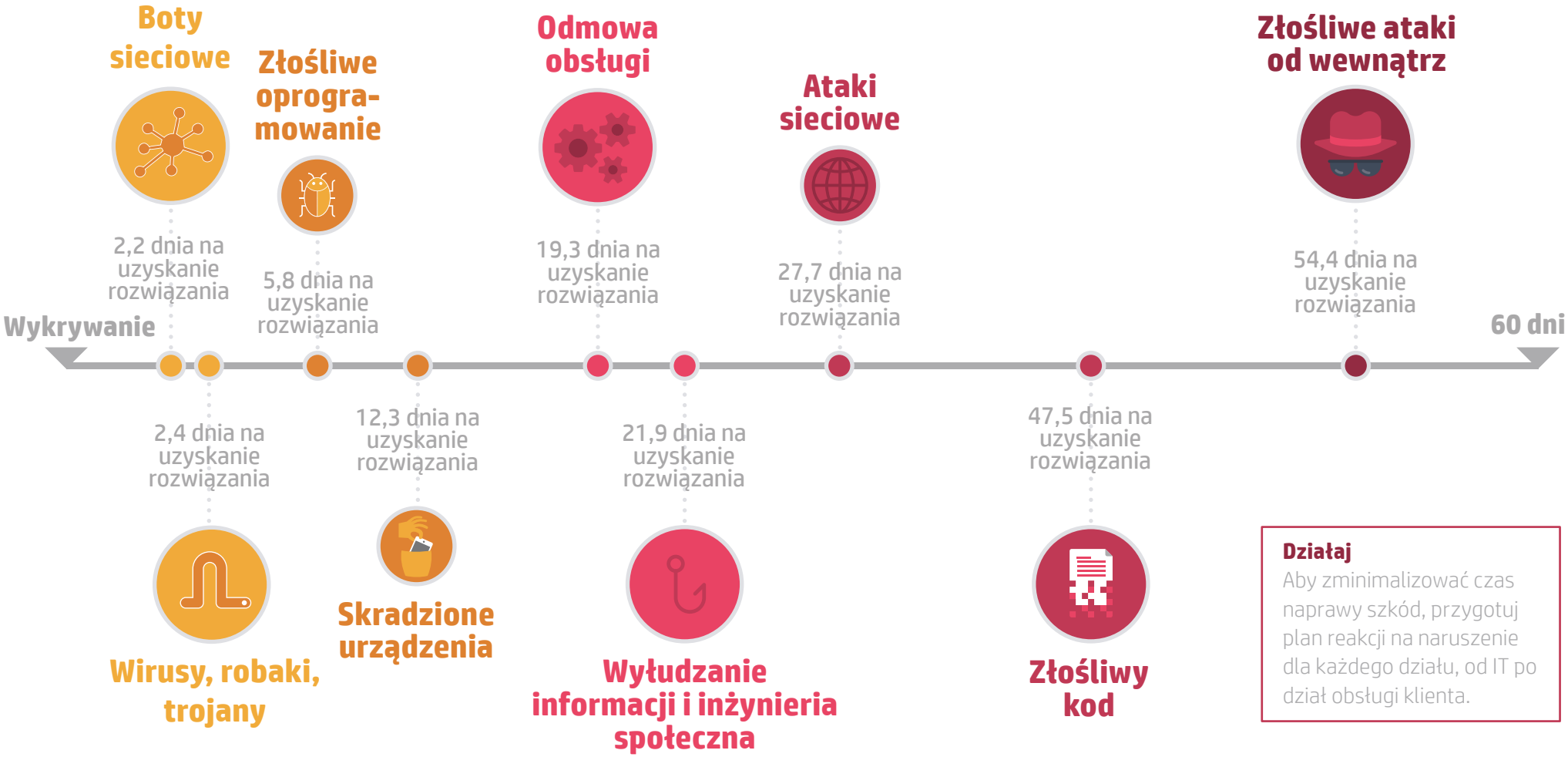
WSKAZÓWKA:
Wiele form oprogramowania typu malware jest przesyłanych w załącznikach wiadomości e-mail. Dlatego warto przeszkolić pracowników, tak aby umieli rozpoznawać podejrzane pliki wyglądające jak legalne dokumenty.

- Szacowany koszt cyberprzestępczości w firmach brytyjskich: 21 mld USD[15]
- Średni koszt cyberprzestępczości w firmie brytyjskiej w roku 2016: 5,7 mln funtów[16]
- Przedsiębiorstwa brytyjskie, które padły ofiarą cyberataku lub naruszenia w latach 2015–2016: 66%[17]

Źródła: [14] http://www.businessinsider.com/how-the-hackers-broke-into-sony-2014-12?IR=T [15] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[16] https://www.statista.com/statistics/293274/average-cyber-crime-costs-to-companies-in-selected-countries/ Jest 7,21 mln USD — przeliczona na £
[17] https://www.gov.uk/government/news/two-thirds-of-large-uk-businesses-hit-by-cyber-breach-or-attack-in-past-year

Cyberprzestępczość: czas usuwania szkód

Jak długo trwa usuwanie szkód po naruszeniu danych? Ponemon Institute[18] szacuje, że średnio 46 dni. To potencjalnie niebezpieczna sytuacja dla firm małej i średniej wielkości, które działają bez przerw.



