Pracownicy z generacji Y – problem dla bezpieczeństwa firmowych sieci

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

Firma Cisco w tegorocznej edycji Cisco’s 2013 Annual Security Report (ASR), poświęconego bezpieczeństwu sieciowemu i przeprowadzonego w różnych krajach świata (także w Polsce) pokazuje, jak ewolują zagrożenia dla bezpieczeństwa przedsiębiorstw, ich działów IT a także prywatnych użytkowników.

W tym roku autorzy raportu ostrzegają 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 przedstawia też 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 dotyczący postępowania pracowników – przedstawicieli generacji Y – z zaleceniami działów bezpieczeństwa firm, w których są zatrudnieni.

Zaskakujące zagrożenia

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 – 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.

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”.

– Mieszanie prywatnych nawyków z realizacją zawodowych obowiązków wymaga od pracodawców, a zwłaszcza firmowych działów IT, zwrócenia szczególnej uwagi na kwestie bezpieczeństwa zwłaszcza, że – jak wynika z raportu – na szczególne zagrożenie zainfekowaniem złośliwym oprogramowaniem narażone są serwisy, z których korzysta legalnie wielu 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 mówi **Gaweł Mikołajczyk**, specjalista d.s. bezpieczeństwa w Cisco Systems Polska.

Socjlizacja ważniejższa od prywatności

W tym kontekście warto przypomnieć wnioski z opublikowanego w grudniu 2012 roku raportu Cisco Connected World Technology Report, który koncentruje się na postawach i tendencjach pracowników następnego

pokolenia, czyli tzw. generacji Y, z całego świata. Większość pracowników generacji Y (91 proc.) 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 proc. 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 będzie można 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.

Aktywność w sieci warta ryzyka

Cisco przeanalizowało trudności, jakie w prowadzeniu biznesu wiążą się z zachowanaimi pracowników generacji Y, tj. osób, które zawsze są „on line" i żyją wedle idei „na żądanie". Co bowiem ciekawe, chociaż większość respondentów z generacji Y nie wierzy w zapewnianą przez serwisy internetowe ochronę danych osobowych (75 proc. na świecie i 70 proc. 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. I co też charakterystyczne 53 proc. 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.

Nie dla kontoroli działu IT

Autorzy raportu odnotowują wprawdzie, że zarówno w Polsce jak i na świecie średnio 9 na 10 (90 proc.) przebadanych specjalistów z branży IT potwierdza posiadanie opracowanych zasad dotyczące użytkowania niektórych urządzeń w pracy, jednak tylko dwóch na pięciu respondentów z generacji Y przyznało, że ma świadomość istnienia takich zasad. Sprawę pogarsza jeszcze to, że aż 70 proc. 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. I 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.

65 proc. polskich respondentów z generacji Y (i 66 proc. 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. 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.

Źródło: Cisco

Zdjęcie: ginasanders / Photogenica