

Walka z ryzykiem IT.

Janusz Grobicki

Analiza ryzyka, według standardowej definicji oznacza określone działania skierowane na obniżenie jego wpływu na funkcjonowanie danego podmiotu.

Tylko rzetelna i dokładnie przeprowadzona analiza może dać podstawę do przygotowania polityki bezpieczeństwa, a tym samym dobranie odpowiednich zabezpieczeń. Zarządzanie informacją to proces powiązany z zarządzaniem bezpieczeństwem systemów informatycznych, definiowanego jako „proces identyfikowania, kontrolowania i minimalizowania ryzyka dotyczącego bezpieczeństwa przy zachowaniu akceptowalnego poziomu kosztów”.

CHRONIĆ INFORMACJE, NIE SYSTEMY

Tworząc politykę bezpieczeństwa instytucji finansowej w obszarze IT, najpierw należy dokonać oceny znaczenia i wartości posiadanych informacji. Trzeba wiedzieć, które informacje są ważne, krytyczne, objęte przymusem ochrony, a które jedynie powinny być chronione. Dopiero na tej podstawie można konstruować politykę bezpieczeństwa dla całej organizacji. Nie można mówić o polityce bezpieczeństwa w obszarze informatycznym, jeżeli nie zostały stworzone odpowiednie dokumenty i procedury dla całej organizacji. Należy dokładnie zidentyfikować te obszary, które mają krytyczne znaczenie z biznesowego punktu widzenia. Należy przyłożyć odpowiednią wagę biznesową do odpowiednich informacji. A także przeanalizować sposoby, które mogą doprowadzić do stracenia poufności, dostępności i integralności informacji. Czyli tych trzech podstawowych cech, które decydują o tym, czy informacja jest bezpieczna, czy też nie. Powinno się również stworzyć hipotetyczną mapę potencjalnych możliwości zaatakowania systemu. Celem polityki bezpieczeństwa jest więc ochrona informacji, a nie systemów informatycznych. Chodzi o to, żeby w razie awarii systemu informacja nadal była dostępna, możliwa do odtworzenia i o nienaruszonej integralności.

AUDYT BEZPIECZEŃSTWA IT

Audyt IT polega na bieżącym pomiarze stanu środowiska w zakresie sposobu przechowywania i ochrony oraz udostępniania informacji w odniesieniu do przyjętego modelu, którego wyrazem jest polityka bezpieczeństwa. Konfiguracja systemu informatycznego powinna wynikać wprost z przyjętej polityki bezpieczeństwa. Drugi element audytu to analiza stanu w odniesieniu do aktualnych zagrożeń.

Adam Gębski - dyrektor Pionu Sprzedaży ZETO SA w Poznaniu

A może polityka bezpieczeństwa?

W polskich firmach najpopularniejszy jest audyt sprawdzający infrastrukturę teleinformatycznej. Analizie poddaje się serwery dostępne, urządzenia sieciowe realizujące połączenia, stacje robocze pracowników etc.

Do ich realizacji wykorzystuje się wyspecjalizowane narzędzia informatyczne. Analiza infrastruktury IT pozwala nie tylko na kompleksowe przeprowadzenie audytów bezpieczeństwa czy sporządzanie inwentaryzacji, ale również na przeanalizowanie sposobu wykorzystania zasobów IT.

Audyt jedno, ale co po nim? Jeżeli firma zastosuje się do zaleceń wynikających z raportu, powinna pomyśleć o wdrożeniu Polityki Bezpieczeństwa Informatycznego, która na stałe obejmie w swoim zakresie bezpieczeństwo fizyczne, bezpieczeństwo systemów i sieci, zarządzanie kopiami zapasowymi, zarządzanie systemami ochrony czy zapewnić ciągłość działania.