**Co minutę nowa ofiara działań hakerów w sieci. W Polsce przestępcy atakują uniwersytety, banki i centra danych.**

**Cyberataki stają się jednym z najpoważniejszych zagrożeń gospodarczych na świecie. Co minutę użytkownik sieci pada ofiarą zainfekowanych stron, co 9 minut korzysta z aplikacji zawierającej wirusy, co 29 minut komputery ściągają aplikację z wirusem, co 49 minut dane osobowe wyciekają z serwerów firmowych na skutek działań hakerów. W ubiegłym roku zaledwie 4 proc. firm z branży IT nie doświadczyło tego rodzaju zagrożenia – takie wnioski płyną z najnowszych badań firmy Check Point Software Technologies, przeprowadzonych w 122 krajach.**

Celem hakerów są zarówno jednostki państwowe jak i komercyjne, również te najbardziej wrażliwe jak bankowość. Zaatakowane firmy są zlokalizowane głównie w Stanach Zjednoczonych, Hiszpanii i Japonii. Wiele z nich znajduje się również w Niemczech, Francji, we Włoszech, Turcji, Irlandii, Polsce oraz Chinach.

Do najbardziej zagrożonych w Polsce sektorów w 2014 roku należały jednostki administracyjne, uniwersytety, centra danych oraz banki. Analitycy wskazują, że polskim użytkownikom bankowości online grozi coraz większe niebezpieczeństwo. To właśnie na ich kontach internetowych bardzo często testowane są złośliwe oprogramowania przez międzynarodowych hakerów. Można stwierdzić, że nasz kraj staje się „królikiem doświadczalnym” dla wszystkich nowinek, które związane sią z atakowaniem banków internetowych. W momencie, gdy dokonywane są ataki na poziomie europejskim jest prawie pewne, że polscy użytkownicy są nimi również atakowani – uważają analitycy.

*Możliwe, że cyberprzestępcy chcą testować w naszym kraju złośliwe oprogramowanie, dlatego, że systemy informacyjne w bankach na terenie Polski należą do najnowocześniejszych na świecie. Mogą oni wychodzić z założenie, że jeśli uda im się pokonać zabezpieczenia w naszym kraju, to w państwach, gdzie ich poziom jest niższy będzie im łatwiej przeprowadzać ataki* – uważa Krzysztof Wójtowicz, dyrektor Check Point Polska.

Zdaniem przedstawicieli Check Point Software Technologies, najgroźniejszym skutkiem działań hakerów jest ujawnienie poufnych informacji, takich jak tajemnice handlowe oraz know-how. To właśnie te informacje hakerzy starają się zdobyć z zainfekowanych komputerów, kopiując m.in. pliki PDF, dokumenty tekstowe czy dokumenty z arkuszami kalkulacyjnymi.

*Najsłabszym ogniwem jest człowiek. Hakerzy nie działają losowo, lecz wybierają sobie konkretne osoby i hasła, które mają dostęp do tajnych danych* – mówi Krzysztof Wójtowicz. Podkreśla jednak, że ze względu na szerokie spektrum zaatakowanych firm trudno znaleźć między nimi ogniwo wspólne.

Rosnącym zagrożeniem jest dynamiczny rozwój smartfonów. Zgodnie z przewidywaniami rynku, do 2020 roku większość smartfonów na świecie będzie miało połączenie z Internetem. Wizją przyszłości jest też połączenie ze sobą niemal wszystkiego - od samochodów do lodówki, lampy, a nawet toalety. Specjaliści podkreślają, że może to spowodować też negatywne konsekwencje - od zakłócenia życia rodzinnego, po zebranie naszych cennych danych.

W sierpniu BBC informowało, że ofiarą hakerów padł m.in. Community Health Systems, amerykański koncern, który prowadzi ponad 200 szpitali. Cyberprzestępcy przejęli dane 4,5 mln osób.

Ostatnio nie ma tygodnia bez informacji o atakach hakerów na renomowane firmy, czy instytucje rządowe. Comminity Health Systems tylko to jeden z przykładów. W Polsce 14 sierpnia doszło do ataku na strony Giełdy Papierów Wartościowych i Prezydenta RP (prezydent.pl), natomiast pod koniec ubiegłego miesiąca doszło do kolejnego ataku na Play Station Network i Sony Entertainment Network.

Ataki mają często wymiar polityczny. W zeszłym roku doszło do serii ataków, dokonanych przez grupę hakerów zwaną Syryjską Armią Elektroniczną, na amerykańskie strony internetowe (między innymi New York Times, Huffington Post i Twitter). Z kolei w zeszłym miesiącu Bloomberg poinformował o włamaniach na serwery JP Morgan Chase i co najmniej czterech innych amerykańskich banków. Hakerzy skradli z nich gigabajty danych klientów i pracowników banków. Śledztwo FBI wykazało, że ataki przeprowadzone zostały przez rosyjskich hakerów za pośrednictwem serwerów południowoamerykańskich. Niewykluczenie, że ofiarami ataków mogą być także banki europejskie.

Trwa wyścig pomiędzy hakerami a wyspecjalizowanymi firmami, które starają się wykryć słabe punkty w oprogramowaniu zanim zrobią to cyberprzetępcy.

Nawet toalety nie są bezpieczne, gdy hakerzy za cel obiorą domowe urządzenia - pisze Bloomberg. Już wkrótce smartfon będzie w stanie zablokować urządzenia domowe, włączyć klimatyzację, sprawdzić, czy mleko jest jeszcze dobre, a nawet na czas rozgrzać żelazko. To dobra wiadomość, ale jak każda ma też tę gorszą stronę – urządzenia te będą też mogły posłużyć przestępcy do włamania do domu i życia prywatnego ofiar. Z powodu coraz większej popularności mobilnej kontroli domów, firmy takie jak Samsung czy LG poważnie zabrały się za bezpieczeństwo swoich produktów.

**Wykryć atak**

Cyberatak przestaje być potężnym zagrożeniem, gdy zostaje wykryty. Zainteresowani wiedzą wtedy, że trzeba się bronić i dostają stosowne narzędzia.

*Technologie te stają się coraz bardziej złożone, otwierając szereg nowych zagrożeń* - podkreśla David Klusacek, Dyr. CEE Check Point Software Technologies. I dodaje, że świat połączonych technologii niesie ze sobą także zagrożenia.

Ataki hakerów powodują bardzo duże straty dla przedsiębiorstw. 27% badanych firm przyznało, że średni czas usunięcia wirusów wynosi 10 dni, a średni koszt wynosi ok 0,5 mln zł. Analitycy Check Point podkreślają, że z roku na rok rośnie zagrożenie i liczba ataków. Obecnie w 84% badanych firm znaleziono złośliwe oprogramowanie w systemach firmowych.