Działaj
Aby zminimalizować czas naprawy szkód, przygotuj plan reakcji na naruszenie dla każdego działu, od IT po dział obsługi klienta.

Źródła: [18] Ponemon Institute Cost of Cyber Crime Study 2015

Jak ochronić firmę przed cyberprzestępczością

Podstawowe wskazówki i zasady bezpieczeństwa

Oto sześć najczęstszych celów ataków hakerskich naruszających systemy firm oraz sposoby obrony przed nimi.

Bazy danych klientów

Usługi w chmurze

Smartfony i tablety pracowników

Błędy pracowników

Internet rzeczy

Bramy sieciowe

Żyjemy w coraz bardziej cyfrowym świecie, w którym dane mają wartość większą niż kiedykolwiek wcześniej, dlatego cyberprzestępczość może mieć wiele form. Cyberprzestępcy często kradną informacje, a ponieważ używamy w pracy coraz większej liczby podłączonych urządzeń — od smartfonów i tabletów do drukarek bezprzewodowych — hakerzy mają coraz więcej punktów dostępu.

1 Bazy danych klientów

Dane finansowe to nie jedyny cel atakujących — informacje, takie jak nazwy i adresy e-mail, mogą być wykorzystywane do oszustw, wysyłania spamu lub włamywania się do innych kont.

Dla zaawansowanych hakerów większą wartość mają włamania do firm, które obsługują globalne korporacje. Pomyśl o tym jako o cyfrowym odpowiedniku włamania do sklepu ze sprzętem, aby uzyskać dostęp do ściany w piwnicy, która jest również ścianą skarbca banku narodowego znajdującego się w sąsiednim budynku.

Gdy atakujący dostaną się do mniejszego systemu, łatwiej im będzie uzyskać dostęp do danych klientów dużej firmy. Jak można naruszyć ochronę baz danych klientów? Wirusy, robaki i konie trojańskie — pobierane ze złośliwych stron lub e-maili — mogą uruchomić kod, który umożliwi hakerom uzyskanie dostępu do danych i ich kradzież.

Jak chronić dane klientów

- Używaj oprogramowania zabezpieczającego przeznaczonego dla firm, które zapewnia ochronę sieci, poczty elektronicznej i punktów końcowych.
- Zawsze aktualizuj oprogramowanie zabezpieczające, aby blokować najnowsze programy typu malware.
- Pobieraj aktualizacje programów systemowych, ponieważ starsze wersje mogą zawierać słabe punkty wykorzystywane przez hakerów.

2 Usługi w chmurze

Jak chronić dane klientów

- Szyfruj najważniejsze informacje za pomocą takich narzędzi, jak Smartcrypt firmy PKWARE, w którym do ustalania złożoności szyfrowania są używane zasady dostępu. W ten sposób autoryzowani użytkownicy widzą te dane, których oczekują, a nieautoryzowani — nie widzą nic.
- Utwórz silne hasło dla swojego konta w chmurze. W ustawieniach swojego konta w chmurze dokładnie zdefiniuj, kto ma dostęp do danych i co może z nimi robić.
- Wymagaj uwierzytelniania dwuskładnikowego — na przykład zarówno kodu smartfona, jak i hasła — aby wprowadzać zmiany w danych w chmurze, takie jak pobieranie, usuwanie i przenoszenie plików.

Przetwarzanie w chmurze stało się elementem spajającym infrastrukturę w wielu przedsiębiorstwach.

W badaniu 2016 IDG Cloud Computing Survey[19] stwierdzono, że 70% przedsiębiorstw ma przynajmniej część infrastruktury w chmurze, natomiast według Tripwire 90% firm używa chmury jako infrastruktury i/lub do przechowywania danych, w tym danych o znaczeniu krytycznym.[20]

Najważniejsze jest oczywiście bezpieczeństwo, ale w rzeczywistości dane są zwykle bezpieczniejsze w chmurze — przechowywane na dobrze zabezpieczonych serwerach przez firmę, której reputacja zależy od ich bezpieczeństwa.

To dlatego 64% przedsiębiorstw ankietowanych przez Tripwire stwierdziło, że chmura jest bezpieczniejsza niż przestarzałe systemy.

Na szczęście to zaufanie nie jest bezpodstawne — według badania 2015 BIS[21] 7% firm (dużych i małych) doświadczyło naruszenia usług w chmurze, co zwykle było wynikiem nieodpowiednich uprawnień dostępu lub zbyt słabych haseł. Jednak bezpieczna chmura nadal wymaga solidnego zarządzania bezpieczeństwem wewnętrznym. Pomyśl o drzwiach frontowych do firmy Sony.

