**Drobne firmy na celowniku cyberprzestępców**

**Miliony bardzo małych firm zatrudniających poniżej 20 pracowników, od gabinetów dentystycznych, doradców finansowych, niezależnych radców prawnych, firm z branży doradztwa IT, skupiają się na swojej podstawowej działalności i wygrywają na takim podejściu.**

Jednocześnie wiele z nich może w ten sposób zaniedbać kwestie bezpieczeństwa IT i narazić na ryzyko swoich klientów oraz przyszłość swojego biznesu. Badanie „2013 Data Breach Investigations Report”1 firmy Verizon zawierające dane pochodzące z ogólnoświatowych dochodzeń kryminalistycznych pokazuje, że spośród 621 przeanalizowanych incydentów naruszenia ochrony danych 193 – ponad 30 procent – miało miejsce w firmach zatrudniających 100 lub mniej pracowników. Eksperci z Kaspersky Lab radzą, jak wyeliminować najczęściej występujące zagrożenia.

Z badania2 przeprowadzonego przez PricewaterhouseCoopers w 2013 r. dla U.K. Department for Business Innovation & Skills wynika, że liczba incydentów naruszenia ochrony danych wzrosła w małych i średnich firmach o 76%. Spośród małych firm, które zostały zaatakowane w zeszłym roku, 15% potwierdziło, że doświadczyło nieautoryzowanego dostępu do swoich danych biznesowych, a 9% przyznało, że padło ofiarą kradzieży własności intelektualnej. Chociaż zyski z włamania się do małej firmy nie są tak wysokie jak w przypadku ataków na duże korporacje, łatwość przeprowadzenia działań cyberprzestępczych na mniejsze organizacje oznacza, że agresorzy mogą po prostu zwiększyć liczbę ataków w celu uzyskania większych przychodów.

Konsekwencje zaniedbania kwestii bezpieczeństwa mogą okazać się tragiczne dla małych firm. Częstym celem cyberprzestępców są firmy, które świadczą usługi finansowe lub związane z ochroną zdrowia. W obu tych sektorach klienci powierzają firmom ogromną ilość poufnych informacji – dokumentację medyczną, dane bankowe i dotyczące płatności oraz inne poufne informacje. W przypadku dostawców usług finansowych i związanych z ochroną zdrowia konsekwencje takich ataków są liczne i obejmują uszczerbek na reputacji oraz utratę rozgniewanych lub zaniepokojonych klientów, jak również awarię sieci komputerowej, która osłabia możliwości działania firmy. Innym problemem małych firm z tych sektorów są potencjalne sprawy sądowe i wysokie grzywny w przypadku, gdy incydent naruszenia ochrony danych stanowił pogwałcenie przepisów.

**Branża usług finansowych pod oblężeniem cyberprzestępców**

Według PricewaterhouseCoopers cyberprzestępczość stała się drugim, zaraz po defraudacji aktywów, najbardziej rozpowszechnionym rodzajem przestępstwa gospodarczego, którego celem padają firmy oferujące usługi finansowe. Chociaż instytucje finansowe czerpią korzyści z wymogów regulacyjnych i przepisów branżowych mających na celu ochronę danych klientów, drobni dostawcy usług finansowych mają związane ręce z powodu ograniczonego budżetu i braku doświadczenia w zakresie ochrony informacji swoich klientów. Jeśli dodamy do tego wymagania dostępu online i wygody, jakie posiada większość klientów, pojawia się spore wyzwanie, z którym firmy muszą się zmierzyć. Organizacje te stanowią oczywisty cel cyberprzestępców, którzy próbują ukraść przechowywane informacje dotyczące karty kredytowej, dane uwierzytelniające i dane dotyczące kont bankowych klientów.

Zdobycie dużego klienta stanowi kamień milowy dla każdej rozwijającej się firmy. W przypadku drobnych dostawców usług finansowych prowadzenie podatków lokalnego sklepu spożywczego lub pomoc w obsłudze płac lokalnym organizacjom charytatywnym świadczy o rozwoju i wiele podmiotów chwali się na swojej stronie internetowej takimi klientami. Jednak cyberprzestępcy mogą widzieć w tym sposobność zaatakowania małej firmy, aby poprzez nią zdobyć dostęp do większych klientów.

**Jaką wartość mają dla cyberprzestępców dostawcy usług związanych z ochroną zdrowia**

Dokumenty finansowe, jakkolwiek niezwykle poufne, nie mogą równać się z dokumentacją medyczną, często przechowywaną w małych gabinetach lekarskich, dentystycznych oraz innych niezależnych dostawców usług związanych ze służbą zdrowia. Incydent złamania zabezpieczeń IT w tych organizacjach spowoduje nie tylko naruszenie poufności danych pacjenta, ale bez wątpienia podważy również zaufanie wszystkich klientów.

