SPECJALNY RAPORT POŚWIĘCONY CYBERBEZPIECZEŃSTWU

MAŁE I ŚREDNIE FIRMY

Małe, lecz potężne

Jak małe i średnie firmy mogą wzmocnić swoją obronę przed zagrożeniami dla bezpieczeństwa?

CISCO

53% firm średniej wielkości doświadczyło naruszenia bezpieczeństwa w jakiejś postaci

nawet

5000

Średnia liczba alertów dotyczących bezpieczeństwa

Firmy średniej wielkości badają 55,6% alertów dotyczących bezpieczeństwa

29% firm średniej wielkości twierdzi, że naruszenia kosztują je mniej niż 100 tys. USD. 20% mówi, że koszt naruszeń mieści się w zakresie 1 000 000–2 499 999 USD

Wiele małych i średnich firm chce stosować efektywniejsze praktyki w dziedzinie cyberbezpieczeństwa na wzór dużych przedsiębiorstw. Średnie i małe firmy są dynamiczne — stanowią fundament innowacyjności i modelowy przykład ciężkiej pracy. Działają szybciej i pracują jeszcze ciężej od dużych przedsiębiorstw, są jednak narażone na takie same cyberzagrożenia.

W obecnym krajobrazie cyberzagrożeń każda organizacja jest narażona na atak. Małe i średnie firmy padają coraz częściej ofiarą takich ataków[1], często pełniąc funkcję platformy wyjściowej lub kanału umożliwiającego uruchomienie większych kampanii. Cyberprzestępcy postrzegają małe i średnie firmy jako łatwe cele, dysponujące mniej zaawansowaną infrastrukturą zabezpieczeń i praktyk dotyczących bezpieczeństwa oraz niewystarczającą liczbą odpowiednio wyszkolonych pracowników, aby być w stanie kontrolować zagrożenia i reagować na nie.[1]

Wiele małych i średnich firm zaczyna uświadamiać sobie swoją atrakcyjność w oczach cyberprzestępców. Bywa, że ta świadomość przychodzi zbyt późno: na skutek ataku. Dla takich firm przywracanie działalności po cyberataku może być trudne i kosztowne — czasami wręcz niemożliwe — w zależności od natury i zasięgu kampanii. Niniejszy raport ułatwi zrozumienie zagrożeń dla mniejszych organizacji, objaśni, jak wyglądają kwestie zabezpieczeń w mniejszych organizacjach w porównaniu z podobnymi przedsiębiorstwami oraz przedstawi kilka wskazówek zarówno na 2018 rok, jak i na przyszłość.

Warto zwrócić uwagę na jedno z ustaleń badania porównawczego przeprowadzonego przez Cisco i dotyczącego możliwości ochrony na 2018 r.: ponad połowa (54%) wszystkich cyberataków skutkuje stratami finansowymi o wartości przekraczającej 500 000 USD, wynikającymi między innymi z utraty zysków, klientów i możliwości biznesowych oraz z poniesionych kosztów. Ta kwota wystarczy, aby trwale zmieść z rynku nieprzygotowaną małą lub średnią firmę.

Wyniki badania przeprowadzonego niedawno przez firmę Better Business Bureau (BBB)[2] podkreślają finansowe problemy, z którymi zmagają się małe i średnie firmy wskutek poważnego cyberataku. Firma BBB zapytała właścicieli małych firm w Ameryce Północnej, jak długo ich firmy mogą przynosić zyski w przypadku utraty dostępu do kluczowych danych. Zaledwie jedna trzecia respondentów (35%) odpowiedziała, że ich firmy mogą w takiej sytuacji zachować rentowność przez ponad trzy miesiące. Ponad połowa odpowiedziała, że firma zaczęłaby przynosić straty w niecały miesiąc.

Za małe firmy uważamy podmioty zatrudniające mniej niż 250 pracowników, zaś średnie firmy definiujemy jako podmioty zatrudniające od 250 do 499 pracowników. Oba segmenty zostały uwzględnione w tym raporcie.

W badaniu porównawczym Cisco dotyczącym możliwości obrony w 2018 r. analizujemy ustalenia dokonane w małych i średnich firmach, które wzięły udział w tym badaniu porównawczym. Raport zawiera analizy obecnie stosowanych praktyk dotyczących zabezpieczeń oraz porównuje pełne wyniki z ostatnich trzech lat.

Nasze dane dotyczące małych i średnich firm zostały zgromadzone od 1816 respondentów z 26 krajów.

1 „Cyberthreats and Solutions for Small and Midsize Businesses", Vistage Research Center, 2018 r. Raport opracowany we współpracy z firmą Cisco i organizacją National Center for the Middle Market Dostępny pod adresem: https://www.vistage.com/research-center/business-operations/risk-management/20180503-22912/.

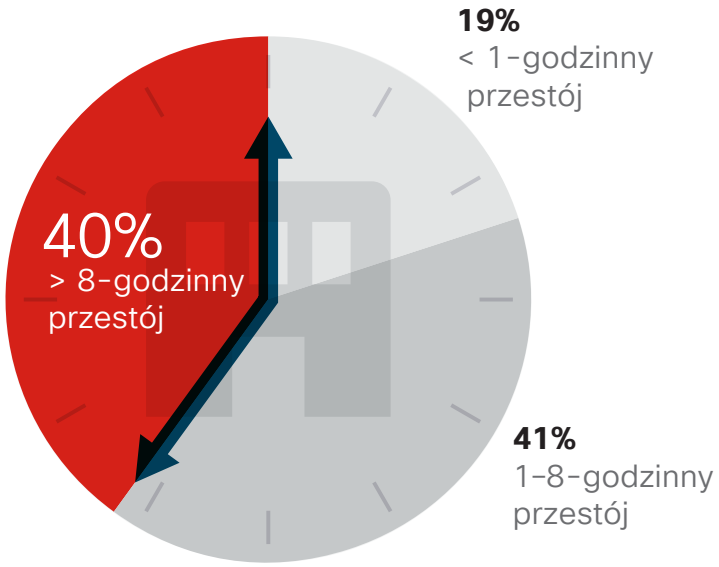
2 „2017 State of Cybersecurity Among Small Businesses in North America, BBB, 2017": https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf.

