**Cisco 2018 Annual Cybersecurity Report: Liderzy cyberbezpieczeństwa stawiają na automatyzację, machine learning oraz sztuczną inteligencję**

Jak wynika z badania przeprowadzonego przez Cisco, 39% organizacji polega na automatyzacji procesów związanych z cyberbezpieczeństwem, 34% wykorzystuje uczenie maszynowe, a 32% jest zależna od funkcjonalności sztucznej inteligencji.

WARSZAWA – 23 marca 2018 — Cyberataki typu malware, polegające na zainfekowaniu komputera złośliwym oprogramowaniem, stają się coraz bardziej wyrafinowane. Cyberprzestępcy wykorzystują usługi chmurowe i unikają wykrycia dzięki ruchowi szyfrowanemu, który pozwala im ukryć zapytania wysyłane do serwerów (command-and-control). Chcąc ograniczyć czas, w którym cyberprzestępcy mogą prowadzić swoje działania, specjaliści ds. bezpieczeństwa coraz chętniej sięgają po rozwiązania wykorzystujące sztuczną inteligencję oraz uczenie maszynowe. Potwierdzają to dane z jedenastej edycji Cisco® 2018 Annual Cybersecurity Report (ACR).

Szyfrowanie połączenia ma na celu zwiększenie poziomu bezpieczeństwa. Wzrost szyfrowanego ruchu sieciowego, który w październiku stanowił aż 50 % całości (zarówno tego właściwego jak i generowanego przez cyberprzestępców) postawił przed specjalistami ds. cyberbezpieczeństwa nowe wyzwania związane z monitorowaniem potencjalnych zagrożeń. W ciągu ostatniego roku eksperci Cisco zaobserwowali trzykrotny wzrost wykorzystania szyfrowanej komunikacji sieciowej w sprawdzanych plikach malware.

Wdrażanie rozwiązań z zakresu uczenia maszynowego może zwiększyć bezpieczeństwo sieci, ponieważ w dłuższej perspektywie pozwalają one „nauczyć się” jak odnajdywać wzorce w szyfrowanych połączeniach, chmurze oraz środowisku Internetu Rzeczy. Część z 3600 profesjonalistów, którzy wzięli udział w badaniu Cisco przyznało, że chętnie uzupełniliby portfolio posiadanych narzędzi o rozwiązania z zakresu uczenia maszynowego oraz sztucznej inteligencji, ale zniechęca ich duża ilość błędnych alertów (false positives) generowanych przez system. Dalszy postęp tych technologii, obecnie wciąż na wczesnym etapie rozwoju, sprawi, że liczba prawidłowych wskazań w monitorowanym środowisku sieciowym będzie coraz większa.

„Zeszłoroczna ewolucja ataków malware pokazuje, że cyberprzestępcy wciąż się uczą” mówi John N. Stewart, Senior Vice President and Chief Security and Trust Officer w Cisco. „Musimy podnieść poprzeczkę – kompleksowe zarządzanie, przywództwo biznesowe, inwestycje technologiczne oraz efektywne praktyki – wciąż istnieje zbyt wiele zagrożeń, naszym zadaniem jest ich zniwelowanie.”

**Główne tezy Cisco 2018 Annual Cybersecurity Report:**

**Koszty cyberataków nie są już tylko hipotetyczną liczbą**

Jak wynika z badania Cisco, ponad połowa cyberataków spowodowała straty finansowe wysokości ponad 500 000 USD, włączając w to m.in. utratę przychodu, klientów, okazji biznesowych oraz koszty operacyjne.

**Wzrost złożoności i szybkości cyberataków wymierzonych w łańcuch dostaw**

Cyberataki skierowane na łańcuchy dostaw mogą zainfekować komputery na ogromną skalę. Co gorsza, mogą utrzymywać się przez miesiące lub nawet lata. Specjaliści ds. cyberbezpieczeństwa powinni mieć świadomość potencjalnych zagrożeń wynikających z wykorzystania oprogramowania i sprzętu dostawców, którzy nie posiadają odpowiedniej polityki bezpieczeństwa.

Dwa tego typu ataki miały miejsce w 2017 roku. Nyetya oraz Ccleaner zainfekowały komputery użytkowników wykorzystując oprogramowanie pochodzące z zaufanego źródła.

Specjaliści ds. cyberbezpieczeństwa powinni korzystać z zewnętrznych testów skuteczności technologii odpowiadających za bezpieczeństwo firm w celu redukcji ryzyka wystąpienia cyberataków skierowanych na łańcuch dostaw.

**Bezpieczeństwo staje się coraz bardziej złożoną kwestią, jednocześnie rozszerza się zakres jego naruszeń**

* Aby lepiej ochronić organizacje, specjaliści odpowiedzialni za kwestie bezpieczeństwa wdrażają zestawy produktów i rozwiązań, pochodzące od różnych dostawców. Biorąc pod uwagę jednoczesny wzrost liczby naruszeń, ta złożoność systemów bezpieczeństwa może nieść negatywne skutki dla zdolności organizacji do obrony przed atakami, m.in. zwiększone ryzyko strat.
* W 2017 r. 25% specjalistów od zabezpieczeń przyznało, że używało produktów od 11 do 20 dostawców. Dla porównania, w 2016 roku potwierdziło to jedynie 18% specjalistów ds. bezpieczeństwa.
* Specjaliści do spraw bezpieczeństwa przyznali, że 32% naruszeń dotyczyło ponad połowy systemów. Dla porównania, w 2016 potwierdziło to jedynie 15%.

