KOMUNIKAT PRASOWY

Zagrożenia wychodzą z cienia

Doroczny raport firmy Cisco na temat bezpieczeństwa

Zachowania i nawyki pracowników nowej generacji, a przede wszystkim – ich podejście do koncepcji „bycia online" – to główne czynniki potęgujące największe zagrożenia – wynika z najnowszego raportu Cisco's Annual Security Report, poświęconego bezpieczeństwu IT. Źródłem zagrożeń, w coraz większym stopniu, stają się – według raportu - również legalne serwisy handlowe, społecznościowe, a także – różnego rodzaju wyszukiwarki internetowe.

Warszawa, Polska – 5 marca 2013 – Cisco prezentuje wyniki tegorocznej edycji Cisco's 2013 Annual Security Report (ASR), poświęconego bezpieczeństwu sieciowemu. Raport przeprowadzony został w różnych krajach świata, również w Polsce. Pokazuje on jakie są coraz większe zagrożenia dla bezpieczeństwa przedsiębiorstw, ich działów IT a także prywatnych użytkowników. W tym roku ostrzega szczególnie przed nowymi zagrożeniami, które spowodowane są mieszaniem przez pracowników prywatnych zachowań i nawyków z obowiązkami zawodowymi. Jest to – zdaniem autorów raportu – coraz wyraźniejsza tendencja tzw. Generacji Y, czyli pokolenia, które chce być cały czas „*online*" i które wykorzystuje internet do wielu czynności życia codziennego – także będąc w pracy.
Raport przekazuje także m.in. dane dotyczące zagrożenia złośliwym oprogramowaniem w poszczególnych krajach, aktualny stan trendów w rozsyłce spamu, czy zachowania Generacji Y w odniesieniu do przeglądania serwisów społecznościowych czy handlowych i skłonności do przekazywania im swoich danych. Na szczególną uwagę zasługuje też zbiór wniosków dotyczy postępowania pracowników – przedstawicieli Generacji Y z zaleceniami działów bezpieczeństwa firm, w których są zatrudnieni.

Największe zagrożenie infekcją – w legalnych serwisach

Wyniki raportu dowodzą, że najwyższe skoncentrowanie zagrożeń dotyczy działających zgodnie z prawem serwisów odwiedzanych przez rzesze użytkowników, takich jak wyszukiwarki internetowe, strony sklepów detalicznych czy platformy mediów społecznościowych, a nie – jak było jeszcze niedawno temu - w przypadku stron pornograficznych, farmaceutycznych czy też stron z grami hazardowymi.
W rzeczywistości - jak pokazuje najnowszy raport Cisco - witryny sprzedaży internetowej stanowią 21-krotnie, a wyszukiwarki – aż 27-krotnie większe zagrożenie związane z infekcją złośliwym oprogramowaniem niż np. strony udostępniające pirackie oprogramowanie. Na niebezpieczeństwo jesteśmy też narażeni przy przeglądaniu reklam internetowych. Niosą one ze sobą aż 182 razy większe zagrożenie związane z infekcją złośliwym oprogramowaniem niż pornografia.

Prywatne nawyki a zawodowe czynności

Według najnowszego raportu Cisco, przyzwyczajenia, jakie wielu pracowników przenosi do każdego miejsca – przede wszystkim do pracy - zwiększają zagrożenia dla bezpieczeństwa przedsiębiorstw. Chodzi tu przede wszystkim o ich nawyki związane z korzystaniem z różnych urządzeń i używaniem ich do realizacji codziennych obowiązków, aby być cały czas „online".
Wpływy tego trendu „konsumeryzacji" na bezpieczeństwo biznesowe dodatkowo potęgowane są wnioskami z opublikowanego w grudniu 2012 roku raportu Cisco Connected World Technology Report (CCWTR), który koncentruje się na postawach i tendencjach pracowników następnego pokolenia, czyli tzw. Generacji Y, z całego świata. Zgodnie z tym opracowaniem, większość pracowników generacji Y (91%) uważa, że era prywatności już minęła, ale zaledwie jedna trzecia z nich nie przejmuje się informacjami, jakie są ogólnie dostępne na ich temat. Są skłonni poświęcić swoją prywatność na rzecz tzw. „socjalizacji" online. W rzeczywistości większość pracowników Generacji Y z całego świata stwierdziła, że czuje się znacznie lepiej, jeśli dzieli się informacjami ze swojego życia prywatnego z serwisami sprzedaży detalicznej niż z działami IT firm, w których są zatrudnieni – w tym przede wszystkim działami, które zajmują się ochroną tożsamości i urządzeń pracowników.

