**41% firm traktuje zapobieganie wyciekom danych jako zadanie priorytetowe**

**Wyciek poufnych danych może mieć poważne konsekwencje dla firmy, a w najgorszym przypadku doprowadzić nawet do jej upadku. Wyniki badania przeprowadzonego przez agencję IDC w grudniu 2012 r. pokazują, że wiele firm dostrzega wagę problemu.**

41% firm jest poważnie zaniepokojonych możliwością wycieku danych, a za główny cel stawia sobie zapobieganie takim incydentom. Według IDC, szyfrowanie – jedno z najbardziej skutecznych i niezawodnych narzędzi do ochrony danych – staje się coraz popularniejsze. Eksperci z Kaspersky Lab radzą, jak firmy mogą zmierzyć się z problemem wycieku informacji.

**Cztery powody stosowania technologii szyfrowania**

Mówiąc ogólnie, technologie szyfrowania można podzielić na dwa obozy – szyfrowanie na poziomie pliku i foldera (FLE) oraz szyfrowanie całego dysku (FDE). Za pomocą FLE chronione są określone pliki i foldery, dlatego technologia ta jest odpowiedniejsza do szyfrowania niewielkich ilości poufnych danych. Z kolei FDE szyfruje cały dysk twardy i idealnie nadaje się do ochrony np. laptopów firmowych na wypadek ich utraty lub kradzieży. Ponieważ FLE i FDE rozwiązują różne problemy, większość organizacji woli stosować obie technologie.

Według specjalistów z IDC, można wyróżnić cztery główne powody stosowania technologii szyfrowania:

- ograniczenie dostępu do poufnych informacji oraz ochrona przed nieautoryzowanym dostępem;

- ochrona poufnych plików przed szkodliwym oprogramowaniem i innymi coraz bardziej rozpowszechnionymi cyberzagrożeniami;

- pomoc w zabezpieczeniu danych przed atakami, za pomocą których cyberprzestępcy mogą skutecznie przeniknąć do sieci korporacyjnej – ataki na infrastrukturę firmową oraz próby kradzieży danych stają się coraz bardziej wyrafinowane;

- uzupełnienie procesu zarządzania ryzykiem w firmie - ochrona danych odgrywa tu coraz ważniejszą rolę jako kluczowy element.

Obecnie wydatki związane z szyfrowaniem nie stanowią priorytetu w większości budżetów działów IT. Jednak analitycy z IDC są pewni, że wkrótce szyfrowanie stanie się jedną z najbardziej pożądanych technologii.

Według IDC, popyt na szyfrowanie stacji roboczych zwiększy się o ponad 50% w ciągu kolejnych kilku lat – z 556 milionów dolarów w 2012 roku do 866 milionów w 2016 roku. W 2013 roku koszty ochrony danych po raz pierwszy przekroczą 2 miliardy dolarów, podczas gdy w 2016 roku sięgną ponad 3 miliardów dolarów.

W celu uniemożliwienia nieautoryzowanego dostępu do poufnych informacji nowa platforma korporacyjna Kaspersky Lab - Kaspersky Endpoint Security for Business oferuje obie technologie szyfrowania: FDE oraz FLE. Rozwiązanie zawiera również kilka innych cennych funkcji, łącznie z funkcjami scentralizowanego zarządzania dla technologii szyfrowania za pośrednictwem konsoli administracyjnej Kaspersky Security Center, możliwością ustanowienia ogólnych reguł szyfrowania danych na nośnikach zewnętrznych oraz automatycznym szyfrowaniem plików stworzonych lub zmodyfikowanych przez dowolny program wskazany przez personel IT firmy.

Ze względu na to, że firmy dążą do ograniczania poziomu złożoności infrastruktury IT, Kaspersky Endpoint Security for Business pozwala na wyeliminowanie kilku różnych narzędzi, dostawców i aplikacji poprzez skonsolidowanie wszystkich funkcji w jednej spójnej platformie. W celu zmniejszenia złożoności funkcja szyfrowania została połączona z szerokim wachlarzem innych technologii firmy Kaspersky Lab. Kaspersky Endpoint Security for Business zapewnia ochronę przed szkodliwym oprogramowaniem, spamem, zagrożeniami ukierunkowanymi oraz innymi cyberzagrożeniami, tworząc prawdziwie bezpieczne środowisko, w którym można obsługiwać poufne informacje na wszystkich węzłach infrastruktury firmowej.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.

Wszystkie informacje prasowe Kaspersky Lab Polska są dostępne na stronie http://www.kaspersky.pl/news.