**Specjaliści ds. bezpieczeństwa dostrzegają wartość narzędzi do analizy behawioralnej w lokalizowaniu autorów ataków sieciowych**

92 % specjalistów ds. bezpieczeństwa przyznaje, że narzędzia do analizy zachowań sprawdzają się w działaniu. Dwie trzecie przedstawicieli sektora opieki zdrowotnej a także usług finansowych uznało analizę zachowań za wyjątkowo skuteczną w identyfikowaniu autorów ataków.

**Wykorzystanie chmury rośnie; napastnicy wykorzystują braki zaawansowanych zabezpieczeń**

* W tegorocznej edycji badania 27% specjalistów ds. bezpieczeństwa stwierdziło, że używa chmur prywatnych działających w oparciu o infrastrukturę zewnętrzną. Odsetek ten wzrósł o 7% w stosunku do 2016 roku, kiedy takiej odpowiedzi udzieliło 20% respondentów.
* 57% badanych przyznaje, że wykorzystuje hosting w chmurze z uwagi na wyższy poziom bezpieczeństwa danych, 48% ze względu na skalowalność, natomiast 46% z uwagi na łatwość użycia technologii.
* Podczas, gdy chmura oferuje wyższy poziom bezpieczeństwa danych, atakujący wykorzystują fakt, że zespoły ds. cyberbezpieczeństwa mają problemy z ochroną rozwijających się środowisk cloud computing. Z pomocą przychodzi połączenie najlepszych praktyk, zaawansowanych technologii bezpieczeństwa, takich jak uczenie maszynowe oraz narzędzi pierwszej linii obrony oraz platform bezpieczeństwa w chmurze.

**Trendy w zakresie wzrostu ilości złośliwego oprogramowania mają wpływ na czas wykrywania niebezpiecznych zdarzeń**

* Średni czas wykrycia przez Cisco nowego incydentu bezpieczeństwa (TTD ang. Time To Detection) wyniósł około 4,6 godzin w okresie od listopada 2016 r. do października 2017 r. To znacznie poniżej 39-godzinnej średniej TTD zgłoszonej w listopadzie 2015 r. oraz 14-godzinnej średniej odnotowanej w raporcie Cisco 2017 Annual Cybersecurity Report za okres od listopada 2015 r. do października 2016 r.
* Wykorzystanie technologii zabezpieczeń w chmurze było kluczowym czynnikiem, który zdaniem specjalistów Cisco wpłynął na utrzymanie średniej TTD na niskim poziomie. Krótszy czas wykrycia zdarzeń pomaga specjalistom odpowiedzialnym za bezpieczeństwo szybciej przeciwdziałać atakom.

**Dodatkowe rekomendacje dla osób odpowiedzialnych za bezpieczeństwo organizacji:**

Ważne jest potwierdzanie przestrzegania zasad i praktyk korporacyjnych dotyczących łatania aplikacji, systemów i urządzeń.

Menedżerowie bezpieczeństwa powinni uzyskiwać dostęp do aktualnych i dokładnych danych oraz procesów dotyczących zagrożeń oraz włączyć te informacje do monitoringu bezpieczeństwa w ramach organizacji.

Analizy bezpieczeństwa powinny być bardziej kompleksowe i prowadzone w bardziej zaawansowany sposób.

W świecie szybko „przemierzających” sieć internetową programów typu ransomware oraz innych cyberzagrożeń ważne jest, aby często tworzyć kopie zapasowe danych oraz testować procedury ich przywracania.

Istotne jest także regularne skanowanie zabezpieczeń firmowych mikroserwisów, usług w chmurze oraz systemów do administrowania aplikacjami.

**O raporcie:**

Cisco 2018 Annual Cybersecurity Report już 11 rok z rzędu przedstawia wyniki i spostrzeżenia wynikające z badań zagrożeń i analizy trendów cyberbezpieczeństwa w ciągu ostatnich 12-18 miesięcy, dostarczone przez partnerów technologicznych firmy: Anomali, Lumeta, Qualys, Radware, SAINT, i TrapX. W raporcie uwzględniono także wyniki corocznego badania potencjału organizacji w zakresie zdolności bezpieczeństwa (Security Capabilities Benchmark Study), w którym w tym roku wzięło udział 3 600 szefów działów bezpieczeństwa (CSO) i menedżerów odpowiedzialnych za bezpieczeństwo (SecOps) z 26 krajów, zapytanych o stan cyberbezpieczeństwa w ich organizacjach.

.:|:.:|:.

**O Cisco:**

Cisco (NASDAQ: CSCO) to światowy lider technologiczny zapewniający działanie Internetu od 1984 r. Pracownicy, partnerzy i produkty Cisco pomagają społeczeństwom łączyć się w bezpieczny sposób i już dziś korzystać z cyfrowych możliwości jutra. Dowiedz się więcej na www.newsroom.cisco.com. Cisco i logo Cisco to zastrzeżone znaki towarowe należące do Cisco i/lub jego podmiotów zależnych w U.S. i innych krajach. Pełna lista znaków towarowych Cisco dostępna jest pod adresem: www.cisco.com/go/trademarks. Znaki towarowe firm trzecich są ich własnością. Użycie słowa partner nie oznacza stosunku partnerstwa pomiędzy Cisco i inną firmą.

**Kontakt:** Łukasz Dąbrowski | ldabrows@cisco.com | tel.: 795 03 12 02