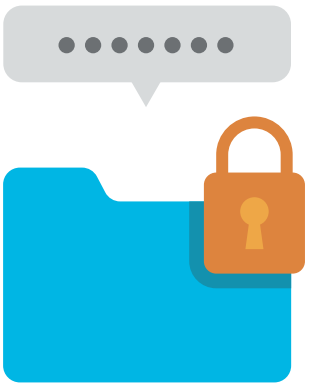
Opracowanie dla biznesu

Bezpieczeństwo zaczyna się w punktach końcowych

Które z nich są najważniejsze

Dostarczone przez

Podsumowanie



W ciągu ostatnich 12 miesięcy 82% organizacji doświadczyło naruszenia bezpieczeństwa.[1] Cyberprzestępczość wzrasta: rośnie częstotliwość ataków, są one coraz groźniejsze i powodują wzrost kosztów usuwania ich skutków.

Dotychczasowe spojrzenie na bezpieczeństwo sieci firmowej - ochrona sieci przy pomocy zapory firewall - przestało być aktualne. Wykrywanie i reagowanie na zagrożenia jest znacznie bardziej efektywne.

Często jednak budżety IT nie wytrzymują obciążeń związanych ze zmieniającymi się zasadami zabezpieczeń. 77% pieniędzy nadal jest wydawane na prewencję i ochronę.[2] Tylko 36% menedżerów IT zdaje sobie sprawę, że powinni znacznie zwiększyć budżet na efektywne zabezpieczenie punktów końcowych.[3]

Skuteczna ochrona danych jest możliwa. Odpowiednia technologia, czyli rozwiązania do wykrywania i reagowania oraz zabezpieczenie pojedynczych urządzeń, odpowiednia strategia i wystarczające zasoby to elementy niezbędne, aby organizacje były w stanie ochronić się przed cyberprzestępczością.

Brak wzrostu inwestycji w zabezpieczenia sieci firmowej oraz w skuteczną ochronę spowoduje zwiększoną częstotliwość naruszeń bezpieczeństwa przy zwiększonych kosztach organizacji.

Wprowadzenie

Bezpieczeństwo cyfrowe w czasach sieci amorficznych

60% specjalistów IT zauważa, że wzrost cyberprzestępczości i poziom jej zaawansowania sprawiają, że ich linie obrony są z łatwością pokonywane. 80% osób zajmujących się bezpieczeństwem zdaje sobie sprawę z istnienia zaawansowanych trwałych zagrożeń (Advanced Persistent Threats, APT), firm przestępczych, hakerów sponsorowanych przez państwa i haktywistów oraz z coraz większego zagrożenia z ich strony, które staje się największym wyzwaniem dla bezpieczeństwa IT.[4]

Nie mylą się. W Wielkiej Brytanii rząd ponosi koszty ekonomiczne cyberprzestępczości na poziomie 27 mld funtów. Jest to wartość „istotna i prawdopodobnie wzrastająca", przy czym straty ponoszone przez przedsiębiorstwa wynoszą 21 mld funtów.[5] W raporcie State of the Endpoint Report przygotowanym w 2016 roku przez firmę Ponemon 78% firm zgłosiło wzrost liczby ataków oprogramowania typu malware. To znaczny wzrost w porównaniu z 47% w 2011 roku.

Jednak skupianie się na zagrożeniach zewnętrznych nie jest najlepszym rozwiązaniem i może prowadzić do naiwnego koncentrowania zasobów na zapobieganiu i ochronie obwodowej.

Ataki zewnętrzne – wirusy, szkodliwe oprogramowanie, wyłudzanie informacji – są wprawdzie bardziej rozpowszechnione, ale ataki wewnętrzne są bardziej kosztowne.[6] Poza tym wiele ataków zewnętrznych wykorzystuje wewnętrzne luki: niedbałych pracowników ignorujących protokoły bezpieczeństwa, niezabezpieczone urządzenia łączące się z siecią – 81% ankietowanych w badaniu Ponemon wskazało je jako największe zagrożenie dla bezpieczeństwa IT.

