Jak ustrzec się zainfekowania systemu?

Kategoria: Aktualności
Opublikowano: czwartek, 08, sierpień 2013 00:00
Odsłony: 1428

Ograniczanie możliwości uruchamiania aplikacji firm trzecich zwiększa bezpieczeństwo korporacyjnych stacji roboczych oraz wydajność pracowników. Jednak 57 proc. firm nie wykorzystuje żadnych narzędzi do kontroli aplikacji – tak wynika z badania przeprowadzonego w listopadzie 2012 r. przez Kaspersky Lab we współpracy z B2B International.

Cyberprzestępcy stosują wiele sztuczek w celu zainfekowania systemu. Jedną z nich jest ukrywanie szkodliwego oprogramowania pod maską popularnej aplikacji - w ten sposób, gdy pracownik próbuje uruchomić aplikację, zainfekowana może zostać cała infrastruktura firmy.

Aby zapobiec takim incydentom, firmy powinny opracowywać i stosować polityki bezpieczeństwa regulujące głównie kwestię instalacji i uruchamiania aplikacji - nie wszystkie jednak to robią. Według przeprowadzonego badania, większość firm nie stosuje metod kontroli aplikacji, a 17 proc. nie jest zainteresowanych wykorzystywaniem nowych technologii kontroli aplikacji lub wręcz nie jest świadoma ich istnienia.

Sprawa wygląda podobnie w przypadku podłączania zewnętrznych urządzeń i nośników danych: tylko 44 proc. firm zwraca wystarczającą uwagę na tę kwestię i stosuje narzędzia kontroli urządzeń, podczas gdy 17 proc. nie jest świadomych istnienia narzędzi kontroli ani nie jest zainteresowanych wykorzystywaniem ich. Jednocześnie szkodliwe oprogramowanie dystrybuowane za pośrednictwem nośników USB stanowi nieustanne zagrożenie.

Użycie narzędzi kontroli punktów końcowych daje wyraźne korzyści niezależnie od rozmiaru firmy. Kontrola aplikacji oferuje dodatkową ochronę przed szkodliwymi programami i ogranicza możliwość korzystania z programów niezwiązanych z pracą, takich jak gry lub komunikatory internetowe. Kontrola urządzeń zewnętrznych uniemożliwia podłączanie do firmowych komputerów nieautoryzowanego sprzętu, a tym samym zapobiega wyciekowi danych i infekcjom szkodliwych programów rozprzestrzeniających się poprzez wymienne nośniki danych.

Ostatni element układanki – kontrola sieci – pozwala administratorowi całkowicie zablokować lub ograniczyć dostęp do określonych stron WWW. Poza tym, że pracownicy nie będą mogli poświęcać czasu na przeglądanie serwisów, które nie są wykorzystywane w pracy, kontrola sieci zwiększy.

Źródło: Money.pl