Źródła:
[19] https://www.scribd.com/document/329518100/IDG-Enterprise-2016-Cloud-Computing-Survey
[20] https://www.tripwire.com/state-of-security/security-data-protection/enterprise-impressions-of-cloud-security-in-2016/
[21] 2015 Small Business Survey. Departament innowacji i umiejętności biznesowych

3 Smartfony i tablety personelu

Wiele osób używa prywatnych urządzeń do celów służbowych.

Zasady BYOD (Bring-Your-Own-Device) są dla firm efektywnym sposobem wykorzystania smartfonów należących do pracowników. Jest to trend rosnący, 53,2% organizacji wdrożyło zasady BYOD w ciągu ostatnich dwóch lat.[22] Ale urządzenia te mogą być gotowym celem dla hakerów.

Szacuje się, że jedna na pięć aplikacji przeznaczonych dla systemu Android zawiera jakąś formę inwazyjnego oprogramowania typu malware, która może zostać przekazana do plików firmowych i systemów w celu monitorowania aktywności lub kradzieży informacji.

Zagrożenie wzrasta, liczba organizacji zgłaszających zagrożenie atakiem, którego celem są urządzenia mobilne, wzrosła do 64,9%.[23]

Pracownicy, którym skradziono telefony, mogą wbrew własnej woli stać się furtką dla hakerów. Złodziej telefonu może sprzedać urządzenie nabywcy na czarnym rynku, który z kolei może naruszyć informacje poszkodowanej firmy lub uzyskać dostęp do systemów większego klienta. Organizacje oceniły swoją zdolność do ochrony przed zagrożeniami z urządzeń mobilnych na 3,54 w skali od 1 do 5. To najniższa ocena ze wszystkich potencjalnych źródeł zagrożeń, o które pytaliśmy.[24]

W jaki sposób zabezpieczyć prywatne urządzenia

- Zainstaluj narzędzie do wykrywania zagrożeń, takie jak Duo's X-Ray dla urządzeń z systemem Android, aby łatwiej śledzić aplikacje i podejrzany kod.
- Poproś pracowników, aby włączyli zdalne czyszczenie (dostępne bezpłatnie dla urządzeń z systemem Android, urządzeń iPhone i telefonów z systemem Windows; z subskrypcją dla telefonów BlackBerry). Wówczas w przypadku utraty urządzenia będzie można usunąć poufne dane, zarówno służbowe, jak i prywatne.
- Poproś pracowników, aby włączyli w swoich smartfonach szyfrowanie urządzenia w celu zabezpieczenia danych (w telefonach z nowymi systemami iOS i Android jest ono włączone domyślnie).

Źródła: [22] 2016 Cyberthreat Defense Report, CyberEdge [23] ibid [24] ibid

4 Błędy pracowników

Jak pomóc zespołowi

- Zorganizuj dla pracowników kurs dotyczący cyberbezpieczeństwa i regularne szkolenia dotyczące najnowszych zagrożeń.
- Zapewnij wdrożenie protokołu zabezpieczeń dostosowanego do Twojej firmy i typów przetwarzanych danych.
- Utwórz zespół ds. wdrażania zasad cyberbezpieczeństwa wśród pracowników oraz klientów i partnerów biznesowych.

Najbardziej podstawową zasadą bezpieczeństwa cybernetycznego jest dobra polityka dotycząca haseł, a 31% najgorszych naruszeń bezpieczeństwa w 2015 r. było wynikiem incydentu związanego z pracownikami.

Atakujący często wykorzystują błędy ludzkie — od hakowania słabych haseł do kradzieży dokumentów przesyłanych w wiadomościach e-mail przez niezabezpieczone połączenia czy wyłudzanie informacji przesyłanych w wiadomościach e-mail do konkretnych pracowników.

5 Przygotuj się na Internet rzeczy

Firma badawcza IDC przewiduje, że liczba urządzeń podłączonych do Internetu w roku 2020 będzie równa 30 mld. Szacuje się, że obecnie jest ich 13 mld.[25]

Komputery w biurze są chronione przynajmniej hasłem, a czasem nawet oprogramowaniem zabezpieczającym, jednak kolejki i zadania druku zwykle nie są chronione w podobny sposób.

Takie niezabezpieczone drukarki — i inny sprzęt podłączony do sieci — mogą paść ofiarą programów podsłuchujących, które mogą rejestrować zadania druku, ruch sieciowy oraz nazwy użytkowników i hasła, a następnie przesyłać je do serwera cyberprzestępców.

Warto zauważyć, że najbardziej znanym naruszeniem Dyn było podłączenie do sieci kamer internetowych CCTV wyprodukowanych przez jedną firmę — XiongMai Technologies. Według firmy Flashpoint zajmującej się zabezpieczeniami

To pokazuje, że każde urządzenie podłączone do sieci jest punktem końcowym, a sieć jest tak silna, jak jej najsłabiej zabezpieczone urządzenie. W około 97% organizacji opracowano procedury zabezpieczeń dla komputerów stacjonarnych i laptopów, w 77% — dla urządzeń przenośnych, a w 57% opracowano procedury zabezpieczeń dla drukarek.[26] Jedynym sposobem zapewnienia bezpieczeństwa w każdej firmie jest przestrzeganie procedur zabezpieczeń na każdym urządzeniu, które jest punktem końcowym.