W miarę upływu czasu powyższe spostrzeżenie jest coraz bliższe prawdy. Punkt końcowy to najsłabszy węzeł w każdej sieci, a wraz ze wzrostem trendu BYOD, pracy zdalnej i Internetu rzeczy (IoT) liczba punktów końcowych wielokrotnie wzrasta. Oznacza to, że liczba wejść dla hakerów również zwiększyła się wielokrotnie.

To zupełnie inny świat niż kontrolowana sieć komputerów stacjonarnych połączonych w sieć Ethernet. Sieci biznesowe stały się amorficzne – to splątanie urządzeń zarówno biznesowych, jak i osobistych. Dostęp do danych można uzyskać przez wiele węzłów Wi-Fi zarówno na terenie firmy, jak i poza nią.

W tej sytuacji wymagane jest nowe podejście do bezpieczeństwa cyfrowego. Nowe strategie, które są odpowiedzią na zmieniającą się cyberprzestępczość. Nowe technologie zdolne stawić czoła coraz bardziej wyrafinowanym rosnącym zagrożeniom.

W tym opracowaniu ocenimy rodzaj i skalę zagrożeń – zdiagnozujemy problem, a następnie zastanowimy się, jak zadbać o bezpieczeństwo w czasach coraz większej liczby urządzeń, niezabezpieczonych sieci i chmur.

[1] HPI Printer Security Research 2016 (Spiceworks)
[2] PAC Incident Response Management 2015: https://www.pac-online.com/download/19443/155514
[3] Ponemon 2016 State of the Endpoint Report
[4] IBM CISO Assessment 2014
[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[6] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic

Skala zagrożenia

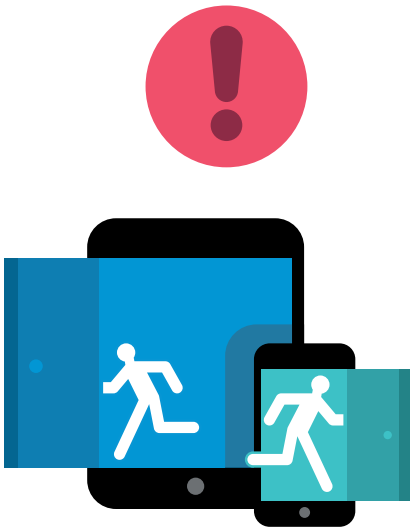
Usunięcie szkód po naruszeniu dostępu do danych kosztuje firmy przeciętnie 907 053 USD oraz obniżenie dochodu o kolejne 13%. Organizacja potrzebuje średnio 9 tygodni na usunięcie szkód.[7]

Około 85% firm ankietowanych w ramach badań do raportu HP Printer Security Report 2015 przyznało, że doświadczyło zagrożenia/naruszenia w ciągu ostatnich 12 miesięcy. 80% ankietowanych specjalistów IT przewiduje wzrost zagrożeń w ciągu najbliższych trzech lat.[8]

Cyberprzestępczość generuje realne koszty. Straty spowodowane kradzieżą lub zniszczeniem. Mniejsze zyski spowodowane utratą reputacji i obniżeniem wydajności. Utrata zasobów wykorzystywanych do usuwania szkód po ataku – czas centrum pomocy, wdrożenie nowych zasad bezpieczeństwa, odejścia pracowników i inne problemy wewnętrzne. Grzywny i kary nałożone przez organy regulacyjne. Spadek wartości akcji.

Zagrożenie wzrasta wraz z liczbą urządzeń podłączonych do sieci. Firma Gartner przewiduje, wzrost liczby punktów końcowych z 6,4 mld w 2016 roku do 11,4 mld w roku 2018. W roku 2020 ponad 25% zidentyfikowanych ataków w przedsiębiorstwach będzie związanych z Internetem rzeczy (Internet of Things, IoT), ale IoT będzie angażować mniej niż 10% budżetów przeznaczonych na bezpieczeństwo.[9]

Zagrożenie cyberprzestępczością jest ogromne i ciągle rośnie.



