100 tysięcy dolarów dziennie - według najnowszego raportu Ponemon Institute, nawet tyle może kosztować przedsiębiorstwa pojedynczy atak cyberprzestępców.

**Jeden tydzień, 50 ataków, 45 firm**
Najnowszy raport Ponemon Institute, organizacji badawczej na polu bezpieczeństwa IT, przedstawia wyniki analizy przeprowadzonej w 45 dużych przedsiębiorstwach, zatrudniających więcej niż 500 pracowników. Według zebranych statystyk, wszystkie uwzględnione firmy padają ofiarą 50 ataków tygodniowo. Średnio ma miejsce więcej niż jeden atak w tygodniu na pojedynczą firmę. Średnia roczna strata dla każdej z nich to 3,8 miliona dolarów. Niektóre organizacje ponoszą koszty rzędu 52 milionów dolarów rocznie.
„Raport Instytutu Ponemon potwierdza to, z czym na co dzień spotykamy się w pracy z klientami" – mówi Łukasz Nowatkowski z G Data Software, międzynarodowego producenta programów antywirusowych. „Oszczędności na bezpieczeństwie potrafią bardzo szybko zemścić się na przedsiębiorstwach, a pośrednio również na ich klientach. Każda większa organizacja powinna stworzyć etat dla wyższego rangą specjalisty ds. bezpieczeństwa IT. Oprócz posiadania dobrej jakości programów antywirusowych, niezbędne są również odpowiednie szkolenia personelu, a to wszystko w myśl zasady: Najskuteczniejsza strategia obrony to założenie, że już się zostało zaatakowanym."

**Kluczowe wnioski**
Najbardziej niszczycielskie ataki to takie, które przeprowadzane są za pomocą Internetu, ze szczególnym uwzględnieniem złośliwych skryptów ingerujących i zmieniających kod wewnętrznego oprogramowania przedsiębiorstw. Wywołane w ten sposób straty wymagają długotrwałych napraw, a więc i sporego nakładu środków finansowych. Ataki tego typu powodują 90 procent wszystkich kosztów.
Uporanie się z cyberatakami zabiera badanym firmom przeciętnie 42 dni. Każdy taki dzień to koszt około 18 tyś. dolarów. Najwięcej zasobów i czasu pochłania wykrycie i przywrócenie systemu informatycznego do stanu używalności – 46 procent kosztów – przy czym obie te operacje mogę zostać znacznie przyspieszone przez zastosowanie w firmach nowoczesnych technologii do zarządzania zagrożeniami i ryzykiem, np. ETRM (Enterprise Threat and Risk Management) czy SIEM (Security Information and Event Management). Oszczędności z ich zastosowania wynoszą nawet 25 procent ogółu wszystkich kosztów.

**Odpowiedzialność za bezpieczeństwo**
Wyznaczenie kierownika do spraw bezpieczeństwa informatycznego, który przejąłby ogólną odpowiedzialność za bezpieczeństwo IT, opracowanie planu kryzysowego oraz inwestycje w technologie bezpieczeństwa potrafią znacznie zmniejszyć finansowe koszty cyberprzestępczych ataków" – mówi Larry Ponemon, założyciel i przewodniczący Ponemon Institute.

Badanie zostało przeprowadzone w okresie luty-czerwiec 2010. Pod uwagę wzięto taki czynniki, jak: bezpośrednie oraz pośrednie koszty utraty bądź kradzieży informacji, zakłócenia w działaniach firm, poniesione koszty finansowe oraz zniszczenia materialne. Koszty uwzględniały wydatki na wykrycie zagrożeń, badanie i analizę sytuacji oraz przywrócenie do działania systemu informatycznego przedsiębiorstw.

*Źródło: http://www.net-security.org*

**Someday Interactive**