Lekceważenie ryzyka informatycznego może słono kosztować. Przedsiębiorcy pochłonięci prowadzeniem biznesu rzadko myślą o zagrożeniach, tymczasem lista czynników ryzyka IT wydłuża się z każdym rokiem. Na co więc warto zwracać uwagę, by uchronić się przed niespodziewanymi stratami i kosztami?

Pentacomp Systemy Informatyczne SA. opracował listę czynników ryzyka informatycznego, które najczęściej występują w prowadzeniu działalności gospodarczej. „Przedsiębiorcy, szczególnie w sektorze MSP, rzadko zdają sobie sprawę z zagrożeń związanych z informatyką, ich źródła, skali i potencjalnych konsekwencji stania się ich ofiarą. Nasuwa się porównanie do kierowców jeżdżących z zamkniętymi oczami bez żadnego ubezpieczenia. Tymczasem przeciwdziałanie ryzyku, choć wiąże się z ponoszeniem dodatkowych kosztów, pozwala wielokrotnie ograniczyć straty, na jakie naraża się niezabezpieczona organizacja." – wyjaśnia Maciej Majewski, Prezes Zarządu w Pentacomp SA.

Na co przedsiębiorcy powinni zwracać szczególną uwagę? Zaczniemy od obszarów szczególnie zaniedbanych.

1. Uwierzytelnianie i autoryzacja - czyli pozostawianie klucza w drzwiach
Obecnie zasoby danych przetwarzane w systemach informatycznych stanowią kluczową wartość zdecydowanej większości organizacji. Jakość usług uwierzytelniania, autoryzacji i zarządzania dostępem użytkowników do systemów w dużej mierze wpływa na bezpieczeństwo informacji. W obszarze tym najczęściej popełniane błędy dotyczą złej polityki haseł, stosowania „słabych haseł" oraz braku silnego dwuskładnikowego uwierzytelniania. Zdarzają się przypadki współdzielenia haseł i kont przez użytkowników. Wiele firm w ogóle nie przywiązuje wagi do uwrażliwiania swoich pracowników na stosowanie haseł dostępu do zasobów cyfrowych firmy. Częstym przykładem zaniedbania jest niezmienianie loginów i haseł nawet od momentu wdrożenia oprogramowania.

Niestosowanie przez firmę konsekwentnej polityki haseł naraża ją, w najlepszym przypadku, na wyciek poufnych informacji (który z przedsiębiorców chciałby pokazać swoim konkurentom własne oferty, historie kontaktów z klientami czy wewnętrzne materiały o produktach?), w najgorszym zaś, na utratę zasobów informacji (czy wyobrażają sobie Państwo, że np. osoba odchodząca z pracy może bez trudu wykasować dane firmowe z serwera, do którego ma dostęp nawet po odejściu z pracy?). Zdrowy rozsądek nakazuje by w drzwiach nie tylko instalować zamki ale by po zamknięciu wyjmować z zamka klucz.

2. Zarządzanie dostępem - czyli kto może mieć klucze do kasy
Stawianie na lojalność wszystkich pracowników połączona z ufnością, że dane gromadzone na dyskach użytkowników i serwerach zamkniętych w serwerowni nie zostaną naruszone choćby w wyniku złej woli, to oczywisty mit. Przekonanie o bezpieczeństwie danych bez stosowania odpowiednich zabezpieczeń prowadzi najczęściej do rozluźnienia polityki zarządzania dostępem do zasobów informacyjnych, a w skrajnych przypadkach do całkowitego zlekceważenia takiej potrzeby. Brak polityki zarządzania uprawnieniami, która pozwoliłaby nadzorować nadawanie/odbieranie uprawnień, zwłaszcza w sytuacjach zmian personalnych to rodzaj zaproszenia pracowników do nadużyć. Podobnie błędem jest nadawanie nadmiarowych uprawnień użytkownikom. Błędy i zaniechania w tym obszarze to nie tylko ryzyko wycieku danych na zewnątrz firmy – to przede wszystkim ryzyko konsekwencji posiadania danych poufnych przez nieuprawnionych pracowników. Wyobraźmy sobie, że pracownicy uzyskują przypadkiem dostęp do informacji o poziomie wynagrodzeń w całej firmie, do wyników ocen pracowniczych lub treści notatek członków zarządu. To tak jakby zamienić pomieszczenie, w którym przechowujemy pieniądze, w stołówkę samoobsługową.

3. Backup - czyli jak odzyskać utracone dane
O kopiach zapasowych danych z reguły nikt nie pamięta, dopóki nie są nagle potrzebne. System backupowania i odzyskiwania danych powinien obejmować wszystkie systemy organizacji. Ważne jest określenie właściwej częstotliwości tworzenia kopii oraz czasu ich przechowywania. Ze względów bezpieczeństwa backupy warto przechowywać w osobnej lokalizacji. W firmach, w których systemy operacyjne odgrywają strategiczną rolę, warto

testować scenariusz odzyskiwania danych oraz postępowania w przypadku awarii systemu, tak aby proces odzyskania danych nie zahamował pracy organizacji. Te same firmy powinny także zadbać o wprowadzenie planu ciągłości działania IT, szczególnie komponentów o kluczowym znaczeniu dla firmy (np. serwery, systemy sprzedażowe itp.).

4. Urządzenia mobilne - czyli w pracy tak jak w domu
Jednym z wyrazów rozwoju technologii jest rosnąca popularność urządzeń mobilnych i coraz powszechniejsze wykorzystywanie ich do pracy. Częstym źródłem ryzyka jest wykorzystywanie do pracy urządzeń prywatnych, które nierzadko nie są objęte szczelnym systemem ochrony. W tym obszarze często popełniane błędy to brak szyfrowania danych, niedostatecznie zabezpieczony dostęp urządzeń mobilnych do zasobów firmy, niestosowanie narzędzi do bezpiecznej komunikacji oraz brak zarządzania konfiguracją urządzeń. Wprawdzie tego trendu zwanego konsumeryzacją nie sposób jest powstrzymać, ale poprzez odpowiednią konfiguracje zabezpieczeń można ograniczyć podatność na ataki, wyciek informacji wrażliwych oraz negatywne ich konsekwencje.