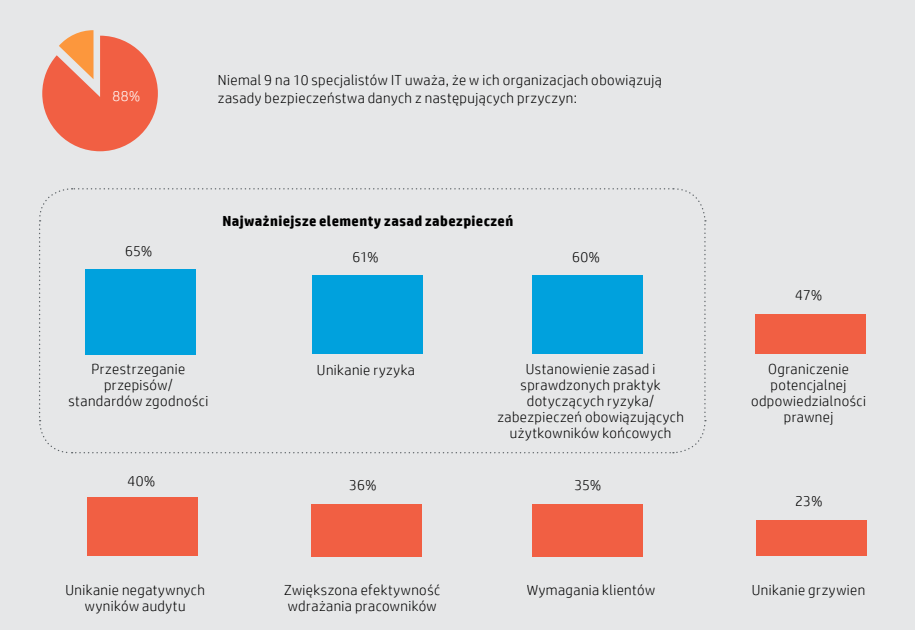
Forma zagrożenia

Firmy codziennie są narażone na cyberataki. Większość z nich to niezbyt szkodliwe wirusy i oprogramowanie typu malware. 99% organizacji uczestniczących w ankiecie przeprowadzonej przez Ponemon w 2016 roku padło ofiarą złośliwego oprogramowania w ciągu ostatnich 12 miesięcy. Zewnętrzne ataki internetowe tego typu są stosunkowo łagodne, kosztują organizacje średnio 4639 USD.[10]

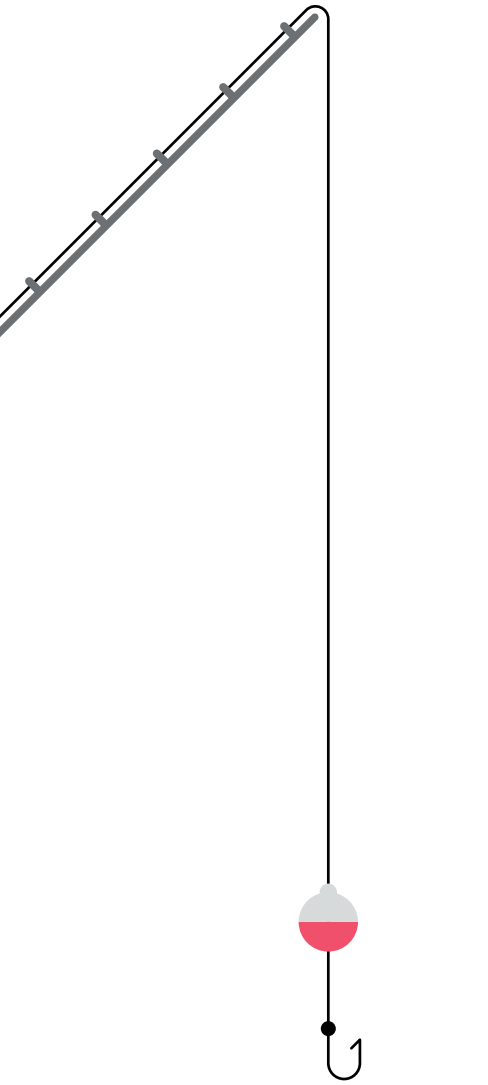
Niestety liczba znacznie poważniejszych ataków ciągle rośnie. 51% organizacji uczestniczących w ankiecie w 2015 r. było ofiarami ataków typu Direct Denial of Service (DDoS), które mogły być paraliżujące – kosztowały średnio 127 000 USD. Znacznie bardziej alarmujący jest fakt, że 35% organizacji uczestniczących w ankiecie było ofiarami ataków złośliwego oprogramowania od wewnątrz, które kosztowały średnio 145 000 USD.[9]

