**Bezpieczeństwo start-upów i bardzo małych firm – element planu, nie dodatek**

**Gdy przedsiębiorcy decydują się założyć własną działalność, niemal całkowicie koncentrują się na swoim produkcie czy usłudze oraz na tym, jak mogą zyskać klientów.**

Pozostały czas poświęcają na zajmowanie się logistyką biznesu obejmującą znalezienie powierzchni biurowej lub produkcyjnej, wypełnianie formularzy rejestracji działalności dla potrzeb podatkowych, zainwestowanie w komputery dla pracowników itd. Jednym z aspektów, który jest zwykle pomijany w tym gorączkowym okresie, jest bezpieczeństwo IT. Eksperci z Kaspersky Lab radzą, jak postępować, by skuteczna ochrona nie wchodziła w drogę rozwojowi firmy.

Gdy bardzo mała firma w końcu zajmuje się kwestiami bezpieczeństwa IT, zwykle następuje to albo wtedy, gdy padnie ofiarą cyberprzestępców, albo dlatego, że właściciel firmy trafił na informację dotyczącą szkodliwego oprogramowania kradnącego dane kart. Bezpieczeństwo IT staje się wtedy palącą kwestią, a pracownicy mozolnie poszukują odpowiedniego rozwiązania. Ponadto, jeżeli mała firma czeka, aż infekcja szkodliwym oprogramowaniem zmusi ją, aby zajęła się problemem bezpieczeństwa, może okazać się, że jest już za późno. Jeżeli w wyniku takiego incydentu konieczne będzie zamknięcie firmy lub jej właściwe działanie przez jeden dzień czy dwa będzie niemożliwe, utracone możliwości zysków oraz koszty usunięcia infekcji mogą wynieść nawet dziesiątki tysięcy dolarów. W wielu przypadkach to wystarczy, aby doprowadzić firmę do bankructwa – nie wspominając nawet o zrujnowanej reputacji, gdy dojdzie do wycieku danych klientów.

Poprzez uwzględnienie podstawowych środków bezpieczeństwa IT w planie przedsiębiorstwa rozpoczynającego działalność, przedsiębiorcy mogą oszczędzić wiele czasu, pieniędzy oraz irytacji i zabezpieczyć się przed szkodliwym oprogramowaniem, które mogłoby wyrządzić wystarczająco duże szkody, aby doprowadzić do zamknięcia firmy. Eksperci z Kaspersky Lab przedstawiają kilka wskazówek, jak skonfigurować po raz pierwszy sieć IT bardzo małej firmy, która posiada mniej niż 25 pracowników. Istotne znaczenie ma edukacja pracowników, natomiast specjalne produkty, takie jak [Kaspersky Small Office Security](http://kaspersky.pl/chron-moj-biznes), stworzone po to, aby spełnić potrzeby bardzo małych firm, domyślnie uwzględniają większość z przedstawionych sugestii i ułatwiają założenie nowej firmy, a także prowadzenie jej w sposób bezpieczny.

**Krok 1: Przeprowadzaj inwentaryzację.**

Nowe firmy z pewnością nie będą posiadały wewnętrznego eksperta IT, ale przynajmniej ich zasoby IT są wystarczająco niewielkie, aby można było nimi stosunkowo łatwo zarządzać. Zrób w dowolnym arkuszu kalkulacyjnym prostą listę obejmującą wszystkie laptopy i stacje robocze, jak również serwery i routery znajdujące się na wyposażeniu firmy. Lista ta powinna zawierać również notatki dotyczące wszystkich krytycznych dla działalności aplikacji wykorzystywanych na każdej maszynie.

**Krok 2: Wyznacz priorytety.**

Do nowej listy sprzętu i aplikacji dodaj notatki, aby określić zadania wykonywane na poszczególnych maszynach oraz wskazać, w jakim stopniu Twoje operacje biznesowe zależą od poszczególnych zadań. Sprzęt IT o największym znaczeniu przydziel do „kategorii 1”, natomiast maszyny, które wykonują mniej krytyczne funkcje – do „kategorii 2” a nawet „kategorii 3”. Na przykład, jeżeli firma prowadzi głównie sprzedaż przez internet, serwer pocztowy będzie należał do sprzętu z kategorii 1. W przypadku działalności posiadających fizyczną lokalizację, komputer obsługujący kasę zostanie przydzielony do kategorii 1. Optymalnie do kategorii 1 powinna należeć nie więcej niż połowa wszystkich komputerów w firmie. Celem tego kroku jest zwiększenie wewnętrznej świadomości odnośnie posiadanych komputerów i programów, od których zależy funkcjonowanie firmy, oraz ewidencjonowanie wszelkich przyszłych dodatków lub zmian. Jeżeli problemem jest niski budżet, należy zadbać, aby sprzęt z kategorii 1 był traktowany priorytetowo pod względem wydatków.

**Krok 3: Chroń granicę sieci.**

Podstawowy krok, którego nie wolno pominąć – zadbaj o to, aby firma posiadała włączoną zaporę sieciową, która może zablokować szkodliwy ruch i uniemożliwić złodziejom wyprowadzenie danych poza Twoją sieć. W przypadku wielu małych firm zapora sieciowa będzie stanowiła element routera internetowego. Biorąc to pod uwagę, właściciele firm powinni skontaktować się ze swoim dostawcą usług internetowych i upewnić się, że zapora została odpowiednio skonfigurowana.