Cyberprzestępcy mają wyraźny interes w atakowaniu organizacji z tego sektora. Badanie z 2012 r. opublikowane przez Ponemon Institute3 pokazuje, że 94% szpitali w Stanach Zjednoczonych doświadczyło w ciągu minionych dwóch lat przynajmniej jednego incydentu naruszenia poufności danych. Jednak cyberprzestępcy zwykle nie są zainteresowani dokumentacją dotyczącą ciśnienia krwi pacjenta czy przyjmowanych przez niego leków... chcą ich pieniędzy. Z raportu wynika, że skradzione informacje w większości obejmowały rachunki wystawiane pacjentom oraz informacje dotyczące ubezpieczenia. Kradzież tożsamości, również w celu zagarnięcia pieniędzy, to częsta konsekwencja takich incydentów.

Chociaż drobni dostawcy usług związanych z ochroną zdrowia nie mają do czynienia z tak dużą ilością informacji o pacjentach jak w przypadku większych szpitali, zmieniający się charakter dokumentacji dotyczącej zdrowia pacjentów oznacza, że jest ona podatna na zagrożenia. Dokumentacja medyczna w coraz większym stopniu ulega cyfryzacji, a przez to może zostać łatwo przeniesiona na laptopy i urządzenia mobilne, takie jak smartfony i tablety. To oznacza, że oprócz rozwiązania problemu infekcji komputerów przez wyrafinowane szkodliwe oprogramowanie bardzo małe firmy muszą również podjąć wysiłki, aby przenośne komputery i urządzenia mobilne zawierające karty pacjenta nie padły ofiarą fizycznej kradzieży.

**Co należy zrobić – kilka porad od ekspertów z Kaspersky Lab**

Małe firmy wszelkiego rodzaju, a szczególnie dostawcy usług finansowych i związanych z ochroną zdrowia, muszą zrozumieć, że przechowywane przez nie dane mogą pozwolić na zidentyfikowanie tożsamości ich klientów (np. nazwisko, adres, numer telefonu itd.); informacji dotyczących stanu zdrowia i wielu innych aspektów (numery kart kredytowych, kody weryfikacyjne, adresy wystawienia faktury i wysyłki, historia zakupów, zachowania konsumenckie itd.).

Eksperci z Kaspersky Lab zalecają drobnym dostawcom usług finansowych i związanych z ochroną zdrowia stosowanie ograniczonej liczby urządzeń mobilnych do celów biznesowych. Wprawdzie smartfony i tablety oferują pewną wygodę i stałą dostępność, niosą jednak ze sobą wiele nowych zagrożeń. Jeżeli jakiekolwiek urządzenia przenośne są wykorzystywane do celów biznesowych, muszą być wyposażone w funkcje ochrony przed kradzieżą, które umożliwiają zdalne zablokowanie zgubionego urządzenia i wyczyszczenie znajdujących się na nim danych.

Ważnym elementem zapewniania bezpieczeństwa poufnym informacjom jest również szyfrowanie danych. Szyfrowanie stanowi istotną technologię nie tylko w przypadku urządzeń mobilnych – powinno być także wykorzystywane na komputerach stacjonarnych i laptopach, jak również serwerach plików. Bardzo małe firmy znajdą technologię szyfrowania w rozwiązaniach bezpieczeństwa takich jak [Kaspersky Small Office Security](http://www.kaspersky.pl/kaspersky_small_office_security), które ułatwia zablokowanie dostępu cyberprzestępców do poufnych danych. Ponadto, właściwie zaszyfrowane dane zapewnią ochronę przed przypadkowym usunięciem oraz nieautoryzowanym dostępem uzyskanym przez pracownika.

W przypadku każdej firmy zapewnienie bezpieczeństwa IT zaczyna się od ochrony przed szkodliwym oprogramowaniem oraz narzędzi wykrywania proaktywnego, które można znaleźć w Kaspersky Small Office Security. Kolejnym łatwym sposobem na poprawienie ochrony jest wdrożenie wśród pracowników rygorystycznej dyscypliny dotyczącej haseł. Skutecznym sposobem wprowadzenia dobrych praktyk w tym zakresie jest stosowanie menadżera haseł, który przechowuje wszystkie hasła pracowników w zaszyfrowanych magazynach, dzięki czemu pracownicy muszą pamiętać tylko jedno „hasło główne”.

Małe firmy, niezależnie od rodzaju prowadzonej działalności, stanowią istotny cel dla cyberprzestępców – im cenniejsze dane posiadają, tym częściej są atakowane. Jedno niedopatrzenie właściciela firmy lub zła decyzja pracownika mogą skutkować włamaniem, które doprowadzi firmę do ruiny, a przy tak wielu cennych danych, które można ukraść, możemy przyjąć, że cyberprzestępcy, jak wszyscy złodzieje, nadal będą atakować cele, które uważają za najsłabsze i najłatwiejsze.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.

Wszystkie informacje prasowe Kaspersky Lab Polska są dostępne na stronie <http://www.kaspersky.pl/news>

1 Verizon’s 2013 Data Breach Investigations Report

2 DBIS(UK)/PWC Information Security Breaches Survey (2013)

3 Third Annual Benchmark Study on Patient Privacy & Data Security by Ponemon Institute, badanie sponsorowane przez ID Experts®, grudzień 2012