Cóż to jest, jeden dzień przestoju? Nic.

Jak świat światem, nikt nigdy nie słyszał podobnych słów z ust żadnego administratora infrastruktury IT. Awarie systemu, zmniejszające produktywność i zyskowność firmy, są jedną z dotkliwych konsekwencji cyberataku. Z badania porównawczego wynika, że w ubiegłym roku 40% respondentów (spośród firm zatrudniających 250–499 pracowników) doświadczyło co najmniej 8-godzinnego przestoju systemu na skutek poważnego naruszenia bezpieczeństwa (ilustracja 1). Firma Cisco zaobserwowała podobne wyniki w odniesieniu do większych organizacji uczestniczących w badaniu (zatrudniających 500 lub więcej pracowników). Różnica polega na tym, że większe organizacje są z reguły bardziej odporne na skutki cyberataku niż małe i średnie firmy, ponieważ dysponują większymi zasobami pozwalającymi im lepiej reagować na atak i skuteczniej przywracać działalność po awarii.

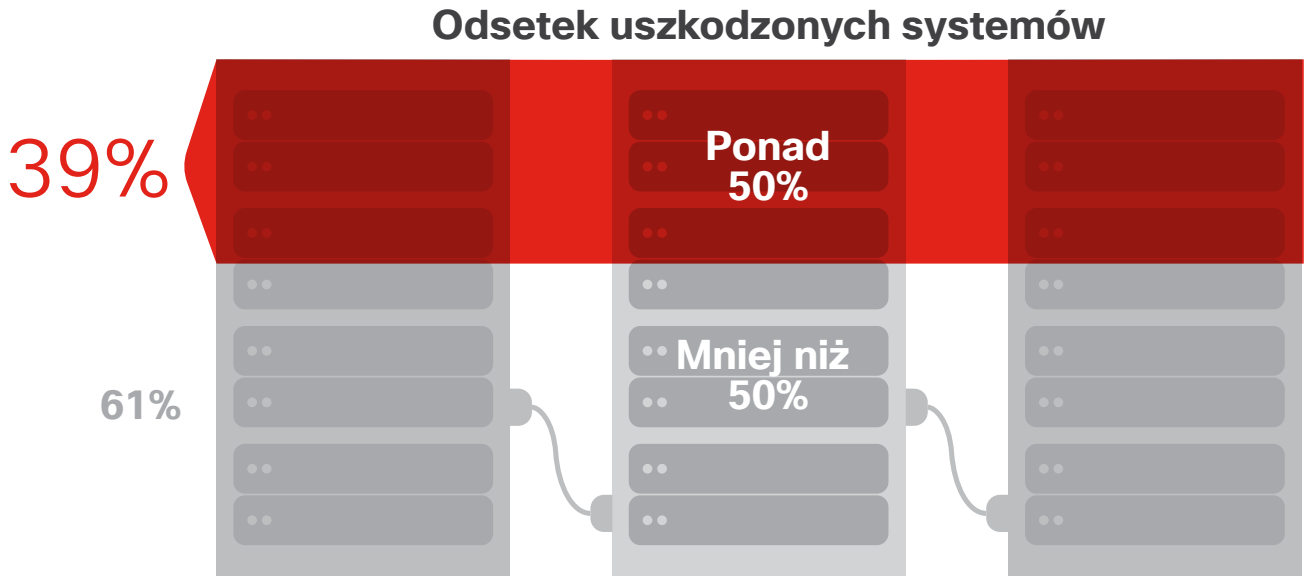
Ponadto 39% respondentów zgłosiło, że przynajmniej połowa ich systemów została uszkodzona na skutek poważnego naruszenia zabezpieczeń (ilustracja 2). Mniejsze firmy nie mają z reguły oddziałów w różnych lokalizacjach ani segmentów biznesowych, w związku z czym ich główne systemy są zazwyczaj ściślej połączone. Kiedy stają się obiektem ataku, zagrożenie może się szybko i łatwo rozprzestrzenić z sieci na inne systemy.