**Krok 4: Chroń swoje dane tam, gdzie się znajdują – serwer plików.**

Gdy firma zatrudnia kilka osób pracujących nad tymi samymi dokumentami, warto zainwestować w niewielki serwer plików umożliwiający pracę grupową lub komputer wykorzystywany wyłącznie do przechowywania danych, tak aby informacje były scentralizowane i dostępne dla wszystkich. Jeśli jednak wszystkie dane znajdują się na serwerze plików, nabiera on krytycznego znaczenia i wymaga niezawodnej ochrony przed szkodliwym oprogramowaniem. Istotne jest również wykonywanie kopii zapasowych – w tym celu należy zdefiniować zadanie codziennego automatycznego wykonywania backupu. Kopie zapasowe można zapisać na serwerze plików, innym zewnętrznym dysku twardym lub w systemie przechowywania danych w chmurze. Poświęcenie czasu na skonfigurowanie zadania wykonywania automatycznych kopii zapasowych każdego dnia może uratować firmę w przypadku potencjalnej awarii IT.

**Krok 5: Chroń swoje komputery PC...**

Komputery wykorzystywane przez pracowników umożliwiają prowadzenie biznesu, dlatego właściciele powinni odpowiednio zadbać o ich ochronę. Współczesne szkodliwe oprogramowanie może ewoluować w ciągu kilku godzin, aby obejść proste skanery antywirusowe, dlatego właściciele firm powinni postarać się o wszechstronny pakiet bezpieczeństwa zapewniający wiele poziomów ochrony. Powinien on obejmować takie funkcje jak wykrywanie proaktywne oraz kontrola aplikacji. Warto również zainstalować na komputerach pracowników program do zarządzania hasłami, który przechowuje je w zaszyfrowanym magazynie i automatycznie wprowadza tam, gdzie jest to wymagane. Jest to o wiele lepsza opcja niż zapisywanie haseł firmowych na kartce przechowywanej obok komputera.

**Krok 6: …oraz komputery Mac i urządzenia z Androidem.**

Jeżeli w firmie wykorzystywane są komputery z systemem innym niż Windows, strategia bezpieczeństwa firmy także musi je uwzględniać. Warto pamiętać, że komputer Mac wykorzystywany w firmie do projektów graficznych również będzie potrzebował zapory sieciowej. Rozsądnym działaniem jest także zainstalowanie oprogramowania bezpieczeństwa na komputerze Mac, ponieważ maszyny te mogą stać się „przechowalnią” szkodliwego oprogramowania dla komputerów z systemem Windows i rozprzestrzeniać infekcje w całym biurze lub, co gorsza, na komputery klientów. Ponadto, jeżeli pracownicy planują uzyskiwać dostęp do dokumentów biznesowych ze swoich smartfonów lub nosić dokumenty ze sobą na swoich tabletach, należy wyposażyć takie urządzenia w program do ochrony przed szkodliwymi programami oraz kradzieżą. W ten sposób, jeżeli telefon kiedykolwiek zginie, pracownicy będą mogli zdalnie usunąć z niego informacje krytyczne informacje firmowe.

**Krok 7: Monitoruj wszystko centralnie.**

Obecnie podstawowa ochrona IT jest lokowana na granicy sieci firmy, serwerze plików oraz urządzeniach punktów końcowych – zatem w jaki sposób właściciel firmy jest w stanie monitorować to wszystko? Idealnie byłoby, gdyby pełną ochronę zapewniało jedno rozwiązanie bezpieczeństwa – takie jak Kaspersky Small Office Security – które chroni wszystkie składniki firmy i umożliwia właścicielom wgląd w status bezpieczeństwa oraz informacje dotyczące licencji na produkty dla każdej maszyny w biurze – a wszystko to z jednego pulpitu.

Kaspersky Small Office Security oferuje również zaporę sieciową, funkcję menedżera haseł, ochronę serwerów plików oraz szyfrowanie danych i pozwala właścicielom egzekwować polityki korzystania z sieci z poziomu prostego menu. Wystarczy kilka kliknięć myszki, aby właściciel uniemożliwił pracownikom dostęp do portali społecznościowych na maszynach firmowych... i nie jest potrzebny do tego żaden dyplom potwierdzający zaawansowaną wiedzę z dziedziny IT. Dodatkowo, Kaspersky Small Office Security zawiera pakiet bezpieczeństwa dla smartfonów i tabletów z systemem Android.

Pamiętaj - złożoność jest wrogiem bezpieczeństwa, dlatego jeżeli możesz stosować jedno wszechstronne rozwiązanie przeznaczone do ochrony, Twoje życie stanie się mniej skomplikowane, a zarazem bezpieczniejsze.

Mając wszystkie podstawowe elementy ochrony w jednym rozwiązaniu, firma nie będzie musiała gorączkowo „kompletować” bezpieczeństwa IT w miarę rozwoju swojej działalności. Co ważniejsze, właściciele firm będą mieć pewność, że praca ich życia i dane klientów są chronione, i będą mogli znów skoncentrować się na swoim biznesie.

Więcej informacji o bezpieczeństwie małych firm zawiera przygotowana przez ekspertów z Kaspersky Lab strona <http://kaspersky.pl/chron-moj-biznes>.

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>.