**Małe firmy podejmują duże ryzyko, nie przywiązując wagi do strategii IT**

**Według badania Kaspersky Lab obejmującego firmy na całym świecie tylko 19% bardzo małych firm, posiadających mniej niż 25 pracowników, traktuje strategię IT jako kluczową kwestię biznesową.**

Dla porównania, w przypadku firm zatrudniających więcej niż 100 pracowników odsetek ten wynosił 30%, a wśród organizacji zatrudniających co najmniej 5 000 osób – 35%. Niepokojące jest to, że ta często zaniedbywana kategoria biznesowa obejmuje polityki dotyczące bezpieczeństwa internetowego i poufności danych.

Wyniki badania, przedstawione w [raporcie podsumowującym 2014 IT Security Risks](http://media.kaspersky.com/en/IT_Security_Risks_Survey_2014_Global_report.pdf) opracowanym przez Kaspersky Lab, wskazują na kluczowe wyzwanie dla bardzo małych firm. Skuteczna strategia IT stanowi istotny element każdej odnoszącej sukcesy firmy i, jeśli jest odpowiednio zarządzana, może sprawić, że mały biznes osiągnie wiele. W rzeczywistości jednak bardzo małe firmy, które w wielu przypadkach muszą skupiać się na walce o ugruntowanie swojej pozycji, najczęściej nie posiadają pieniędzy i wiedzy, aby odpowiednio zaimplementować istotne elementy infrastruktury IT, takie jak oprogramowanie bezpieczeństwa. Właściciel nowej firmy prawdopodobnie zaangażuje wszystkie swoje zasoby w rozwinięcie sprzedaży swojego głównego produktu lub usługi, ponieważ inwestowanie w infrastrukturę biznesową nie ma sensu, jeśli sam biznes kuleje. W którym zatem momencie bardzo mała firma powinna zacząć budować plan IT oraz bezpieczeństwa na przyszłość i jakie są potencjalne konsekwencje zwlekania zbyt długo?

**Konsekwencje cyberprzestępczości**

Według szacunków IDC na całym świecie działa około 80 milionów firm zatrudniających mniej niż 10 osób. Wiele z tych firm wykazuje postawę „bezpieczeństwo przez niewidoczność”, uważając, że są za małe, aby stały się celem cyberprzestępców, i nie posiadają żadnych danych, które mogłyby ich zainteresować. Jednak z raportu [Verizon: 2013 Data Breach Investigations Report](http://www.verizonenterprise.com/DBIR/2013/), który obejmuje dane z dochodzeń śledczych na całym świecie, wynika, że na 621 przeanalizowanych przypadków naruszenia bezpieczeństwa danych **193 incydentów – ponad 30% - miało miejsce w firmach zatrudniających 100** (1) lub mniej osób. Można więc rozsądnie założyć, że bardzo małe firmy stanowią znaczną część takich ofiar.

Właściciele firm muszą zrozumieć, że gdy przetwarzają płatności przy użyciu kart kredytowych, przechowują informacje klientów, czy nawet tworzą plany nowych produktów, znajdują się w posiadaniu informacji, które mają wartość dla cyberprzestępców. Co więcej, niektórzy cyberprzestępcy mogą preferować takie „miękkie cele”, które posiadają słabą ochronę IT. Korzyści, jakie otrzymują z każdej zaatakowanej ofiary, są mniejsze, z drugiej strony jednak, przeprowadzenie skutecznego ataku na wiele bardzo małych firm zamiast na jedną dużą może wymagać mniej wysiłku. Jednak kluczowa różnica polega na tym, że większe firmy będą posiadały środki, aby stanąć na nogi po incydencie naruszenia bezpieczeństwa IT. W przypadku małych firm koszty utraconych danych klientów, długi czas pozostawania odciętym od Sieci oraz związane z atakiem koszty „sprzątania” mogą wynieść tysiące dolarów w zależności od rodzaju incydentu, co wystarczy, aby doprowadzić je do poważnych problemów finansowych.