W przyszłości możemy spodziewać się nieustających drobnych ataków z zewnątrz i rzadszych, ale znacznie poważniejszych ataków, których przyczyną będą najczęściej zaniedbania pracowników lub ich złośliwości. 62% organizacji padło ofiarą ataków polegających na wyłudzaniu informacji, a łatwowierność pracowników kosztowała firmy średnio 86 000 USD.[11]

Oddzielna ankieta przeprowadzona przez Spiceworks na zlecenie HP pokazała, że w 90 brytyjskich firmach liczba ataków zmalała w latach 2014–2015.[12]



[7] NTT Security Risk:Value Report 2016
[8] HP 2Printer Security Report 2015
[9] http://www.gartner.com/newsroom/id/3291817
[10] https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-8392enw.pdf
[11] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic
[12] HPI Printer Security Research, Spiceworks 2016



Skąd się biorą naruszenia

Hakerzy są czasem przedstawiani jako profesjonaliści dążący do uszczelnienia sieci rządowych i korporacyjnych, ale rzeczywistość jest zwykle bardziej przyziemna.

Wirusy mogą być wykorzystywane do wyszukiwania zagrożeń w sieci, ale oprogramowanie typu malware zwykle wymaga błędu użytkownika. Od tego zależą ataki polegające na wyłudzaniu informacji/inżynierii społecznej. Duże ataki DDoS i kradzieże informacji są również często wynikiem zaniedbań użytkowników.

Na przykład słynny do dziś atak hakerski na Dropbox był podobno spowodowany przez nieostrożnego pracownika Dropbox, który używał dla systemów wewnętrznych tego samego hasła, co dla konta LinkedIn.[13] Domniemane rosyjskie włamania do DNC wyszły na jaw, ponieważ John Podesta, były doradca pani Clinton, kliknął łącze w wiadomości e-mail wyłudzającej informacje, błędnie oznaczonej przez asystenta jako „sprawdzona".[14]

Czasem hakerzy nie muszą nic robić, aby odnieść sukces. Oto jak niebezpieczne mogą być nieznajomość lub lekceważenie protokołów zabezpieczeń. Coraz większym zagrożeniem są pracownicy, którzy przynoszą do pracy prywatne urządzenia lub korzystają z komercyjnego oprogramowania w chmurze. W obu przypadkach wprowadzają oni do dobrze zabezpieczonej sieci niezabezpieczone elementy bez wiedzy pracowników IT, tworząc w ten sposób ukrytą lukę w zabezpieczeniach.

W większości przypadków hakerzy nie potrzebują zaawansowanych algorytmów czy najnowocześniejszych technologii. Wystarczy im, że ktoś z nas jest trochę nieostrożny.

Zapory zostały pokonane

Do niedawna podstawą cyberbezpieczeństwa były programy antywirusowe i zapory. Zapobieganie i ochrona. Tworzenie obwodu zabezpieczeń. Obecnie w miejscu pracy po prostu nie da się wdrożyć wiarygodnej strategii.

81% respondentów Ponemon twierdzi, że urządzenia przenośne w ich sieciach były celem oprogramowania typu malware. Inne rosnące zagrożenia bezpieczeństwa to między innymi korzystanie przez pracowników z komercyjnych aplikacji w chmurze – wskazało na to 72% respondentów – BYOD (69%) i pracownicy pracujący w biurach domowych i innych miejscach (62%).[15]

Po prostu zapora miała sens wówczas, gdy administrator sieci mógł kontrolować, jakie urządzenia są do niej podłączane. W czasach, gdy pracownicy przynoszą do pracy swoje urządzenia – często nawet kilka – i nie informują o tym pracowników IT, a coraz większa liczba pracowników pracuje zdalnie, zwyczajnie nie da się chronić obwodu. Każde niezweryfikowane urządzenie jest wrażliwym punktem końcowym, który może zostać wykorzystany przez hakerów.