Jak przygotować się na Internet rzeczy

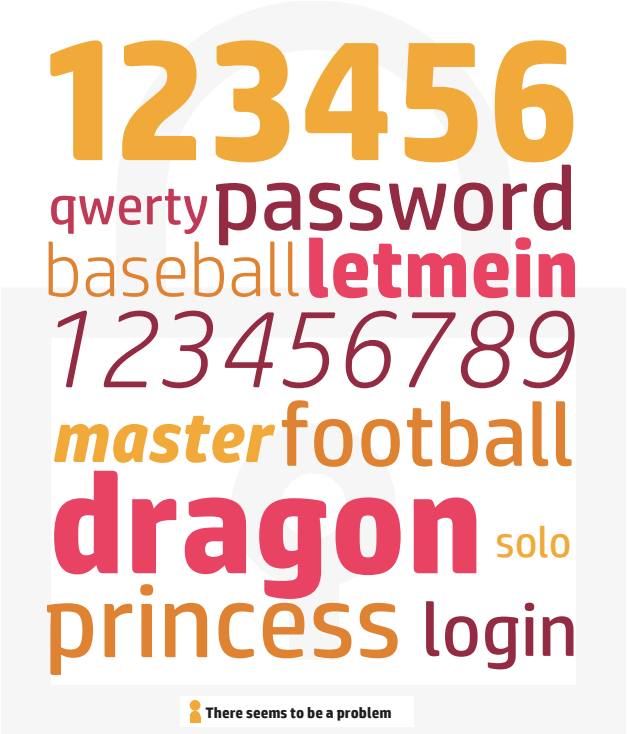
- Usuń lub wyłącz sprzętowo nieużywane funkcje, gdyż więcej funkcji oznacza więcej furtek dla atakujących.

Źródła: [25] PwC: The Global State of Information Security Survey 2016 [26] HPI Printer Security Research, Spiceworks 2016

Hasła i oprogramowanie typu ransomware

Najpopularniejsze hasła

Na początku roku 2013 reporter Ars Technica, który nigdy wcześniej nie był cyberprzestępcą ani nie miał żadnego doświadczenia w łamaniu haseł i uzyskiwaniu dostępu do systemów chronionych hasłami, złamał 8000 z ponad 16 000 zaszyfrowanych haseł w ciągu jednego dnia*. Jaką szansę mają najczęściej używane hasła przeciwko zmotywowanemu włamywaczowi?



Co to jest oprogramowanie typu ransomware

Cyberprzestępcy coraz częściej korzystają z oprogramowania typu ransomware. Jest to rodzaj złośliwego kodu, który przejmuje kontrolę nad systemem i odblokowuje go po przekazaniu okupu odpowiedniej wysokości w bitcoinach. Tysiące osób zostało poszkodowanych w wyniku ataku trojana o nazwie Cryptolocker z 2013 r., który zwrócił uwagę brytyjskiej krajowej agencji ds. przestępczości (National Crime Agency) i jej jednostki ds. cyberprzestępczości (National Cyber Crime Unit). Oto krótki przegląd sposobu działania ataków tego typu.

1. Instalacja	Złośliwy kod działa na komputerze po niezamierzonym pobraniu, za pośrednictwem wiadomości e-mail lub złośliwej strony.
2. Powiado-mienie swoich twórców	Oprogramowanie typu ransomware (do wymuszania okupu) łączy się ze swoim serwerem głównym i ustanawia klucz szyfrowania.
3. Szyfrowanie Twoich plików	Oprogramowanie typu ransomware skanuje pliki w sieci i szyfruje je, przez co stają się niedostępne.
4. Wymuszenie	Zwykle na ekranie użytkownika jest wyświetlane okienko z komunikatem informującym, ile czasu zostało do usunięcia plików i jaką kwotę należy wpłacić, aby je odzyskać.
5. Zapłacenie okupu	Właściciel firmy może zamówić walutę cyfrową, taką jak bitcoin i przekazać ją atakującemu z nadzieją, że ten odszyfruje pliki.

* Splashdata

6 Bramy sieciowe

Gdy hakerzy chcą wejść do sieci, mogą zainaugurować atak DDoS — tysiące komputerów zainfekowanych oprogramowaniem typu malware zostaje połączonych w celu wygenerowania tak dużego niepożądanego ruchu, że sieć pada pod ciężarem ataku.