Ilustracja 1 Przestój systemu po poważnym naruszeniu zabezpieczeń



Źródło: Porównawcze opracowanie Cisco na temat możliwości ochrony, 2018

Ilustracja 2 Odsetek systemów dotkniętych poważnym naruszeniem zabezpieczeń



Źródło: Porównawcze opracowanie Cisco na temat możliwości ochrony, 2018

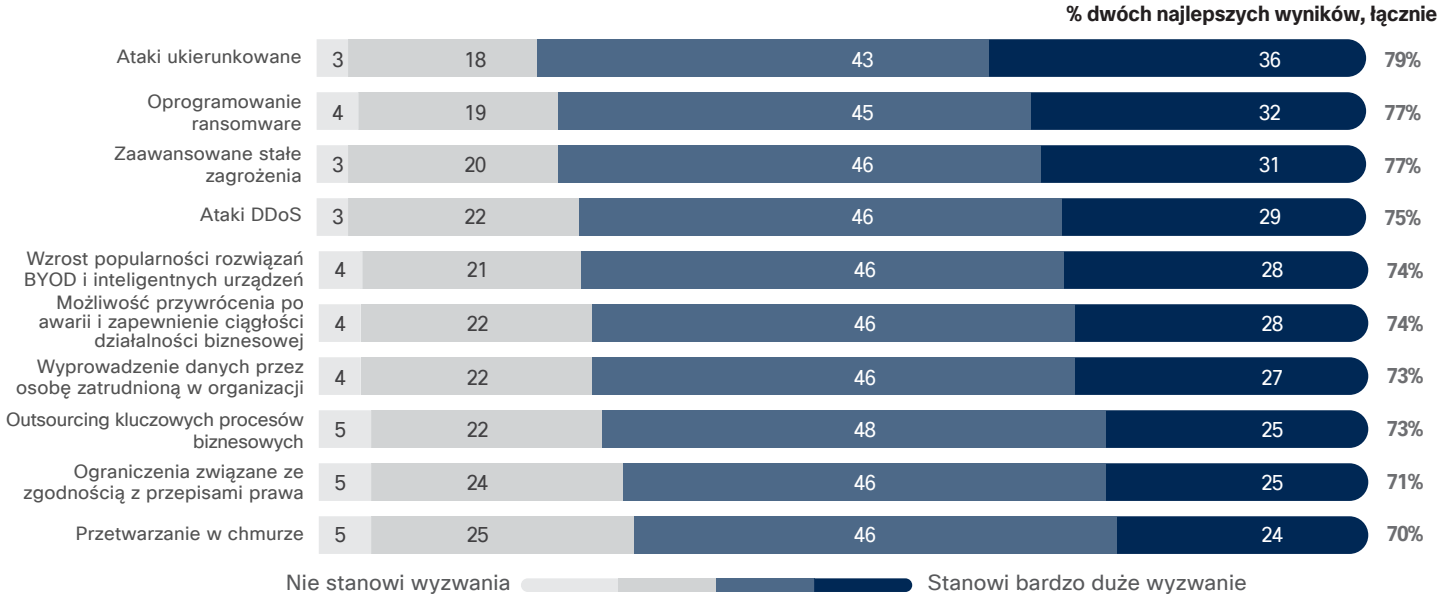
Bezsenne noce administratorów zabezpieczeń

Zapytani o największe wyzwania dotyczące bezpieczeństwa respondenci wymieniali przede wszystkim trzy kwestie:

- ataki ukierunkowane na pracowników (przemyślane próby wyłudzenia informacji),
- zaawansowane stałe zagrożenia (zaawansowane złośliwe oprogramowanie najnowszej generacji),
- oprogramowanie ransomware.

Oprogramowanie ransomware (co ciekawe, niewymieniane w „wielkiej trójce" największych zagrożeń dla dużych przedsiębiorstw) to inaczej – jak z pewnością wiesz – złośliwe oprogramowanie szyfrujące dane, które zostają odblokowane dopiero po zapłaceniu przez użytkownika żądanego okupu. Ataki przy użyciu tego oprogramowania mogą powodować poważne zakłócenie działania systemu i jego awarie w małych i średnich firmach. Oprogramowanie ransomware również generuje koszty innego rodzaju dla takich firm: eksperci Cisco ds. zabezpieczeń są zdania, że małe i średnie firmy są bardziej skłonne do płacenia takich okupów cyberprzestępcom, aby móc szybko wznowić normalną działalność operacyjną, ponieważ nie mogą sobie pozwolić na przestoje i brak dostępu do kluczowych danych, w tym danych klientów (patrz ilustracja 3).

Ilustracja 3 Najważniejsze zagrożenia dla bezpieczeństwa w firmach średniej wielkości[5]



Źródło: Porównawcze opracowanie Cisco na temat możliwości ochrony, 2018

Inne zagrożenia, których nie mogą ignorować małe i średnie firmy

Mimo obaw dotyczących oprogramowania ransomware eksperci Cisco ds. zabezpieczeń sugerują, że w przypadku tego zagrożenia można zaobserwować tendencję spadkową, ponieważ cyberprzestępcy przenoszą obecnie swoją uwagę na nielegalne wydobywanie kryptowalut („kryptokopanie"). Atrakcyjność tego procederu ma trzy wymiary: może być bardzo lukratywny, nie można namierzyć wypłat i cyberprzestępcy nie muszą się obawiać sankcji karnych za swoje działania. (Nie ma na przykład ryzyka, że pacjenci zostaną pozbawieni opieki lekarskiej istotnej dla ich zdrowia, ponieważ system i kluczowe dane szpitala zostaną zablokowane przez oprogramowanie ransomware). Cyberprzestępcy także mogą dostarczać oprogramowania do wydobywania kryptowalut („miner") przy użyciu różnych metod, w tym kampanii w postaci rozsyłania niechcianych wiadomości e-mail oraz zestawów do wykorzystywania luk w oprogramowaniu.[3]

3 Jaki okup? Przejęcie dokonane przez cyberprzestępców zajmujących się wydobywaniem kryptowalut generuje straty liczone w milionach" blog Cisco Talos, 1 stycznia[3] 2018 r.: https://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html.