Wraz z ukończeniem szkół przez przedstawicieli Generacji Y i ich wejściem na rynek pracy, polityka, a także kultura działania firm zostały wystawione na nie lada próbę. Związana ona była z dość specyficznymi oczekiwaniami tej nowej siły roboczej, które dotyczyły między innymi wolności korzystania z mediów społecznościowych, wyboru urządzeń do pracy, czy mobilnego stylu życia. Chodziło więc o oczekiwania, których nie stawiało dotąd żadne poprzednie pokolenie. Jak pokazywał już grudniowy raport Cisco poświęcony internetowym zwyczajom Generacji Y, w swoim pierwszym rozdziale Connected World Technology Report, przedstawiciele tego pokolenia nieustannie sprawdzają media społecznościowe, skrzynkę pocztową i aktualizacje publikacji tekstowych, bez względu na to czy znajdują się w łóżku (aż 4 na 5 przebadanych w Polsce), spożywając przy stole obiad (20% w Polsce), w łazience (1 na 3), czy nawet podczas prowadzenia samochodu (1 na 5). Ten styl wkracza teraz z pełną mocą do środowisk pracy, wymagając od firm zastanowienia się na tym, jak przełoży się on na jakość pracy w przyszłości i jak- w związku z tym – można będzie współzawodniczyć z innymi firmami, aby pozyskać kolejną falę talentów. Niestety, jak pokazują badania nad bezpieczeństwem, styl życia siły roboczej następnego pokolenia niesie ze sobą także zagrożenia dla bezpieczeństwa, z jakimi firmy dotąd nie miały styczności na aż tak szeroką skalę.

Kluczowe wnioski

Android Malware

- Zagrożenie od złośliwego oprogramowania (malware) dla systemów Androida wzrosło w 2012 roku o 2577 procent. *(ASR)*
- Jednakże złośliwe oprogramowania atakujące aplikacje mobilne stanowią zaledwie 0,5 procenta wszystkich czyhających w sieci niebezpieczeństw tego typu. *(ASR)*
- Trendy te stają się szczególnie ważne zwłaszcza, jeśli weźmiemy pod uwagę, że smartfon jest teraz najpopularniejszym urządzeniem generacji Y na świecie, wyprzedzając pod tym względem laptopy, komputery oraz tablety *(CCWTR)*

Zagrożenie złośliwym oprogramowaniem w poszczególnych krajach

W roku 2012 nastąpiła znacząca zmiana w obszarach występowania złośliwego oprogramowania na całym świecie. Chiny spadły z zajmowanego w roku 2011 drugiego miejsca na liście państw najbardziej ogarniętych plagą złośliwego oprogramowania, na pozycję szóstą w roku ubiegłym. Kraje skandynawskie, takie jak Dania i Szwecja doświadczyły wzrostu wystąpień złośliwego oprogramowania w swoich zasobach internetowych, awansując odpowiednio na trzecie i czwarte miejsce. Stany zjednoczone utrzymały pierwszą pozycję z wynikiem 33 procent wszystkich światowych zasobów złośliwego oprogramowania internetowego. *(ASR)*

1. Stany Zjednoczone	33,14%
2. Rosja	9,79%
3. Dania	9,55%
4. Szwecja	9,27%
5. Niemcy	6,11%
6. Chiny	5,65%
7. Wlk. Bryt.	4,07%
8. Turcja	2,63%
9. Holandia	2,27%
10. Irlandia	1,95%