Atakujący za pomocą DDoS często chcą skierować uwagę administratorów witryn na zablokowany system, a sami w tym czasie kradną dane lub instalują oprogramowanie typu malware i planują skoki na dane w przyszłości. Niektóre ataki DDoS są również wynikiem „skryptów dzieciaków" („script kiddies"), początkujących hakerów, którzy po prostu chcą zablokować stronę internetową, bo umieją to zrobić. Nawet kilkugodzinne wyłączenie witryny internetowej może być szkodliwe dla podstawowej działalności firmy i jej reputacji.

WSKAZÓWKA:
Zainwestuj w sprzęt z wbudowanymi zabezpieczeniami, takimi jak zaawansowane uwierzytelnianie i narzędzia do szyfrowania.

Jak zabezpieczyć sieć

- Zbuduj systemy sprawdzające ruch wchodzący i wychodzący z sieci. Nieoczekiwane zwiększenie ruchu może oznaczać atak, natomiast stały, ale trudny do wyjaśnienia wzrost aktywności może wskazywać, że trojan przekazuje informacje do swojej bazy.
- Filtruj cały ruch, tak aby w końcu do sieci trafiał tylko ruch wymagany do obsługi firmy.
- Upewnij się, że każdy router, przełącznik czy inne urządzenie sieciowe korzysta z tej samej wersji oprogramowania i funkcjonalności oraz zawsze pobieraj aktualizacje oprogramowania.

Przyszłość cyberbezpieczeństwa firm

W przypadku firm internetowych lub intensywnie wykorzystujących Internet solidne zabezpieczenia są wyjątkowo ważne.

Obecnie pracownicy coraz częściej przynoszą do pracy własne urządzenia. Firmy korzystają z platform przetwarzania danych w chmurze i zlecają na zewnątrz kluczowe usługi techniczne. Coraz więcej osób pracuje zdalnie. Zapewnienie bezpieczeństwa w cyberprzestrzeni staje się znacznie trudniejsze, gdy nie kontrolujesz ani urządzenia, ani infrastruktury, ani miejsca pracy.

Jednocześnie smartfony nauczyły nas, że interesy można robić zawsze i wszędzie. Kawiarnia jest tak samo dobrym miejscem do pracy jak biuro. Korzystamy z publicznych sieci Wi-Fi do przetwarzania dużych ilości danych biznesowych i osobistych — często na słabo zabezpieczonych smartfonach. Przestępcy zauważają tę zmianę. Jeśli nie zwracamy uwagi na warunki pracy, odbywa się to kosztem bezpieczeństwa.

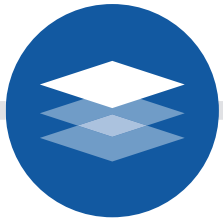
W najbliższych latach termin „cyberbezpieczeństwo" będzie oznaczać znacznie więcej niż dodawanie oprogramowania antywirusowego do naszych urządzeń lub aktualizowanie haseł co sześć miesięcy. Firmy powinny korzystać raczej z udoskonalonych środków bezpieczeństwa, które działają w taki sam sposób zarówno zdalnie, jak i w biurze zarządzanym przez administratora IT

W rozproszonych organizacjach jutra cyberbezpieczeństwo zależy od wyrafinowanej analizy, która izoluje nietypowe zachowanie i chroni wszystkie punkty dostępu.

Przyszłość cyberbezpieczeństwa firm

Analityka: wykrywanie zagrożeń cyberbezpieczeństwa

Nawet jeśli na Twojej stronie internetowej nie ma zbyt dużego ruchu, jest on zgodny z pewnymi wzorcami. Korzystanie z narzędzi analitycznych, które mierzą i rejestrują aktywność, może ułatwić postawienie właściwej diagnozy, gdy coś jest nie tak. Ich działanie polega na śledzeniu i dokumentowaniu normalnych zachowań w celu wykrywania anomalii w późniejszym czasie. Po ich wykryciu administratorzy mogą przejść do kontrofensywy i odpierać ataki, zanim zdążą one wywołać chaos w cyberprzestrzeni.



Hierarchia warstwowa: bądź o krok przed atakującymi

Warstwowe zabezpieczenia, nazywane czasem „obroną w głąb", chronią każdy punkt dostępu na wiele sposobów. Typowe podejścia obejmują takie warstwy, jak rozszerzone certyfikaty SSL do sprawdzania poprawności, które utrudniają fałszowanie danych uwierzytelniających wymaganych podczas wchodzenia do bezpiecznej sieci. Wieloczynnikowe uwierzytelnianie wymaga od atakujących większego wysiłku niż tylko złamania hasła.

Niezależnie od konkretnej technologii, która zostanie wykorzystana, głównym celem tworzenia wielu warstw jest zabezpieczenie wszystkich wrażliwych obszarów sieci firmowej. Użytkownicy i partnerzy mogą potrzebować dodatkowego czasu i wysiłku, aby uzyskać dostęp do kluczowych danych, ale te niedogodności powinny dać znacznie więcej korzyści, niż tylko zapewnić spokój Twojej firmie.