Eksperci Cisco zajmujący się badaniem zagrożeń wyjaśniają, że cyberprzestępcy stosujący nowy model biznesowy polegający na nielegalnym kryptokopaniu „nie karzą już ofiar za otworzenie załącznika lub uruchomienie złośliwego skryptu, biorąc zakładnika w postaci systemu i domagając się okupu. Teraz aktywnie wykorzystują zasoby zainfekowanego systemu”.[4] Dla małych i średnich firm będących nieświadomymi pomocnikami w nielegalnym procederze kryptokopania wolniejsza praca systemu może być jedynym sygnałem ostrzegawczym informującym o włamaniu, jeśli nie dysponują odpowiednią technologią pozwalającą wykryć działanie programu do kryptokopania.

0,5% zagrożeń wewnętrznych: o 100% za dużo

W miarę przenoszenia przez firmy naszych respondentów danych i procesów do chmury, muszą one podejmować również odpowiednie działania umożliwiające kontrolowanie innego potencjalnego zagrożenia: ze strony niesubordynowanych pracowników. Bez narzędzi do wykrywania podejrzanych działań (np. pobierania wrażliwych danych klientów) firmy są narażone na ryzyko utraty swojej własności intelektualnej, wrażliwych danych finansowych lub danych klientów za pośrednictwem firmowych systemów w chmurze.

Wyniki najnowszego badania przeprowadzonego przez ekspertów Cisco ds cyberzagrożeń podkreślają to ryzyko: od stycznia do czerwca 2017 r. zajmowali się badaniem trendów kopiowania i ekstrahowania danych przy użyciu uczenia maszynowego, aby utworzyć profile 150 000 użytkowników z 34 krajów, korzystających z chmury. Przez 1,5 miesiąca odkryli, że 0,5 procent użytkowników dokonywało podejrzanych pobrań plików. Czy pół procenta to dużo? Inaczej mówiąc, oznacza to, że w firmie zatrudniającej 400 osób dwóch pracowników stanowi zagrożenie wewnętrzne. To o 100% za dużo. Owi użytkownicy pobrali łącznie ponad 3,9 milionów dokumentów z firmowych systemów w chmurze. To średnio 5200 dokumentów na użytkownika w czasie 1,5 miesiąca.[5]

Porównawcze opracowanie Cisco na temat możliwości ochrony, 2018

Ten specjalny raport zawiera wyselekcjonowane dane z porównawczego opracowania Cisco na temat możliwości ochrony na 2018 r. W badaniu wzięło ponad 3600 respondentów z 26 krajów. Aby uzyskać więcej analiz dotyczących praktyk w zakresie zabezpieczeń stosowanych obecnie przez organizacje, niezależnie od ich wielkości, oraz porównanie wyników z poprzednich badań przeprowadzonych przez Cisco, pobierz *doroczny raport Cisco na temat cyberbezpieczeństwa na 2018 r.* dostępny pod adresem: https://www.cisco.com/c/en/us/products/security/security-reports.html.

4 Tamże.

5 Więcej szczegółów można znaleźć w dorocznym raporcie Cisco na temat cyberbezpieczeństwa na 2018 r., „Insider threats: taking advantage of the cloud”, dostępnym pod adresem: https://www.cisco.com/c/en/us/products/security/security-reports.html.

Wyzwania

Opisane wcześniej najlepsze metody obrony przed zagrożeniami wymagają koordynacji i zsynchronizowania zasobów IT. Te zasoby to najczęściej personel, procesy i technologie gromadzone przez firmy, aby bronić się przed atakami.

Dla mniejszych firm jeszcze większym wyzwaniem jest jednak skoordynowanie tych zasobów w sposób zapewniający wgląd w zagrożenia i umożliwiający powstrzymanie ataku lub zniwelowanie jego skutków zanim jeszcze zdąży wyrządzić szkody. Uporczywy niedostatek specjalistów ds. zabezpieczeń trapiący duże przedsiębiorstwa jest jeszcze bardziej dotkliwy w przypadku mniejszych firm.

Trendy technologicznie w dziedzinie zabezpieczeń w małych i średnich firmach

W miarę rozwoju mniejsze organizacje usiłują stawić czoła wyzwaniom dotyczącym cyberbezpieczeństwa, sięgając po nowe narzędzia, by powstrzymać zagrożenia.

Respondenci w badaniu porównawczym przyznali, że gdyby pozwalały im na to zasoby personelu, z większym prawdopodobieństwem sięgaliby po następujące rozwiązania:

- Zastąpienie istniejących zabezpieczeń urządzeń końcowych bardziej wyrafinowanymi i zaawansowanymi rozwiązaniami zapewniającymi ochronę przed złośliwym oprogramowaniem / technologią EDR – najczęstsza odpowiedź, wybrana przez 19%.
- Zastanowienie się nad wdrożeniem lepszych zabezpieczeń aplikacji internetowych, chroniących przed atakami w sieci WWW (18%).
- Wdrożenie rozwiązań zapobiegających dostępowi nieupoważnionych użytkowników, postrzeganych wciąż jako istotna technologia pozwalająca zapobiegać atakom w sieci i próbom wykorzystania luk zabezpieczeń (17%). (Patrz ilustracja 5).