Trendy w rozsyłce SPAMu

- Ilość rozsyłanych niechcianych wiadomości (SPAMu) spadła o 18 procent, jeżeli porównamy rok 2012 do roku 2011, w przypadku niechcianych wiadomości rozsyłanych w godzinach pracy, i o 25% w przypadku rozsyłanych w weekendy. *(ASR)*
- W 2012 większość niechcianych wiadomości była rozsyłana w ciągu roboczych dni tygodnia - wtorek był najbardziej „spamowym" dniem tygodnia. *(ASR)*
- Czołowym generatorem niechcianych wiadomości są Indie, a na drugie miejsce w roku 2012, z szóstego w roku 2011, awansowały Stany Zjednoczone. W pierwszej piątce znalazły się także Korea, Chiny oraz Wietnam. *(ASR)*
- Najczęściej niechciane wiadomości zawierały w swojej treści informacje na temat leków, takich jak Viagra czy Cialis oraz luksusowych zegarków, jak Rolex czy Omega. *(ASR)*
- Spamerzy maksymalizują zwrot z poniesionych inwestycji, reklamując się przy okazji różnych wydarzeń ze świata rzeczywistego, poprzez specyficzne i krótko

trwające kampanie. *(ASR)*

- Styczeń-marzec: Oprogramowanie Windows, które zbiegło się z wydaniem systemu Windows 8 Consumer Preview firmy Microsoft.
- Luty-kwiecień: Oprogramowanie do rozliczeń podatkowych, podczas kampanii sezonu podatkowego w Stanach Zjednoczonych.
- Styczeń-marzec oraz sierpień-grudzień: Profesjonalne sieci, takie jak LinkedIn, w kontekście chęci zmiany obranej ścieżki zawodowej - na początku i na końcu roku.
- Wrzesień-listopad: Dostawcy telefonów komórkowych - w ramach wydania iPhone'a 5 firmy Apple.

Kompromisy ze szkodą dla prywatności

Cisco przeanalizowało trudności, jakie w prowadzeniu biznesu wiążą się z tymi i innym zagrożeniami statystycznymi, poprzez przebadanie tendencji i zachowań pracowników z Generacji Y – a więc osób, które zawsze są „on line" i żyją wedle idei „na żądanie".

- Chociaż większość respondentów z Generacji Y nie wierzy w zapewnianą przez serwisy internetowe ochronę danych osobowych (75 procent na świecie i 70 procent w Polsce), takich jak dane z karty kredytowej czy osobiste dane kontaktowe, to ich brak zaufania nie wpływa na ich zachowanie w sieci. Dlatego ryzykują, że może nikt na nich nie zwróci uwagi. To powoduje wywieranie presji na firmy, w których tacy pracownicy ryzykują rozpowszechnieniem prywatnych danych z wykorzystaniem swoich urządzeń firmowych i sieci korporacyjnych. *(CCWTR)*
- Pięćdziesiąt trzy procent respondentów z Generacji Y w Polsce nie ma nic przeciwko temu, że witryny internetowe śledzą i rozpowszechniają informacje o ich aktywności internetowej, pod warunkiem, że wcześniej są poproszeni o udzielenie na to zgody. *(CCWTR)*

Zgodność postępowania z polityką działów IT

- Zarówno w Polsce jak i na świecie średnio 9 na 10 (90 procent) przebadanych specjalistów z branży IT potwierdziło, że mają opracowane zasady dotyczące użytkowania niektórych urządzeń w pracy, ale tylko dwóch na pięciu respondentów z generacji Y przyznało, że ma świadomość istnienia takich zasad. *(CCWTR)*
- Sprawę pogarsza jeszcze to, że aż 70 procent respondentów z generacji Y świadomych istnienia zasad opracowanych przez działy IT, przyznaje, że się do nich nie stosuje. Młodzi ludzie w Polsce – podobnie jak ich rówieśnicy w Indiach i Japonii - wydają się zwracać większą uwagę na zasady panujące w firmach, gdyż współczynnik ten wyniósł tu znacznie mniej - 44 procent w Polsce. *(CCWTR)*
- Informatycy wiedzą o tym, że wielu pracowników nie stosuje się do tych zasad. W Polsce, podobnie jak i na całym świecie, około połowa informatyków jest przekonana, że pracownicy w ich firmach łamią zasady opracowane przez działy IT. *(CCWTR)*
- 65 procent polskich respondentów z generacji Y (i 66 procent na świecie) stwierdziło, że dział IT nie ma prawa monitorować ich aktywności internetowej, nawet jeśli aktywność ta prowadzona jest z firmowych urządzeń i za pośrednictwem korporacyjnych sieci. *(CCWTR)*