Zacznij działać

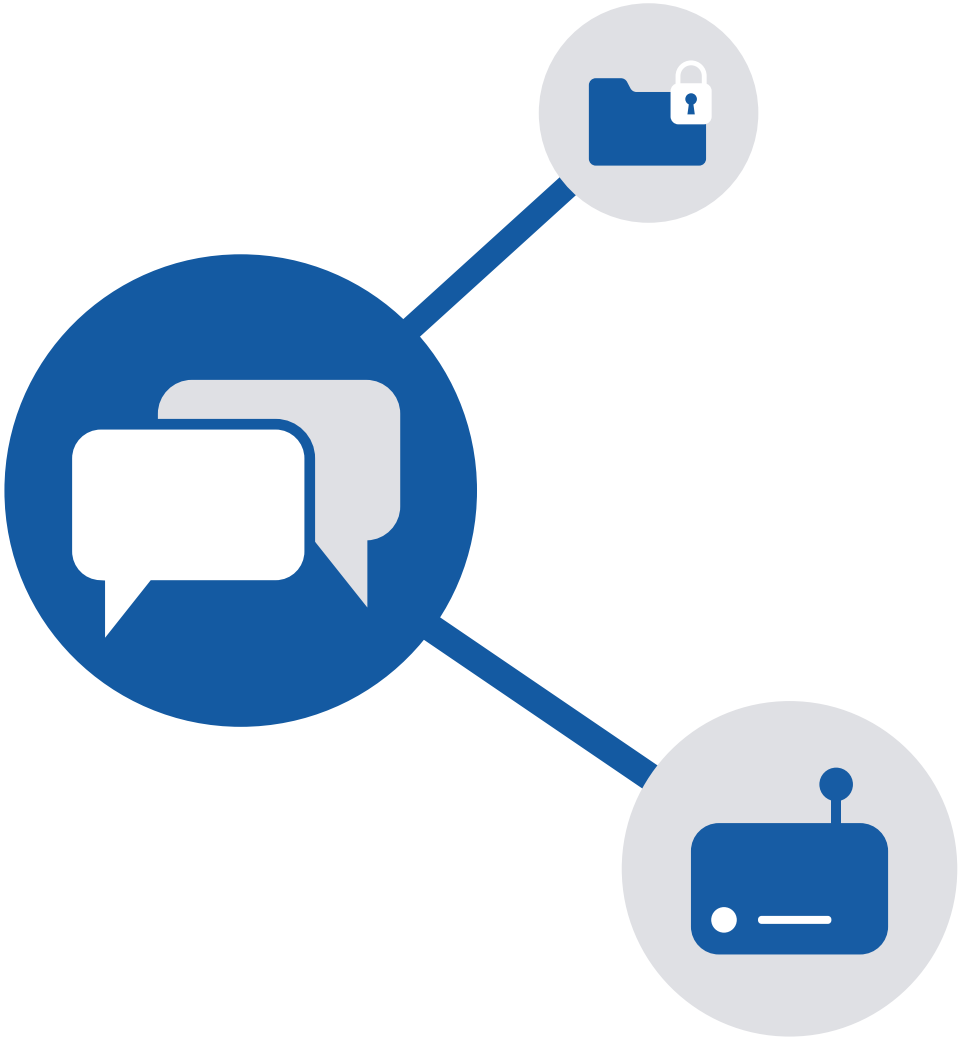
Inwestowanie w oprogramowanie zabezpieczające i szkolenia to najlepsza obrona. Zacznij od sprawdzenia systemów i infrastruktury. Czy robisz wystarczająco dużo? Co możesz zrobić lepiej?

Możesz także zadzwonić do naszych ekspertów z firmy Hewlett Packard Inc. Nasza zbiorowa baza wiedzy koncentruje się na tym, aby stawiać czoła zagrożeniom, a nie tylko reagować na nie. Więcej informacji znajdziesz na naszej stronie internetowej: HP.com.

WSKAZÓWKA:
Śledź i dokumentuj normalne zachowanie teraz, aby w przyszłości wykrywać anomalie.

Uwagi na temat zabezpieczania urządzeń końcowych

Zabezpieczenie wszystkich urządzeń w sieci



Badanie zabezpieczeń przeprowadzone przez firmę Spiceworks[27] pokazało, że głównym źródłem zagrożeń bezpieczeństwa w badanych firmach były:

- Komputery stacjonarne i przenośne: 81% zewnętrznych i 80% wewnętrznych
- Urządzenia przenośne: 36% zewnętrznych i 38% wewnętrznych
- Drukarki: 16% zewnętrznych i 16% wewnętrznych

Które z tych zagrożeń wymagają najpilniejszego zabezpieczenia? Na wszystkie te pytania jest prosta odpowiedź. Choć powinno to być zupełnie oczywiste, w niepokojąco dużej liczbie organizacji obserwujemy wybiórcze podejście do tego, które urządzenia zabezpieczać.

Z perspektywy HP każde urządzenie, które łączy się z siecią, musi być zabezpieczone. Po prostu: sieć jest tak bezpieczna, jak bezpieczne jest najmniej zabezpieczone urządzenie.