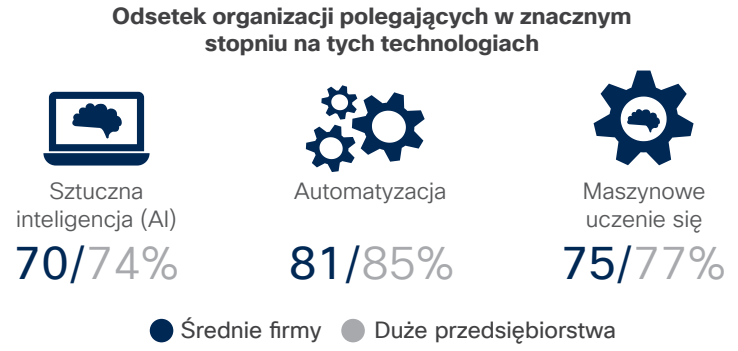
Podczas gdy organizacje zastanawiają się nad stosowaniem nowych technologii, pojawia się pytanie, na ile dobrze te rozwiązania będą współpracować, aby zapewnić ochronę na wymaganym poziomie. Nie należy też nie doceniać obciążeń związanych z zarządzaniem wynikających z konieczności sprawdzania wielu konsol w celu zareagowania na zagrożenia lub zdarzenia dotyczące bezpieczeństwa.

„Wiele osób uważa, że najskuteczniejszą ochronę zapewni im sięgnięcie po prostu po najlepsze w klasie zabezpieczenia dostarczane przez różnych producentów", mówi Ben M. Johnson, CEO firmy Liberty Technology z Griffin w stanie Georgia, Partnera Cisco. „Zauważyliśmy jednak, że takie podejście skutkuje wzrostem obciążeń związanych z zarządzaniem oraz kosztów, a także obniżeniem ogólnej skuteczności zabezpieczeń".

Uczenie maszynowe: efektywne czy tylko efektowne?

Wszyscy słyszeliśmy o bardzo obecnie popularnym uczeniu maszynowym. Okazuje się, że średnie firmy w mniej więcej takim samym stopniu co duże przedsiębiorstwa polegają na rozwiązaniach analiz zachowań do efektywnego wykrywania cyberataków. Rozwiązania wykorzystujące uczenie maszynowe i automatyzację są nieco mniej rozpowszechnione w średnich firmach w porównaniu z dużymi organizacjami zatrudniającymi ponad 1000 pracowników (ilustracja 4).

Ilustracja 4 Firmy średniej wielkości w mniejszym stopniu polegają na automatyzacji i narzędziach wykorzystujących AI



Źródło: Porównawcze opracowanie Cisco na temat możliwości ochrony, 2018

Uczenie maszynowe jest najbardziej efektywne, gdy stanowi dodatkową warstwę wykrywającą w już wdrożonym produkcie, w przeciwieństwie do zakupu oddzielnego produktu, aby „stosować uczenie maszynowe". W ten sposób zespoły mogą wykorzystywać zalety uczenia maszynowego, aby wykrywać anomalie i zagrożenia z maszynową prędkością, bez dodatkowych obciążeń.

Średnie firmy i mobilność

Firmy zdają sobie także sprawę, że ich koncepcje zabezpieczeń muszą spełniać wymogi nowoczesnego środowiska pracy, w szczególności wymogi mobilności i powszechnego stosowania urządzeń przenośnych. 56% respondentów przyznało, że ochrona urządzeń przenośnych przed cyberatakami stanowi bardzo duże lub ekstremalnie duże wyzwanie.

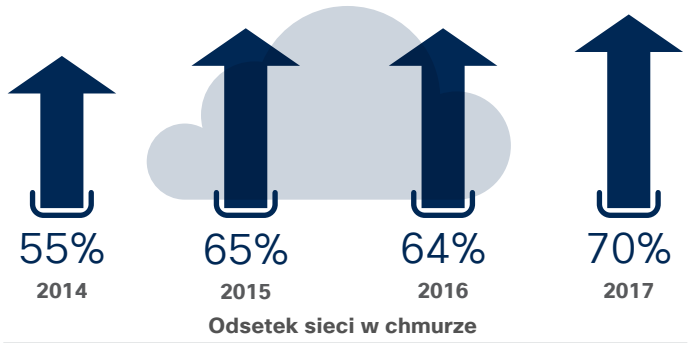
Średnie firmy i chmura

W związku ze świadomością wyzwań dotyczących zabezpieczeń wielu respondentów wyraża nadzieję, że technologia chmury pomoże im wzmocnić linię obrony bez konieczności zatrudniania dodatkowych pracowników lub zwiększania obciążeń istniejących zasobów. Pytanie brzmi: czy przeniesienie zabezpieczeń do chmury jest wystarczająco skuteczną strategią odpierania cyberataków? Firmy nie mogą tak po prostu pozbyć się odpowiedzialności za zapewnianie bezpieczeństwa przez przeniesienie danych do chmury. Muszą w dalszym ciągu dysponować wiedzą na temat mechanizmów kontroli bezpieczeństwa stosowanych przez dostawców rozwiązań w chmurze oraz tego, jak potencjalne cyberataki na chmurę mogą wpływać na zasoby w ich siedzibach.

Obecnie obserwujemy wyraźny trend wzrostowy wdrażania usług w chmurze przez przedsiębiorstwa, widoczny w badaniach prowadzonych przez Cisco. W 2014 r. 55% tych firm informowało, że część ich sieci jest obsługiwana w chmurze w jakiejś postaci; w 2017 r. ten odsetek wzrósł do 70% (ilustracja 5).

