

Puls Biznesu - 21.11.2007

<http://bonnierbusinesspolska.pb.pl/Issue.aspx?id=26d73cdc-6d04-4a13-bafe-f5960f4d50f8&date=2007-11-21>

Aby e-twierdzą być

Najlepsze praktyki ograniczają zagrożenia

Na bezpieczeństwo informatyczne firmy składają się trzy czynniki — sprzęt, ludzie oraz organizacja.

W świecie współczesnego internetu, gdy hakerzy gotowi są włamać się nawet na serwery Pentagonu, firma powinna przypominać twierdzę. Musi mieć solidne mury, obrońców oraz ustalone plany działania. Mury to hardware i software, obrońcy to pracownicy, plan działania to odpowiednia organizacja pracy. Jeśli firma zadba o te trzy czynniki, może czuć się umiarkowanie bezpieczna. Wbrew pozorom wprowadzenie zmian nie wymaga dużo pracy. Bardzo często przedsiębiorstwa ponoszą straty przez zwykłą głupotę — niezabezpieczona sieć bezprzewodowa, brak programu antywirusowego czy stosowanie tego samego hasła na wszystkich kontach. Jak zadbać o bezpieczeństwo? Zacznijmy od sprzętu.

— W przypadku małych i średnich przedsiębiorstw zasadne wydaje się stosowanie rozwiązań zintegrowanych, skupiających pakiet funkcji w jednym urządzeniu. To z jednej strony znacznie obniża koszty, a z drugiej ułatwia zarządzanie w firmach, w których personel IT nie jest zbyt liczny. Ponadto należy zwrócić uwagę na zabezpieczenie styku komputerów osobistych i serwerów zawierających dane istotne dla firmy z internetem — mówi Marek Szczepański z McAfee, firmy zajmującej się bezpieczeństwem IT.

W przypadku stosowania sieci bezprzewodowych trzeba zainwestować w dodatkowe środki bezpieczeństwa.

— Wysoki standard zabezpieczeń można osiągnąć dzięki zastosowaniu rozwiązań do szyfrowania transmisji, uwierzytelnianiu mobilnych użytkowników oraz skanowaniu sieci — wyjaśnia Tomasz Dzideczek, inżynier systemowy w dziale korporacyjnych rozwiązań mobilnych Motoroli.

Podsumowując, firma powinna mieć firewalle sprzętowe, software'owe, oprogramowanie antywirusowe. Niezbędne są też procedury i urządzenia do tworzenia zapasowych kopii danych. Wydaje się skomplikowane? W praktyce nie jest. Dostawcy oprogramowania oferują produkty zawierające w sobie wszystkie te funkcje, a dostawcy sprzętu produkują bramy dostępu z firewallem.

Zmieniać hasła

Wszystkie te zabezpieczenia na nic się zdadzą, jeśli się z nich nie będzie korzystać. Trzeba do tego przekonać użytkowników. Podobnie jak do kilku innych rzeczy. Kevin Mitnick, najslawniejszy haker, powiedział, że nie łamał haseł, ale ludzi. Miał rację.

— W kwestii blokowania klawiatury czy zostawiania haseł w szufladzie technologia jest bezsilna wobec ludzkiej niefrasobliwości — przyznaje Marek Szczepański.

Żeby się o tym przekonać, wystarczy wykonać eksperyment myślowy, wyobrażając sobie, jak łatwo obcy człowiek mógłby wejść do siedziby firmy i skopiować dane z włączonego komputera, którego użytkownik poszedł np. na kawę lub lunch. Wbrew pozorom do takich incydentów dochodzi. Jak tego uniknąć?

— Można stosować systemowe wymuszanie zmiany haseł co określony czas i o odpowiedniej specyfikacji znaków — radzi Adam Gębski z ZETO Poznań.

Warto pamiętać, żeby hasła zawierały duże i małe litery, cyfry (byle nie cyfrę 1, którą stosuje większość użytkowników) oraz takie znaki, jak %, \$ czy #.

Silna organizacja

Specjaliści zalecają, żeby wewnątrz firmy stworzyć zespół osób odpowiedzialnych za szacowanie ryzyka utraty informacji oraz wdrożenia działań mających to ryzyko obniżyć.

— Brak osób odpowiedzialnych za bezpieczeństwo IT prowadzi do oczywistej sytuacji, gdy osobami odpowiedzialnymi za te sprawy są wszyscy, czyli nikt — mówi Adam Gębski.

Kolejną dobrą radą jest ograniczenie dostępu do informacji. Pracownik powinien mieć dostęp do tych danych, które są mu potrzebne do pracy.

Wojciech Chmielarz