[13] https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach

[14] https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0

[15] Ponemon 2016 State of the Endpoint Report

Perspektywa HP: wyjście poza bezpieczeństwo sieci

Michael Howard, menedżer zajmujący się w firmie HP praktykami bezpieczeństwa w skali światowej

Obecnie kluczowym problemem jest to, że przedsiębiorstwa starają się zabezpieczyć każdy punkt końcowy z powodu braku wiedzy i świadomości na temat niektórych urządzeń i ryzyka, jakie ponoszą. Czują się bezpiecznie za zaporą, mimo że nie jest ona wystarczającą ochroną przed atakiem. Zespoły zajmujące się bezpieczeństwem muszą znać każdy punkt końcowy w infrastrukturze i mieć pewność, że ma on kilka warstw zabezpieczeń chroniących go przed coraz bardziej wyrafinowanymi atakami.

Bardzo istotne jest sprawdzanie wszystkich elementów infrastruktury IT sieci korporacyjnej i utworzenie dodatkowej warstwy ponad standardowymi parametrami sieci. Same zapory nie mogą powstrzymać złożonych ataków, a polityka obrony z wieloma warstwami zabezpieczeń w każdym punkcie końcowym jest konieczna, jeśli firma chce spełnić wymogi prawne i uniknąć kosztownych kar.

Firma HP z każdym nowym rozwiązaniem, usługą lub produktem udowadnia, że bezpieczeństwo jest dla nas najważniejsze. Zespoły badawczo-rozwojowe wiedzą, że muszą reagować na kwestie związane z bezpieczeństwem i umieć je wdrożyć w życie w bezpieczny sposób.

Bardziej niż dotychczas bezpieczeństwo powinno być newralgicznym elementem, a nie „piątym kołem u wozu". Taka jest od lat polityka firmy HP.

Zabezpieczenia warstwowe

Nowe podejście do cyberbezpieczeństwa musi być wielowarstwowe.
Zabezpieczenia w sieci są nadal ważne, ale powinny polegać na dzieleniu sieci na części. Wiele naruszeń wykorzystuje fakt, że wystarczy raz dostać się do sieci, aby mieć dostęp do całego systemu. Pomyśl o błędnej ocenie próby wyłudzenia informacji przez Johna Podestę. Najważniejsze jest wyodrębnienie poufnych informacji i ukrycie ich za kilkoma warstwami zabezpieczeń, tak aby kradzież jednego klucza nie otwierała całej twierdzy.

Urządzenia muszą być ewidencjonowane. Kluczowym wyzwaniem dla menedżerów IT jest zapewnienie, aby każde urządzenie podłączone do sieci było chronione regularnie aktualizowanym oprogramowaniem zabezpieczającym przed wirusami, szkodliwym oprogramowaniem typu malware i spyware oraz regularnie skanowane pod kątem anomalii. Lepiej używać urządzeń jako czujników gromadzących informacje w czasie rzeczywistym i ostrzegających przed naruszeniami sieci, której są częścią.

Rozbudowanymi zabezpieczeniami należy zarządzać w miejscu, w którym pracują osoby przeszkolone w zakresie protokołów cyberbezpieczeństwa. Błąd ludzki – od kliknięcia nieodpowiedniego łącza do połączenia się z urządzeniem klienta – to główne zagrożenie dla sieci. Błędy ludzkie można zredukować dzięki szkoleniom.