Wielu respondentów uważa, że chmura może pomóc w uszczelnieniu niektórych luk w ich zabezpieczeniach, jak również rozwiązać kwestie niektórych niedostatków infrastruktury oraz możliwości i kwalifikacji pracowników. Według badań prowadzonych przez Cisco najczęstszą przyczyną przenoszenia przez średnie firmy obsługi sieci do chmury jest przekonanie, że chmura zapewnia większe bezpieczeństwo danych (68%). Drugą pod względem popularności przyczyną był brak dostatecznej liczby pracowników wewnętrznego działu IT (49%) (patrz ilustracja 6).

Ilustracja 5 W firmach średniej wielkości można zaobserwować stały wzrost wdrożeń w chmurze



Źródło: Porównawcze opracowanie Cisco na temat możliwości ochrony, 2018

Ilustracja 6 Firmy średniej wielkości wybierają rozwiązania w chmurze ze względu na ich bezpieczeństwo i efektywność

Źródło: Porównawcze opracowanie Cisco na temat możliwości ochrony, 2018

Firmy średniej wielkości preferują rozwiązania w chmurze ze względu na ich skalowalność, pozwalającą zmniejszyć uzależnienie od wewnętrznych zasobów, oraz elastyczną zmianę ukierunkowania na koszty utrzymania zamiast wydatków kapitałowych (ilustracja 6).

Ludzie: wyszukiwanie odpowiednich pracowników, aby zwiększyć bezpieczeństwo

Do dobrych wiadomości należy zaliczyć fakt, że według badania porównawczego 92% firm średniej wielkości ma wyznaczoną osobę na dyrektorskim stanowisku odpowiedzialną za bezpieczeństwo (patrz ilustracja 7).

Pod warunkiem dysponowania odpowiednimi zasobami ludzkimi średnie firmy chętnie stosowałyby dodatkowe zabezpieczenia, na przykład w postaci zaawansowanej ochrony urządzeń końcowych lub firewalli chroniących aplikacje sieciowe.

Średnie firmy i duże przedsiębiorstwa łączy wspólna bolączka: niedostatek personelu IT ograniczający ich możliwości rozbudowy i wzmacniania zabezpieczeń. Z badań prowadzonych przez Cisco wynika, że firmy zwyczajnie nie dysponują odpowiednią liczbą pracowników, aby zarządzać narzędziami mogącymi zwiększyć poziom bezpieczeństwa.

Z tego względu wiele małych i średnich firm szuka uzdolnionych i wykwalifikowanych podwykonawców na zewnątrz, aby zapewnić sobie dostęp do niezbędnej wiedzy na temat zagrożeń, ograniczać koszty i sprawniej reagować na cyberataki. Dążenie do uzyskania obiektywnej opinii ekspertów było najczęstszym powodem wymienianym przez średnie firmy w związku z outsourcingiem zadań dotyczących zabezpieczeń (ilustracja 8), obok efektywności kosztowej oraz konieczności sprawnego reagowania na zdarzenia związane z bezpieczeństwem.

Outsourcing pozwala firmom optymalnie wykorzystywać ograniczone zasoby, jednak wiele z nich może wpaść w kłopoty przez założenie, że wynajęty podwykonawca lub partner dostarczający usług w chmurze zapewni im wszelkie zabezpieczenia, których nie są w stanie obsługiwać samodzielnie.

Chad Paalman, CEO firmy NuWave Partners z Kalamazoo w stanie Michigan będącej Partnerem Cisco, zauważył, że wiele małych i średnich firm nie wie, jak dokładnie wygląda oferta ich zewnętrznych podwykonawców pod względem wykonywanych analiz i monitorowania bezpieczeństwa.

Ilustracja 7 Osoby na stanowiskach dyrektorskich odpowiedzialne za bezpieczeństwo w średnich firmach

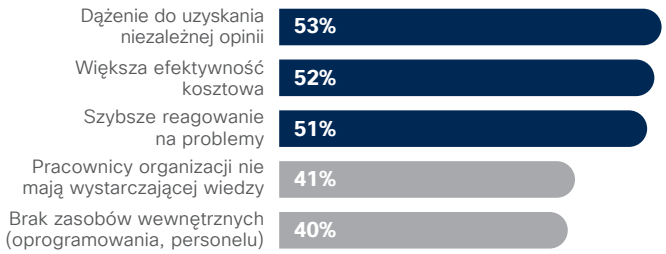
92%
Ma dyrektora odpowiedzialnych za bezpieczeństwo

Tytuł członka kadry kierowniczej odpowiedzialnego za bezpieczeństwo

42%	(CISO) Dyrektor ds. bezpieczeństwa informatycznego
24%	(CSO) Dyrektor ds. bezpieczeństwa
10%	(CEO) Dyrektor generalny
8%	(CIO) Dyrektor ds. IT
3%	(COO) Dyrektor ds. operacyjnych
5%	(CTO) Dyrektor ds. technologii
6%	(SVP lub VP) Starszy wiceprezes lub wiceprezes ds. IT
2%	(CRO lub CCO) Dyrektor ds. ryzyka lub dyrektor ds. zgodności z przepisami

Źródło: Porównawcze opracowanie Cisco na temat możliwości ochrony, 2018

Ilustracja 8 Średnie firmy zatrudniają podwykonawców, aby rozwiązać problem niedostatecznych zasobów wewnętrznych



Źródło: Porównawcze opracowanie Cisco na temat możliwości ochrony, 2018

„Wielu liderów biznesowych nie ma wiedzy na temat swoich sieci. Zakładają, że firewall jest odpowiednikiem kłódki na drzwiach, uniemożliwiającej dostęp komukolwiek z zewnątrz. Przyjmują również, że zlecenie kwestii zabezpieczeń dostawcy usług zarządzanych jest równoznaczne z monitorowaniem dzienników zdarzeń lub że świadczone usługi obejmują wykrywanie włamań”.