Intuicja może podpowiadać, że zabezpieczenie podłączonej drukarki jest mniej ważne niż zabezpieczenie floty komputerów przenośnych. Ale ryzyko jest takie samo. Hakerzy często celują w takie urządzenia, jak drukarki i inne inteligentne urządzenia podłączone do sieci. Wiedzą, że zwykle nie są one zbyt dobrze zabezpieczone, mimo że zapewniają taki sam poziom dostępu do sieci.

Źródła: [27] HP Printer Security Research 2016, Spiceworks

HP: Wytyczamy nowe szlaki

Cyberbezpieczeństwo ciągle się zmienia. HP oferuje narzędzia, które pomogą Ci zorganizować obronę.

W cyberbezpieczeństwie nie ma szybkich poprawek. Solidna obrona wymaga kompleksowego podejścia obejmującego sieci, urządzenia i ludzi. Wybór odpowiedniej technologii to dobry początek.

W HP bezpieczeństwo stawiamy na pierwszym miejscu. Urządzenia HP Premium Elite wyposażone są w czołowe na rynku funkcje zabezpieczeń, niedostępne gdzie indziej, takie jak HP SureStart — pierwszy na świecie samonaprawiający się system BIOS.

Urządzenia HP mają wbudowane następujące elementy:

- **Blokada Bluetooth:** Urządzenie korzystające z technologii Bluetooth automatycznie blokuje się po utracie zasięgu i odblokowuje się, gdy ponownie znajdzie się w zasięgu.
- **Zabezpieczenia biometryczne:** Systemy rozpoznawania twarzy i linii papilarnych umożliwiają dostęp tylko użytkownikom uwierzytelnionym metodą biometryczną.
- **Ekrany HP SureView*:** Przyciemniony monitor uniemożliwia osobom postronnym oglądanie ekranu, chroniąc poufny materiał podczas pracy w podróży.
- **Samonaprawiający się system BIOS HP SureStart:** Każdy system HP Elite monitoruje swój BIOS co 15 minut. Wykrycie jakiejkolwiek anomalii powoduje reset komputera do oryginalnego stanu, a tym samym usunięcie intruzów.

System HP Elite sam nie zabezpieczy Twojej firmy. Jednak będzie to solidna pierwsza linia obrony. Więcej informacji o naszych urządzeniach HP Elite znajdziesz na stronie www8.hp.com.

* Wybrane modele

HP: Wytyczamy nowe szlaki w dziedzinie drukowania

Chroń swoją sieć przy pomocy najbezpieczniejszych na świecie rozwiązań w zakresie drukowania*

„Firma HP posiada najszerszą oraz najbardziej rozbudowaną ofertę rozwiązań i usług zabezpieczających na rynku, co potwierdza długofalową strategię inwestowania w bezpieczeństwo druku”.

– Quocirca, styczeń 2017**

Urządzenia HP mają wbudowane następujące elementy:

- **Wykrywanie włamań podczas pracy:** Oferowana przez HP funkcja wykrywania włamań w trakcie pracy pomaga chronić urządzenia, gdy pracują i są podłączone do sieci – wówczas ma miejsce największa liczba ataków.
- **Oprogramowanie Jet Advantage Security Manager:** Pozwala menedżerom IT na sprawną ocenę sytuacji i w razie konieczności podjęcie działań mających na celu poprawę bezpieczeństwa floty urządzeń oraz zapewnienie zgodności z firmową polityką zabezpieczeń.
- **Funkcja samonaprawy systemu BIOS HP SureStart:** Po uruchomieniu komputera rozwiązanie HP SureStart wykrywa próby manipulacji i automatycznie naprawia system BIOS. Przywracana jest wbudowana fabryczna kopia oprogramowania.
- **Tworzenie list dozwolonych kodów:** Rozwiązanie to sprawia, że do pamięci ładowany jest oryginalny, znany kod HP. W razie wykrycia anomalii, urządzenie uruchamia się ponownie w bezpiecznym trybie offline i następuje powiadomienie personelu informatycznego.

Źródła: *5 Zapewnienie dotyczące „najbezpieczniejszych rozwiązań w zakresie drukowania” na podstawie przeprowadzonego przez firmę HP przeglądu opublikowanej w 2016 r. listy zabezpieczeń konkurencyjnych drukarek danej klasy. Tylko firma HP oferuje kombinację funkcji zabezpieczeń, które umożliwiają monitorowanie, wykrywanie i automatyczne powstrzymywanie ataku, a następnie autoryzację oprogramowania podczas ponownego uruchomienia. **Quocirca, „Print security: An imperative in the IoT era”, quocirca.com/content/print-security-imperative-iot-era, styczeń 2017.

Słownik i inne publikacje

Dostęp do narzędzi do zarządzania

Bot sieciowy:
Ogólnie jest to typ automatycznego programu zaprojektowanego w celu uzyskania dostępu do komputerów połączonych z Internetem i ich kontrolowania bez wiedzy ich właścicieli. Komputery często są infekowane oprogramowaniem typu malware. Hakerzy używają botów sieciowych do ataków typu **Denial of Service** na stronie internetowej.