5. Licencjonowanie, czyli „uniezależnienie" od producenta
Bezpieczeństwo informatyczne w dłuższym terminie zależy od tego, czy dostawca użytkowanego oprogramowania zapewnia jego aktualizowanie np. pod kątem zmieniających się przepisów, rozwoju organizacji lub rozwoju technologicznego. Opieranie się wyłącznie na systemach dostarczanych przez jednego producenta może być ryzykowne, szczególnie jeśli nie zapewnia on jasnej polityki wspierania swoich klientów. Równie ważne jest zarządzanie licencjami – ustalenie standardów oprogramowania, korzystanie wyłącznie z licencjonowanego i odpowiednio zainstalowanego oprogramowania oraz okresowa kontrola ważności licencji.

6. Systemy zabezpieczone przed atakami - czyli bezsenność w Seattle
Dla zdecydowanej większości przedsiębiorców polityka bezpieczeństwa kojarzy się z oprogramowaniem antywirusowym i firewall. Zabezpieczanie stacji roboczych przed potencjalnymi atakami z zewnątrz jest oczywiste, jednak już zabezpieczanie serwerów i użytkowanych aplikacji webowych już nie zawsze. System obrony przed atakami z zewnątrz powinien być zorganizowany kompleksowo – obejmować wszystkie komputery, serwery i aplikacje, które utrzymują łączność z Internetem. Szczególnie ważne jest regularne monitorowanie zabezpieczeń oraz dobór oprogramowania, które nie tylko posiada możliwie najszersze spektrum ochrony (identyfikację zagrożeń), ale też szybko pobiera wszystkie aktualizacje bibliotek zagrożeń. W tym obszarze równie ważne jest wdrożenie w przedsiębiorstwie polityki bezpieczeństwa, która wskazuje sposoby postępowania w przypadku zidentyfikowania zagrożenia, pogłębia świadomość pracowników oraz precyzyjnie określa sposób użytkowania systemów i aplikacji w codziennej pracy oraz w pracy zdalnej.

W wieku Internetu musimy brać pod uwagę nie tylko działania konkurencji ale również fakt, że wśród 7 miliardów ludzi są tacy dewianci, dla których sens życia realizuje się poprzez włamania do serwerów na innym kontynencie. Trzy ostatnie tematy to zarazem tak zwane dobre praktyki. W ich przypadku zaniechanie zwiększa ryzyko, natomiast stosowanie się do nich jest sprawdzonym środkiem na obniżenie poziomu ryzyka.

7. Monitorowanie podatności – czyli auto-testowanie
Kolejny aspekt ryzyka wiąże się z zaniechaniem lub zaniedbywaniem tzw. zarządzania podatnościami. Jest to działanie, które ma na celu skanowanie użytkowanej infrastruktury IT w poszukiwaniu luk i błędów oraz raportowanie i podejmowanie procesu naprawczego. Zarządzanie podatnościami jest bardzo istotne w przypadku korzystania z większej lub mającej charakter rozproszonej infrastruktury IT, pozwala bowiem wielokrotnie ograniczyć potencjalne zagrożenia zarówno w kontekście ataków zewnętrznych, jak i wewnętrznych nadużyć.

8. Polityka bezpieczeństwa – czyli unikanie chaosu
Polityka bezpieczeństwa to kompendium wewnętrznych reguł organizacji, które określa sposób użytkowania infrastruktury IT, uprawnienia pracowników, scenariusze postępowania w obliczu zagrożeń oraz przewidziane sankcje za naruszenie zapisów zawartych w polityce bezpieczeństwa. W bardzo wielu przypadkach firmy w ogóle nie stosują polityki bezpieczeństwa lub co gorsza starają się ją stosować, ale robią to w sposób niewłaściwy. Nieumiejętne wdrażanie polityki bezpieczeństwa – najczęściej spowodowane jej niewłaściwym komunikowaniem, brakiem

konsekwencji lub nieumocowaniem jej na szczeblu zarządu samo w sobie stanowi źródło ryzyka informatycznego.

9. Świadomość zagrożeń – czyli zachowanie należytej staranności
Można powiedzieć, że w zasadzie wszystkie czynniki ryzyka sprowadzają się do kwestii zasadniczej – poziomu świadomości zagrożeń wśród wszystkich pracowników, od zarządu, przez stanowiska kierownicze po pracowników operacyjnych. Budowanie świadomości wpisuje się w działania związane z wdrażaniem polityki bezpieczeństwa, ale ma szerszy wymiar. To odpowiedzialność kadr kierowniczych, które krzewią wśród podwładnych postawy nastawione na ochronę pracodawcy i miejsca pracy. Firmy, które tego nie potrafią, są bardziej narażone na czynniki ryzyka.

Według firmy PwC w 2011 r. aż 37% polskich firm zauważyło wzrost ryzyka cyberprzestępczości. Firma przewiduje, że ryzyko to będzie ciągle rosło, tymczasem, wyniki ankiety „Global Economic Crime 2011" wynika, że kierownictwo ponad 40% firm w Polsce w ogóle nie informowało swoich pracowników o możliwym ryzyku cyberprzestępczości. Warto wziąć to pod uwagę, zanim będzie za późno…

Maciej Majewski, Prezes Zarządu w **Pentacomp SA**
Pentacomp Systemy Informatyczne
www.pentacomp.pl