Chad Paalman, CEO firmy NuWave Technology Partners

Niemniej jednak małe i średnie firmy są skłonne powierzać podwykonawcom następujące zadania:

- zewnętrzne usługi doradcze i konsultacyjne (57%),
- reagowanie na zdarzenia (54%),
- monitorowanie zabezpieczeń (51%).

Mniej chętnie jednak zlecają na zewnątrz inne zadania, takie jak gromadzenie informacji na temat zagrożeń (39%) (patrz ilustracja 9).

Dobrą wiadomością jest to, że średnie firmy wydają się poświęcać część swoich ograniczonych zasobów przypisanych do zwiększania wiedzy na temat zagrożeń i reagowania na nie na skuteczniejsze gromadzenie informacji o zagrożeniach i reagowanie na wydarzenia związane z bezpieczeństwem.

Procesy: regularne kontrole w ramach zarządzania zabezpieczeniami

Kompleksowe, regularnie wykonywane procesy dotyczące zabezpieczeń, jak na przykład kontrole cennych aktywów i weryfikacja praktyk dotyczących bezpieczeństwa, pomagają firmom identyfikować słabe punkty swoich zabezpieczeń. Takie procesy nie są rozpowszechnione w małych i średnich firmach w wystarczającym stopniu, być może z powodu braków w personelu.

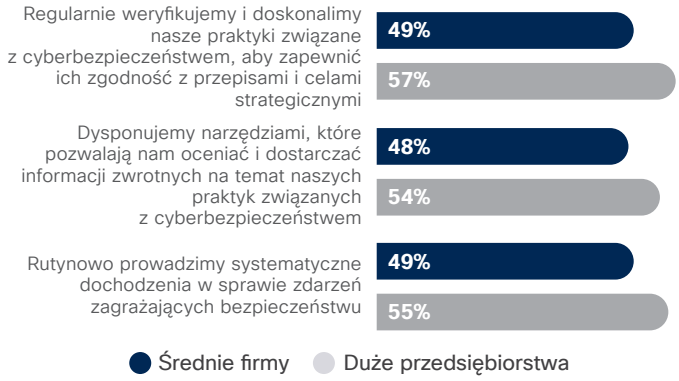
Na przykład według badania porównawczego Cisco na temat możliwości ochrony na 2018 r. średnie firmy rzadziej niż duże przedsiębiorstwa przyznają się do regularnej weryfikacji praktyk związanych z bezpieczeństwem, stosowania narzędzi umożliwiających sprawdzanie działania zabezpieczeń oraz rutynowego badania zdarzeń dotyczących bezpieczeństwa (ilustracja 10).

Z drugiej strony aż 91% średnich firm twierdzi, że przynajmniej raz w roku przeprowadza ćwiczenia mające na celu działanie planów reagowania na wydarzenia dotyczące bezpieczeństwa. Podobnie jednak jak w przypadku polegania na zabezpieczeniach chmury i podwykonawcach nasuwa się pytanie, czy takie plany reagowania na wydarzenia dotyczące bezpieczeństwa są wystarczające, aby odeprzeć coraz bardziej wyrafinowane ataki cyberprzestępców.

Ilustracja 9 Średnie firmy zlecają na zewnątrz usługi doradcze i konsultacyjne oraz zadania w zakresie reagowania na wydarzenia dotyczące bezpieczeństwa

Źródło: Porównawcze opracowanie Cisco na temat możliwości ochrony, 2018

Ilustracja 10 Średnie firmy są mniej skłonne do stosowania procesów operacyjnych



Źródło: Porównawcze opracowanie Cisco na temat możliwości ochrony, 2018

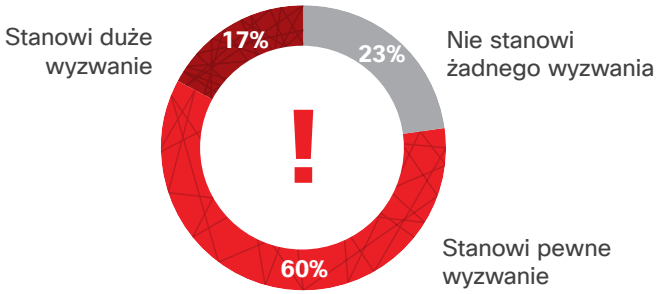
Łączenie ludzi, procesów i technologii: wyzwanie synchronizacji

Czy rozbudowa zabezpieczeń o większą liczbę produktów różnych dostawców oraz przydzielenie odpowiednich zasobów IT do ich obsługi pomoże małym i średnim firmom lepiej zarządzać bezpieczeństwem? Skutek może być wręcz odwrotny, przynajmniej pod względem zrozumienia i synchronizacji alertów dotyczących bezpieczeństwa.

Większość firm małych i średnich firm już dziś zdaje sobie sprawę, że wraz ze wzrostem złożoności środowiska produktów różnych dostawców rosną również ich obowiązki. Na przykład 77% przedstawicieli średnich firm uznało synchronizację alertów pochodzących z wielu różnych rozwiązań za dość duże lub duże wyzwanie (ilustracja 11).