- Niechęć przedstawicieli generacji Y w stosunku do monitoringu aktywności internetowej prowadzonego przez pracodawcę była nawet w pewnym sensie większa niż do monitoringu, jaki prowadzą sklepy internetowe. Generacja Y jest zatem mniej uprzedzona do monitoringu aktywności internetowej prowadzonego przez kompletnie obce osoby związane z witrynami zakupowymi niż do monitoringu prowadzonego przez działy IT firm, których zadaniem jest ich ochrona i ochrona informacji firmowych. *(CCWTR)*

Internet Wszechrzeczy i przyszłość bezpieczeństwa

Patrząc w przyszłość możemy powiedzieć, że koncepcja Internetu Wszechrzeczy obrazuje największy współczesny trend w rozwoju Internetu. Im więcej osób, rzeczy i urządzeń podłączanych będzie do Internetu, tym więcej danych z większej liczby miejsc będzie trafiało do sieci korporacyjnych i należących do usługodawców. W związku z tym pojawiają się nowe zagrożenia i potrzeba bardziej złożonego podejścia do kwestii bezpieczeństwa.

- Wykładniczo rośnie liczba połączeń typu maszyna-z-maszyną (M2M), co prowadzi do zwielokrotnienia punktów końcowych, których różnorodność wykracza daleko poza takie urządzenia jak mobilne laptopy i komputery stacjonarne przyjmując formę połączenia „czegokolwiek –do -czegokolwiek". Forma ta umożliwia połączenie dowolnego urządzenia z dowolną chmurą i z dowolną aplikacją w obrębie dowolnej sieci.
- Do roku 2020, przy otwarciu Internetu na szacunkową liczbę 50 miliardów rzeczy, liczbie węzłów komunikacyjnych przekraczającej 13 biliardów (a dokładnie 13 311 666 640 184 600), dodanie zaledwie jednej „rzeczy" (50 miliardów + 1) zwiększy liczbę potencjalnych połączeń o kolejnych 50 miliardów.[1]
- Te nowe połączenia generują dane, których ruch musi być zabezpieczony w czasie rzeczywistym
  i oceniany pod kątem ich zagrożenia dla sieci, w której są przesyłane, zanim zdążą spowodować nieodwracalne szkody.
- W przypadku informatyków zajmujących się bezpieczeństwem sieci zadanie to polega na zarządzaniu ruchem treści neutralnych - przepuszczaniu ich z urządzeń końcowych i peryferyjnych do sieci.

Przykładowe wypowiedzi

- **Gaweł Mikołajczyk, specjalista d.s. bezpieczeństwa w Cisco Systems Polska**

  „Mieszanie prywatnych nawyków z realizacją zawodowych obowiązków wymaga od pracodawców, a zwłaszcza firmowych działów IT zwrócenia szczególnej uwagi na kwestie bezpieczeństwa – zwłaszcza, że – jak widać z raportu – na szczególne zagrożenie zainfekowaniem złośliwym oprogramowaniem narażone są serwisy, z których korzysta legalnie wielu

[1] **http://blogs.cisco.com/news/how-the-internet-of-everything-will-change-the-worldfor-the-better-infographic/**

użytkowników, i to przy coraz częstszym użyciu sieci firmowej, swoimi własnymi urządzeniami. Ze szczególną uwagą należy odnieść się do zasad bezpieczeństwa przez pracowników, którzy po prostu ich nie przestrzegają w wystarczającym stopniu. Pod tym względem jednak Polska wypada lepiej niż inne kraje, co dobrze rokuje , zwłaszcza jeśli chodzi o rozwój coraz popularniejszych trendów – takich jak BYOD."