Zabezpieczanie urządzeń

Być może największym problemem charakterystycznym dla współczesnego cyberbezpieczeństwa jest kontrola urządzeń, które mają dostęp do sieci.
Prostym, często stosowanym rozwiązaniem są oddzielne sieci Wi-Fi dla gości i pracowników, dzięki czemu niezabezpieczone urządzenia zewnętrzne nie mają dostępu do sieci głównej. Powinno ono iść w parze ze szkoleniem pracowników w zakresie korzystania z własnych urządzeń na potrzeby uzyskiwania dostępu do sieci.

Kolejną sprawą jest zapewnienie kontroli nad urządzeniami pracowników. Powinna się ona opierać na obowiązujących w firmie zasadach dotyczących BYOD lub CYOD – ze wskazaniem na CYOD, która daje większą kontrolę nad używanymi urządzeniami, wybieranie tych lepiej zabezpieczonych, sprawdzanie ich konfiguracji, a także zarządzanie nimi i ich monitorowanie.

Na przykład jeden z naszych komputerów klasy HP Elite będzie lepszym rozwiązaniem niż tani laptop. Wszystkie komputery klasy HP Elite mają wbudowaną technologię HP SureStart, która co 15 minut sprawdza system BIOS i po wykryciu anomalii resetuje komputer do oryginalnego stanu, blokując w ten sposób niepożądanych intruzów. Dzięki tej funkcji – i wielu innym – komputery z naszej serii HP Elite 800 zostały ostatnio uznane za „najbezpieczniejsze komputery osobiste na świecie".[16] Jednak jest mało prawdopodobne, że pracownicy kupią je sobie sami.

Pracownicy zwykle wolą używać własnych urządzeń z dwóch powodów:
1. Są bardziej zaawansowane technologicznie niż te dostępne w pracy
2. Pracownicy lubią używać technologii, które znają.

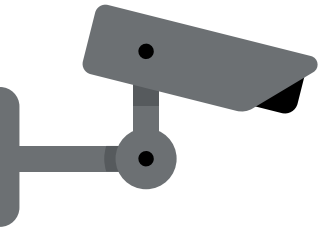
Jeśli w ramach CYOD pracownicy otrzymają nowoczesne urządzenia, które będą regularnie uaktualniane, organizacje będą w stanie zapewnić pracownikom sprzęt lepszy niż ich prywatny i zagwarantować lepszą kontrolę urządzeń. Oto dlaczego oferujemy nasze urządzenia HP w modelu sprzedaży Device as a Service (DaaS).

Bardzo ważne jest objęcie strategią bezpieczeństwa wszystkich urządzeń, nawet tych, o których często zapominamy. W badaniu IDC 80% respondentów stwierdziło, że bezpieczeństwo IT jest ważne w ich firmach, ale tylko 59% uważało, że zabezpieczenie drukarki jest ważne, chociaż ponad połowa z nich w ciągu ostatnich 12 miesięcy była ofiarami naruszeń związanych z bezpieczeństwem druku. To oczywisty paradoks.

Średnia liczba naruszeń zabezpieczeń przed wprowadzeniem zasad bezpieczeństwa drukowania wynosiła 9,9 rocznie, a związane z tym koszty wyniosły 521 400 USD (w tym grzywny). Po wdrożeniu zasad bezpieczeństwa druku średnia liczba naruszeń spadła do 1,5, co przyniosło oszczędności rzędu 200 godzin czasu pracy rocznie i 250 000 USD związanych z kosztami, w tym audytu i zgodności.[17]

[16] http://www8.hp.com/us/en/campaign/computersecurity/

[17] IDC The Business Value of Printer Security 2015



Proaktywne wykrywanie i reagowanie

Według badań prowadzonych przez PAC 77% specjalistów zabezpieczeń IT zajmuje się prewencją i ochroną, na przykład oprogramowaniem antywirusowym. Lecz takie podejście jest nieefektywne. Badania pokazały również, że w ciągu ostatnich 12 miesięcy 67% firm padło ofiarą cybernaruszeń, a 100% – w przeszłości.[18]

Zwłaszcza oprogramowanie antywirusowe jest szokująco nieefektywne. Firma Damballa przeprowadziła testy, w których celowo zaatakowano sieć w celu pomiaru reakcji antywirusowej. Znalezienie wszystkich złośliwych plików zajęło ponad 6 miesięcy.[19] Porównajmy to z innym badaniem PAC, w którym firmy stwierdziły, że wykrycie ataku zajmowało im od 1 do 6 miesięcy.