Jak ustalono w badaniu porównawczym, gdy przedsiębiorstwa starają się analizować te alerty, trudności w skoordynowaniu działań ludzi, procesów i technologii mogą skutkować tym, że wiele z tych alertów pozostanie niezbadanych (ilustracja 12):

Ilustracja 11 Średnie firmy są mniej skłonne do stosowania procesów operacyjnych



Źródło: Porównawcze opracowanie Cisco na temat możliwości ochrony, 2018

Ilustracja 12 Odsetek alertów zabezpieczeń, w przypadku których nie stosuje się badania ani środków zaradczych

Źródło: Porównawcze opracowanie Cisco na temat możliwości ochrony, 2018

Zalecenia na przyszłość

Technologia

Zastanawiając się nad wdrożeniem nowych narzędzi, organizacje mogą starać się unikać zwiększania liczby producentów rozwiązań, którymi zarządzają i na alerty z których muszą reagować.

Mając to na uwadze, należy zadać sobie pytanie, czy produkty zostały opracowane w sposób zapewniający ich kompatybilność? Na ile skutecznie będzie można zintegrować je z innymi rozwiązaniami pod względem udostępniania danych i informacji o zagrożeniach? Czy jest możliwa integracja konsoli zarządzania?

Jeśli dostawca twierdzi, że jego produkty są kompatybilne z innymi, czy wymaga to jakichś działań ze strony użytkownika, na przykład znacznych nakładów pracy dotyczących interfejsu API?

Uczenie maszynowe, niezależnie od otaczającego je szumu, ma swoje miejsce pośród technologii zabezpieczeń. Należy jednak szukać rozwiązań, w których uczenie maszynowe stanowi dodatkową warstwę wykrywania zagrożeń w już wdrożonych produktach, nie zaś odrębny produkt od innego dostawcy, wymagający osobnego zarządzania.

Ludzie i procesy

Krótko mówiąc, zwiększenie poziomu cyberbezpieczeństwa wymaga opracowania strategii. Według Vistage Research Center, centrum zasobów dla liderów biznesu, zaledwie 38% małych i średnich firm opracowało i wdrożyło aktywną strategię obrony przed cyberzagrożeniami.[6]

Czy plany firmy obejmują odpowiednie szkolenia dla użytkowników końcowych? Czy polisy ubezpieczeniowe firmy pokrywają straty odniesione na skutek cyberataku? Opracowanie planów zapewnienia ciągłości działalności biznesowej i komunikacji w sytuacjach kryzysowych umożliwia szybsze przywrócenie działalności po awarii i pomaga zapobiec stratom wizerunkowym.

Ponadto osoby kierujące działem IT muszą dostarczać kadrze kierowniczej firmy niezbędnych i zrozumiałych informacji na temat włamań:

- Jaki skutki dla organizacji niesie cyberatak?
- Jakie środki zespół ds. zabezpieczeń podejmuje w celu opanowania i zbadania zagrożenia? Jak długo potrwa przywrócenie normalnej działalności operacyjnej?[7]

„Przez przyjęcie zestawu współpracujących ze sobą platform i narzędzi, w odróżnieniu od rozproszonej grupy odrębnych rozwiązań mogących wręcz kolidować ze sobą, można wzmocnić skuteczność zabezpieczeń, a także uprościć zarządzanie nimi.”

Ben M. Johnson, CEO firmy Liberty Technology

„Małe i średnie firmy powinny dokonać oceny tych zagrożeń i opracować plany reagowania zanim dojdzie do naruszenia bezpieczeństwa, a nie w jego wyniku”.

Chad Paalman, NuWave Technology Partners

6 „Cyberthreats and Solutions for Small and Midsize Businesses”, Vistage Research Center, 2018 r. Raport opracowany we współpracy z firmą Cisco i organizacją National Center for the Middle Market Dostępny pod adresem: https://www.vistage.com/research-center/business-operations/risk-management/20180503-22912/.

7 Półroczny raport Cisco 2017 r.: https://www.cisco.com/c/dam/global/es_mx/solutions/security/pdf/cisco-2017-midyear-cybersecurity-report.pdf. 13 Tamże.

Wnioski

Końcowe zalecenie dla małych i średnich firm dotyczące zwiększania poziomu cyberbezpieczeństwa przedstawia się następująco: zmiany wprowadzane stopniowo są lepsze niż żadne. Krótko mówiąc, nie należy dopuścić, aby dążenie do osiągnięcia perfekcji w kwestii zabezpieczeń stanęło na drodze do ich stopniowego ulepszania. Doskonałość w tej, jak i w innych dziedzinach, jest po prostu nieosiągalna.

Małe i średnie firmy muszą także zrozumieć, że nie istnieje żadne magiczna technologia stanowiąca odpowiedź na wszelkie problemy dotyczące cyberbezpieczeństwa. Krajobraz zagrożeń jest zbyt złożony i dynamiczny, a obszary ataku stale się powiększają i zmieniają. W reakcji na to technologie i strategie zabezpieczeń muszą również stale ewoluować.

Więcej informacji na temat skoncentrowanego na zagrożeniach podejścia stosowanego przez Cisco do cyberbezpieczeństwa można znaleźć na stronie cisco.com/go/security.

Centrala dla krajów Ameryki Północnej i Południowej
Cisco Systems, Inc.
San Jose, CA

Centrala dla krajów Azji i Pacyfiku
Cisco Systems (USA) Pte. Ltd.
Singapur

Centrala europejska
Cisco Systems International BV, Amsterdam,
Holandia

Firma Cisco ma ponad 200 biur na całym świecie. Pełną listę adresów, numerów telefonów oraz faksów można znaleźć na stronie internetowej firmy Cisco pod adresem www.cisco.com/go/offices.

Opublikowano w lipcu 2018 r.