**Dodatkowe wyniki dotyczące bardzo małych firm**

Według badania firmy Kaspersky Lab **bardzo małe firmy rozumieją niebezpieczeństwo związane z zagrożeniami online**. 35% bardzo małych firm umieściło w pierwszej trójce najważniejszych spraw związanych z IT firmy ochronę danych – jest to najwyższy wynik we wszystkich segmentach biznesowych (w przypadku średnich firm odsetek ten wyniósł 26%, a dla korporacji – 29%). Równie istotną kwestią było dla bardzo małych firm zapewnienie ciągłości działania krytycznych systemów. Wyraźnie widać, że bardzo małe firmy mają świadomość, że ich strategia IT odgrywa istotną rolę w ochronie poufnych danych oraz zabezpieczeniu ich codziennych operacji biznesowych przed szkodliwym oprogramowaniem i cyberprzestępcami.

Ponadto, bardzo małe firmy doskonale orientują się w korzyściach - oraz zagrożeniach dla bezpieczeństwa – jakie zapewnia wykorzystywanie **urządzeń mobilnych w firmach**. 34% bardzo małych firm przyznało, że zintegrowało urządzenia mobilne z systemami IT w ciągu minionych 12 miesięcy – odsetek adaptacji niemal identyczny jak w przypadku dużych firm (na korzystanie z urządzeń mobilnych wskazało 32% dużych firm oraz 35% korporacji). Co więcej, 31% bardzo małych firm określiło zabezpieczenie mobilnych/przenośnych urządzeń komputerowych jako jeden z ich trzech najważniejszych priorytetów w zakresie bezpieczeństwa IT na następne 12 miesięcy. Dane te przeczą wszelkim twierdzeniom, według których bardzo małe firmy w mniejszym stopniu niż ich więksi konkurenci zdają sobie sprawę, z jakimi zagrożeniami wiąże się wykorzystywanie urządzeń mobilnych przez pracowników.

**Wnioski i zalecenia**

Wyniki pokazują, że niewielka waga, jaką bardzo małe firmy przywiązują do strategii IT, a tym samym do bezpieczeństwa IT, nie jest spowodowana niską świadomością znaczenia tych kwestii. A zatem, z czego wynika? Logiczny wniosek jest taki, że brak budżetu stanowi największą barierę uniemożliwiającą bardzo małym firmom stosowanie bardziej zaawansowanych środków IT, w tym rozwiązań bezpieczeństwa. Dlatego Kaspersky Lab zaleca bardzo małym firmom zainwestowanie w środki ochrony, które zapewnią im możliwie natychmiastową ochronę przed zagrożeniami, na jakie są narażone. Według badania obejmującego bardzo małe firmy, spośród respondentów, którzy wskazali na utratę danych biznesowych na skutek cyberataku, **32% przyznało, że przyczyną najpoważniejszego incydentu było szkodliwe oprogramowanie**. Inne istotne źródło utraty danych przez bardzo małe firmy stanowiły **luki w zabezpieczeniach szkodliwego oprogramowania, wskazane przez 9% bardzo małych firm** – prawie tyle samo (8%) wynosi globalna średnia dla wszystkich badanych przedsiębiorstw, niezależnie od rozmiaru. To oznacza, że luki w zabezpieczeniach oprogramowania stanowią problem bezpieczeństwa, który dotyka w równym stopniu niemal wszystkie firmy niezależnie od rozmiaru.

Wobec powyższych faktów Kaspersky Lab zaleca bardzo małym firmom rozważenie zainwestowania w oprogramowanie takie jak [Kaspersky Small Of fice Security](http://www.kaspersky.pl/ksos). Rozwiązanie to zawiera technologie klasy biznesowej w formie, która nie wymaga wiedzy IT w celu jego instalacji i obsługi. Produkt zapewnia skuteczne wykrywanie szkodliwych programów oraz luk w oprogramowaniu, co umożliwia błyskawiczne zidentyfikowanie firmowych komputerów, które mogą zostać wykorzystane przez cyberprzestępców. Kaspersky Small Office Security oferuje również ochronę przed kradzieżą urządzeń mobilnych, które w szybkim tempie są wprowadzane do bardzo małych firm, jak również narzędzia szyfrowania danych, które pozwalają zabezpieczyć dane klientów przed kradzieżą lub przypadkowym usunięciem.

(1) jednostka analizy śledczej Verizon Communications Inc.

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>.