Zapewnienie bezpieczeństwa punktów kontrolnych nie może już opierać się na prewencji. Rosnąca liczba przypadków wykrywania wirusów/oprogramowania typu malware w połączeniu z nieodłącznym brakiem zabezpieczeń BYOD/pracy mobilnej oznacza, że naruszenia są nieuchronne. Nikt nie sugeruje, że należy całkowicie zrezygnować z zapobiegania i ochrony, ale wyraźnie widać, że wykrywanie i reagowanie powinny zajmować znacznie wyższą pozycję.

Konieczne jest ciągłe monitorowanie w czasie rzeczywistym, najlepiej z wykorzystaniem punktów końcowych jako czujników ostrzegających resztę sieci po wykryciu naruszenia. Umożliwia to specjalistom IT ds. zabezpieczeń zdalne reagowanie i inicjowanie takich procesów, jak:

- Zdalne wyłączenie urządzenia
- Wyeliminowanie zainfekowanego procesu lub rozprzestrzeniającego się oprogramowania typu malware
- Poddawanie kwarantannie konkretnego pliku lub grupy plików
- Przerywanie komunikacji sieciowej w celu odizolowania zainfekowanych urządzeń[20]

Zaakceptowanie faktu, że naruszenia mogą się zdarzać i ustanowienie odpowiednich protokołów reagowania, a także wdrożenie technologii niezbędnych do ich realizacji jest jedynym sposobem zapewnienia bezpieczeństwa w sieci, gdy nie można już ograniczyć się do zapobiegania.

„Żadna technologia nie zapewni bezpieczeństwa, jeśli ludzie nie będą wystarczająco zdeterminowani”

– Joseph Steinberg [21]

Bezpieczeństwo pracowników

Równie ważne, jeśli nie ważniejsze niż zabezpieczenie samego urządzenia, jest zapewnienie bezpieczeństwa osobie korzystającej z niego.
Każdy pracownik powinien przejść szkolenie z zakresu cyberbezpieczeństwa. Wszyscy muszą zdawać sobie sprawę z ryzyka wyłudzania informacji. Na przykład podczas przeglądania wątpliwych stron czy pobierania podejrzanych załączników. Pracownicy muszą znać zasady dotyczące tworzenia bezpiecznych haseł – używania silnych, unikalnych haseł podczas każdego wrażliwego logowania oraz używania odpowiedniego menedżera haseł do ich przechowywania.

Pracownicy powinni mieć świadomość, jak duże znaczenie ma regularne aktualizowanie oprogramowania zabezpieczającego w urządzeniu, aby zmniejszyć obciążenie monitorowania IT. Powinni być ostrożni i korzystać wyłącznie z zabezpieczonych urządzeń, aby uzyskać dostęp do sieci organizacji, a także unikać używania osobistych urządzeń w niezabezpieczonych sieciach zewnętrznych w celu uzyskania dostępu do poufnych danych.

Wielu wybitnych specjalistów zajmujących się bezpieczeństwem cyberprzestrzeni zaleca przeprowadzanie symulowanych ataków mających na celu wyłudzanie tożsamości – tworzenie fałszywych stron i sprawdzanie, jak reagują pracownicy – tak aby szkolenie w zakresie bezpieczeństwa cyfrowego było tylko formalnością. Ponieważ większość ataków polega na wykorzystaniu ludzkiej słabości, czy to przez zaniedbanie, czy złośliwość.

Najsłabszymi ogniwami każdej sieci są ludzie.