Narzędzia zapobiegające utracie danych:
Szeroka kategoria oprogramowania do monitorowania poufnych danych i blokowania prób dostępu do nich i ich kopiowania przez nieautoryzowane osoby. Różne podejścia umożliwiają ochronę w punkcie dostępu (tj. w punkcie końcowym) podczas ruchu w sieci lub w systemie plików. Gartner ocenia wzrost tego rynku **o 25%** w 2013 roku.

Technologie szyfrowania:
Narzędzia przekształcające **dane do postaci niemożliwej do odczytu** bez specjalnego dekodera. Brytyjski komisarz ds. informacji w ostatnich latach **zdecydowanie opowiada się** za różnego rodzaju szyfrowaniem. Niedawno rząd został zmuszony do **zmiany stanowiska dotyczącego technologii szyfrowania** w wyniku poważnej krytyki.

Technologie zapór:
Inny szeroki termin opisujący pewien typ urządzenia, w którym są wykorzystywane algorytmy i inne techniki umożliwiające blokowanie dostępu do sieci nieautoryzowanym użytkownikom i przesyłom danych. **Wersje następnej generacji** tych urządzeń mogą już łączyć funkcje, które dotychczas były obsługiwane przez różne urządzenia. Na przykład wykrywanie intruzów. Pojawia się również tendencja do korzystania z aplikacji w celu rozróżnienia między ruchem internetowym z implementacji salesforce.com i z serwisu Facebook.

Narzędzia GRC:
Określenie to odnosi się do szeroko zakrojonych i skoordynowanych inicjatyw wewnątrz firmy dotyczących operacji zarządzania w sposób zgodny z przepisami i przyjętymi zasadami, co zmniejsza ryzyko.

Oprogramowanie typu malware:
Szeroka kategoria oprogramowania, które może uszkodzić, a nawet zniszczyć inne systemy. Przykłady oprogramowania typu malware to wirusy, robaki i trojany. W badaniach przeprowadzonych przez firmę Ponemon cytowanych w tej broszurze przyjęto, że do oprogramowania typu malware nie zalicza się wirusów, które „znajdują się w punkcie końcowym, ale jeszcze nie infiltrują sieci".

Kontrola obwodowa:
Ogólna kategoria opisująca sposób cyberobrony w punkcie, w którym publiczny Internet lub inna sieć publiczna łączy się z siecią prywatną, należącą do lokalnego właściciela i zarządzaną lokalnie. **Zwykle wymaga wielu warstw** i typów urządzeń.

Wyłudzanie informacji:
Zwykle przy użyciu poczty elektronicznej, gdy atakujący prosi o informacje identyfikacyjne w poważnie wyglądającym oknie dialogowym.

Narzędzia do zarządzania zasadami:
Ogólnie rzecz ujmując, narzędzia do zarządzania zasadami służą do definiowania standardów określających, do jakich danych konkretne grupy użytkowników mają dostęp, a do jakich nie oraz do wymuszania respektowania tych zasad w całej sieci. Spójność zapewnia bezpieczeństwo (przynajmniej w teorii).

Słownik i inne publikacje

Inteligentne systemy zabezpieczeń:
Szeroka gama inteligentnych zabezpieczeń, które mogą pomóc gromadzić i syntetyzować informacje dotyczące zagrożeń. Mogą to być bardzo różne systemy, od systemów logowania do systemów wykrywających anomalie w sieci.

Inżynieria społeczna:
O inżynierii społecznej mówimy, jeśli atakujący próbuje przekonać autoryzowanego użytkownika do przekazania informacji, których ten przekazywać nie powinien, nadając mu potrzebne uprawnienia dostępu.

Koń trojański:
Podobnie jak wirusy i robaki, aby konie trojańskie mogły działać, muszą zostać zainstalowane przez użytkownika, dlatego zwykle są starannie ukryte. Ich działanie może być bardzo różne: od zmiany ustawień komputera czy usuwania plików do utworzenia „tylnych drzwi", które haker może wykorzystać w późniejszym czasie.

Wirusy:
Złośliwy kod zdolny do replikowania i rozprzestrzeniania się w całej sieci.

Ataki sieciowe:
Najczęściej atak sieciowy polega na przekierowaniu przeglądarki na złośliwą stronę.

Robaki:
W przeciwieństwie do wirusów, które rozprzestrzeniają się razem z plikiem-gospodarzem, robaki replikują się niezależnie od pliku-gospodarza, takiego jak dokument programu Word lub arkusz kalkulacyjny programu Excel, dlatego nie potrzebują dodatkowych działań człowieka, aby siać spustoszenie. Komunikatory są często narażone na rozprzestrzenianie się robaków; Skype padł ofiarą takiego ataku w 2012 roku.

4AA7-1085PLE