Rola czynnika ludzkiego w bezpieczeństwie IT jest całkowicie zaniedbywana

Kategoria: Aktualności
Opublikowano: czwartek, 05, grudzień 2013 23:00
Rafał Rudka

W zeszłym roku 87% organizacji w Europie Wschodniej doświadczyło wewnętrznego incydentu naruszenia bezpieczeństwa informacji, który w części przypadków spowodował utratę poufnych danych - tak wynika z badania Global Corporate IT Security Risks 2013 przeprowadzonego przez Kaspersky Lab wraz z agencją badawczą B2B International. W badaniu ustalono, że trzy najpowszechniejsze rodzaje wewnętrznych zagrożeń to: luki w zabezpieczeniach lub błędy w istniejącym oprogramowaniu, nieumyślne wycieki danych na skutek błędu człowieka oraz utrata lub kradzież urządzeń przenośnych.

Większość firm na świecie zdaje sobie sprawę ze znaczenia środków prewencyjnych w bezpieczeństwie IT i stosuje je w różnym stopniu. W celu zminimalizowania wewnętrznych zagrożeń bezpieczeństwa połowa badanych organizacji posiada rozwiązania, które pozwalają oddzielić sieci krytyczne dla działalności od innych, a 52% stosuje różne poziomy praw dostępu do systemów IT.

Mimo to wiele firm przyznaje, że aktualne środki są niewystarczające, a niektóre z nich stosują nowe rozwiązania bezpieczeństwa, które potrafią egzekwować polityki i zapewnić dodatkową ochronę przed utratą danych. Na przykład, mniej niż połowa badanych firm wykorzystuje kontrolę aplikacji, kontrolę urządzeń lub agenta zapewniającego ochronę przed szkodliwym oprogramowaniem dla urządzeń mobilnych. Jeszcze mniej organizacji wdrożyło rozwiązania pozwalające na zarządzanie urządzeniami mobilnymi (28%) lub szyfrowanie na urządzeniach przenośnych (36%).

Kolejny problem polega na tym, że pracownicy nie zawsze przestrzegają obowiązujących polityk bezpieczeństwa korporacyjnego, a odsetek firm, które jasno przedstawiły sankcje i procedury dyscyplinarne w przypadku naruszenia takich polityk, wynosi jedynie 32%. Co więcej, zaledwie 33% badanych firm uważa, że personel respektuje polityki bezpieczeństwa.

Źródło: Kaspersky Lab