[18] PAC Incident Response Management 2015
[19] https://www.damballa.com/time-to-fix-malware-strategies-2/
[20] The Essential Endpoint Detection Checklist – HP Now
[21] https://digitalguardian.com/blog/data-security-experts-answer-what-biggest-misconception-companies-have-about-endpoint-security

Wnioski

Wydatki na zabezpieczenia IT powinny zostać przesunięte z prewencji i ochrony na wykrywanie i reagowanie w punktach końcowych
Ochrona danych organizacji w obecnej atmosferze wokół IT w obliczu rosnącego zagrożenia przestępczością cybernetyczną i utratą kontroli nad obwodem sieci wymaga dwóch rzeczy: zmiany koncepcji i większych zasobów.

Zmierzamy w kierunku zmiany koncepcji sieci. Idea sieci jako ogrodzenia wokół zbioru urządzeń nie ma już zastosowania. Nadszedł czas, aby przyjrzeć się rzeczywistości. „Sieć" to chimera. Wyłania się z podłączonych urządzeń – z każdego punktu końcowego. Zabezpieczenie sieci oznacza zabezpieczenie punktów końcowych. Każdy punkt końcowy składa się z dwóch elementów: urządzenia i człowieka, który je obsługuje. Należy uwzględnić je oba.

Jednak zapewnienie bezpieczeństwa w tym nowym paradygmacie jest znacznie bardziej skomplikowane niż dawne proste środowisko komputerów stacjonarnych połączonych przez Ethernet. Wymaga większych zasobów i ciągłej obsługi. Zauważyło to 61% respondentów Ponemon.

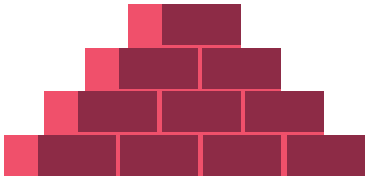
Ale jak przekonać pozostałe organizacje? Tylko 36% respondentów uważa, że mają wystarczający budżet i odpowiedni personel, aby zapewnić bezpieczeństwo punktów końcowych. 69% twierdzi, że działy IT nie są w stanie zapewnić pracownikom potrzebnej pomocy. 71% stwierdziło, że zasady zabezpieczenia punktów końcowych są trudne do wyegzekwowania.[22]

80% menedżerów ds. bezpieczeństwa IT stwierdza, że najlepszym sposobem na zdobycie funduszy na nowe programy zabezpieczeń jest konieczność zapewnienia zgodności z regulacjami prawnymi, a jednocześnie uważa, że jest to najmniej istotny powód zwiększenia budżetów. Zgodność oznacza spełnienie pewnego minimum.[23]

Osoby podejmujące decyzje dotyczące IT powinny poprosić o wsparcie zarząd, aby podkreślić znaczenie bezpieczeństwa. Jasne jest, że koszty związane z bezpieczeństwem są niewielkie w porównaniu z kosztami przywracania do poprzedniego stanu, utraconymi dochodami, spadkiem wartości akcji – na dłuższą metę to spore oszczędności. Wiele rozwiązań związanych z bezpieczeństwem pozytywnie wpływa również na inne obszary. Pomyśl o zwiększonej efektywności wdrażania zabezpieczeń druku i wydajności związanej z zapewnieniem regularnie odświeżanych technologii w elastycznym programie CYOD udostępnianym przez firmę zewnętrzną w ramach subskrypcji (np. HP DaaS). Popatrzmy, jak to działa.

Wyzwanie jest ogromne. Z czasem – wraz z gwałtownie rosnącą liczbą urządzeń w Internecie rzeczy (IoT) oraz rosnącym wyrafinowaniem cyberprzestępczości – stanie się to bardziej zniechęcające. Ale jest to wykonalne. Dzięki odpowiedniej technologii, trafnej strategii i właściwym zasobom możemy chronić nasze punkty końcowe. Możemy zapewnić bezpieczeństwo naszych danych.

Więcej informacji o HP Device as a Service i o tym, jak możemy pomóc Ci wdrożyć rozbudowany, elastyczny i bezpieczny program CYOD znajdziesz **tutaj.**



Zapisz się, aby otrzymywać bieżące informacje
hp.com/go/getupdated

Podziel się informacjami ze znajomymi

Oceń ten dokument

4AA7-1089PLE

[22] Ponemon 2016 State of the Endpoint Report

[23] https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697