O badaniu

Raport Cisco 2013 Annual Security Report podkreśla najbardziej kluczowe w bieżącym roku trendy w zakresie bezpieczeństwa oraz dostarcza wytycznych i wskazówek pozwalających utrzymać większe bezpieczeństwo środowisk technologii korporacyjnych. Raport Cisco Connected World Technology przybliża zagrożenia nakreślone w raporcie bezpieczeństwa.

Trzeci raport w rocznej serii Cisco Connected World Technology Report został zlecony przez firmę Cisco i przeprowadzony przez InsightExpress, niezależną firmę badającą rynek z siedzibą w Stanach Zjednoczonych. Globalne badanie składa się z dwóch ankiet: jednej skierowanej do studentów szkół wyższych oraz pracowników w wieku od 18 do 30 lat oraz drugiej skupiającej się na specjalistach z branży IT. Każda ankieta obejmuje 100 respondentów z każdego z 18 krajów, co daje łącznie 3600 respondentów. Wśród 18 krajów znalazły się: Stany Zjednoczone, Kanada, Meksyk, Brazylia, Argentyna, Wielka Brytania, Francja, Niemcy, Holandia, Rosja, Polska, Turcja, Republika Południowej Afryki, Indie, Chiny, Japonia, Korea Południowa i Australia.

ŹRÓDŁA DODATKOWE

- Informacje na temat Cisco 2013 Annual Security Report
- Odwiedź stronę internetową: Cisco Connected World Technology Report
- Informacje na temat przejęcia Cognitive Security - Christopher Young, wiceprezes działu Security and Government Group w firmie Cisco
- Materiał wideo: **John N. Stewart,** wiceprezes i dyrektor ds. bezpieczeństwa, Government and Corporate Security firmy Cisco **-** Bezpieczeństwo informacji: Globalny obraz w kontekście lokalnym
- Dodatkowe informacje na temat badań nad zachowaniem konsumentów dokonujących zakupów. Informacje prasowe Cisco, 14 stycznia 2013 *Ośmiu na dziesięciu konsumentów dokonuje zakupów korzystając z sieci*
- Materiał wideo: Generacja Y a technologia
- Dowiedz się więcej na temat koncepcji: Internet Wszechrzeczy
- Dowiedz się więcej na temat problemu Ruchu danych

- Dołącz do konwersacji na temat bezpieczeństwa na kanale Twittera @CiscoSecurity. Możesz również polubić profil Cisco Security na Facebooku http://facebook.com/ciscosecurity

- Dowiedz się więcej: Platforma blogowa Cisco

- Przeczytaj Blogi Cisco

Informacje o firmie Cisco:

Polski oddział Cisco został założony w Warszawie w 1995 roku. Od tego czasu Cisco aktywnie wspiera budowę w Polsce gospodarki opartej na wiedzy. W tym czasie powstała też sieć partnerów do której należy blisko 1000 przedsiębiorstw w całym kraju. W maju 2012 r. otwarto Cisco Global Support Center w Krakowie.

Największą inicjatywą Cisco w dziedzinie społecznej odpowiedzialności biznesu jest Cisco Networking Academy – program edukacyjny działający w Polsce od 2000 r. W całym kraju funkcjonuje dziś ponad 400 współpracujących z programem szkół i uczelni, w których uczy się ok. 20 tys. studentów. Od uruchomienia programu w oferowanych przez Cisco Networking Academy kursach z różnych obszarów IT wzięło udział ok. 80 tys. uczniów i studentów.

Cisco (NASDAQ: CSCO) jest światowym liderem w dziedzinie rozwiązań sieciowych, które zmieniają sposób kontaktowania się ludzi między sobą, komunikacji i współpracy. Więcej informacji na temat Cisco – na stronach http://www.cisco.pl i http://www.cisco.com

Polskie informacje Prasowe firmy znaleźć można na stronie:
http://www.cisco.com/web/PL/prasa, natomiast centralny serwis informacyjny znajduje się na http://newsroom.cisco.com

W razie dodatkowych pytań, proszę o kontakt:

Gabriela Mojkowska, Point of View
Tel. 669 518 899; 22 375 65 04; gm@pov.pl

Andrzej Mazurowski Point of View
Tel. 502 221 491; 22 375 65 23; am@pov.pl