Informacja prasowa Warszawa, 21 listopada 2017 r.

**Hakerzy coraz bardziej niebezpieczni dla polskich firm**

**W 2016 r. 96% polskich firm miało do czynienia z ponad 50 incydentami związanymi z ich danymi i informacjami. Jednocześnie łączne straty firm wygenerowane przez cyberprzestępców w tym okresie na świecie szacowane są na 3 miliardy dolarów. Eksperci wskazują, że liczba przypadków związanych z naruszeniem cyberprzestrzeni polskich firm będzie rosnąć.**

Jak podaje PWC w swoim raporcie „Ochrona biznesu w cyfrowej transformacji”, 35% polskich firm wśród skutków incydentów związanych z ich danymi podaje m.in. straty finansowe. Jednocześnie w raporcie z 2016 r. zespół Cert.Gov.pl tylko w 2015 r. zarejestrował w Polsce 8914 zgłoszeń naruszenia cyberprzestrzeni, które były zakwalifikowane jako incydenty. Według ekspertów liczba ta dynamicznie rośnie.

*Na przestrzeni ostatniego roku obserwujemy wzmożoną aktywność hakerów na terenie naszego kraju, szczególnie tych z Rosji, ale nie tylko. Opinia publiczna otrzymuje jednak informacje tylko o tych najbardziej medialnych przypadkach, jak choćby ostatnie doniesienia o potencjalnym ataku na pracowników Ministerstwa Obrony Narodowej. W rzeczywistości częstotliwość takich incydentów jest znacznie więcej a cyberataki coraz częściej dotyczą podmiotów działających komercyjnie i dotyczą zarówno dużych jak i małych podmiotów gospodarczych. Niestety, zbyt mało polskich firm wzięło sobie do serca historię pewnej znanej firmy prawniczej, która w 2015 r. stała się obiektem szantażu hakerów, którzy grozili ujawnieniem danych jej klientów* - mówi Jarosław Bartniczuk, prezes CyberBlock.

Według szacunków Światowego Forum Ekonomicznego z 2016 r., straty finansowe, jakie poniosą firmy na świecie na skutek ataków cyberprzestępców w 2021 r. mogą wynieść nawet 6 mld dolarów. Jak wskazują eksperci, wzrostowi wysokości strat będzie towarzyszyło obniżenie kosztów przeprowadzenia ataku hakerskiego, co jest kolejnym czynnikiem wpływającym na ich ostateczną liczbę.

*Obecnie koszt przeprowadzenia ataku DDoS, czyli skierowanego przeciwko systemom IT usługom internetowym, paraliżującym ich działanie za pomocą wielu zainfekowanych komputerów, wynosi około 38 dolarów na godzinę. Wraz z rozwojem oprogramowania hakerów, stawka ta będzie spadać. Niestety, cyberprzestępcy są o krok przed administratorami zasobów IT, co wymusza stałe zwiększanie nakładów na zapewnienie swoim organizacjom cyberbezpieczeństwa. Jeżeli przyjmiemy jednak, że, jak donosi w swoim raporcie z 2016 r. Hewlett Packard i Ponemon Institute, realna wysokość strat dla firm wynosi 40 tys. dolarów na godzinę, wydatki te są jak najbardziej uzasadnione* – wskazuje Jarosław Bartniczuk.

*Niestety, mimo że wśród pracowników IT w polskich firmach świadomość zagrożeń ze strony hakerów jest na zadawalającym poziomie, to realne działania przeciwdziałające takim incydentom są niewystarczające. Wiąże to się z niechęcią do zwiększenia kosztów bezpieczeństwa IT oraz przekonaniem zarządzających organizacjami, że ich firmy tego typu incydenty nie będą dotyczyć. Na skutek takich działań managementu, nie tylko w Polsce, cyberprzestępcy z łatwością będą mogli znaleźć słabe ogniwa w systemach zabezpieczeń i bez skrupułów je wykorzystywać.*

*Nie mówimy tu wyłącznie o jakości infrastruktury IT i obejmujących jej procedur, ale również o poziomie wyszkolenia pracowników z innych pionów działających w przedsiębiorstwie. Z doświadczenia wiemy, że ponad 70 % incydentów związanych z cyberbezpieczeństwem w polskich firmach miało miejsce w wyniku nieodpowiedniego zachowania jej pracowników. Mamy nadzieję, że wraz z przygotowaniami do wejścia w życie rozporządzenia RODO, stan ten będzie sukcesywnie ulegał poprawie* – dodaje Jarosław Bartniczuk.

Jak wskazują eksperci, najpopularniejszymi w Polsce formami ataków w cyberprzestrzeni jest phishing i spear phishing. Pierwsza metoda polega na wyłudzeniu od danego użytkownika jego danych osobistych. Obejmuje kradzież haseł, numerów kart kredytowych, danych kont bankowych i innych poufnych informacji. Wiadomości phishingowe najczęściej są fałszywymi powiadomieniami z banków, komunikatami od dostawców systemów e-płatności i innych poważanych organizacji. Wiadomość zawsze próbuje zachęcić odbiorcę pod pretekstem utraty krytycznych danych, awarii systemu do wprowadzenia lub zaktualizowania swoich poufnych informacji. Główne cele phisherów to banki, elektroniczne systemy płatności oraz aukcje internetowe. Spear phishing, czyli atak celowany to mechanizm podobny do zwykłego phishingu, oparty na wysłaniu do ofiary e-mail, który wydaje się pochodzić od zaufanej osoby bądź organizacji. Celem ataku są pojedyncze osoby, wobec których oszust przeprowadza pogłębiony wywiad środowiskowy oparty na informacjach dostępnych w internecie.

O CyberBlock:

Spółka zajmuje się szeroko pojętym cyberbezpieczeństwem. CyberBlock wspiera swoich Klientów na każdym etapie procesu zapewnienia bezpieczeństwa informacji. Swoje działania planuje i prowadzi z wykorzystaniem metod CPM i PERT. Zespół CyberBlock tworzy grupa ekspertów, w skład którego wchodzą informatycy, inżynierzy oraz analitycy, których łączy wieloletnie doświadczenie w obszarze techniki specjalnej i bezpieczeństwa informatycznego.

Więcej informacji:

Grzegorz Ćwiek
mail: g.cwiek@innerlook.pl
tel.: 731 810 571