Bezpieczeństwo urządzeń mobilnych - przejmij kontrolę lub strać wszystko

Kategoria: Aktualności
Opublikowano: wtorek, 20, sierpień 2013 00:00
Rafał Rudka

Firmy są poważnie zaniepokojone bezpieczeństwem urządzeń mobilnych z dostępem do danych korporacyjnych, ale nadal nie spieszą się ze znalezieniem sposobów kontrolowania ich wykorzystywania. Tak wynika z badania przeprowadzonego przez B2B International i Kaspersky Lab w drugiej połowie 2012 r.

Zastanawiające jest to, że tak palący problem jak bezpieczne wykorzystywanie urządzeń mobilnych w sieciach korporacyjnych został uszeregowany dopiero na trzecim miejscu przez pracowników odpowiedzialnych za krytyczne decyzje biznesowe, w tym te związane z bezpieczeństwem IT. Ponad połowa (55%) tych samych specjalistów biorących udział w badaniu B2B International potwierdziła, że jest poważnie zaniepokojona bezpieczeństwem urządzeń mobilnych.

Eksperci ds. IT i biznesu w firmach zostali poproszeni o zidentyfikowanie trzech zadań, które uważają za najistotniejsze dla swojego personelu informatycznego z punktu widzenia zbudowania bezpiecznej infrastruktury firmowej. Bezpieczeństwo urządzeń mobilnych zostało ocenione stosunkowo nisko – zaledwie 13% badanych zalicza wykorzystywanie systemów do zarządzania urządzeń mobilnych (Mobile Device Management - MDM) do trzech najbardziej krytycznych zadań. Ochronę poufnych informacji wskazało 27%, dzięki czemu zagadnienie to zajęło drugie miejsce wśród najważniejszych zadań. Najistotniejszą kwestią – wskazaną przez 31% badanych - było uniemożliwienie cyberprzestępcom przeniknięcia do sieci korporacyjnej.

Ponieważ cyberprzestępcy szukają przede wszystkim poufnych informacji, należy podjąć wszelkie możliwe działania, aby zapewnić ochronę takich danych. Firmy muszą dzisiaj zdawać sobie sprawę z konieczności tworzenia barier powstrzymujących cyberprzestępców oraz stosować różne skuteczne metody w celu zapewnienia niezbędnej ochrony danych: wykonywanie kopii zapasowych, eliminowanie wycieków danych spowodowanych przez personel, odpieranie cyberataków itd. Niepokojące jest jednak to, że tak wiele firm lekceważy znaczenie technologii MDM, mimo że niemal jedna czwarta (23%) respondentów przyznała się do utraty danych biznesowych na skutek zgubienia lub kradzieży urządzeń mobilnych.

Technologia MDM, taka jak moduł wbudowany w rozwiązanie Kaspersky Endpoint Security for Business, pozwala firmom:

- Stosować ograniczenia odnośnie instalacji i uruchamiania oprogramowania na korporacyjnych urządzeniach mobilnych. Niekontrolowane instalowanie nowych aplikacji przez pracowników może wyrządzić poważną szkodę sieciom korporacyjnym.
- Obsługiwać zdalne zarządzanie smartfonami i tabletami, tak aby w przypadku zgubienia lub kradzieży urządzenia możliwe było zablokowanie dostępu i usunięcie informacji.
- Zabezpieczać urządzenia za pomocą kodów PIN oraz chronić aplikacje mające dostęp do danych korporacyjnych przy użyciu mocnych haseł.
- Szybko i łatwo wdrażać konfigurację poczty e-mail oraz polityki bezpieczeństwa na urządzeniach mobilnych nowych pracowników.
- Zapewnić wykorzystywanie ochrony antywirusowej wysokiej jakości, zwłaszcza dla urządzeń z Androidem.

Badanie, obejmujące ponad 3 300 specjalistów IT z 22 państw na świecie, zostało przeprowadzone we współpracy z Kaspersky Lab. Uczestnicy reprezentowali firmy wszystkich rozmiarów: małe (10-99 skomputeryzowanych stanowisk oraz urządzeń użytkowników końcowych, z wykluczeniem telefonów, z

dostępem do internetu), średnie (100-999 stanowisk) oraz duże (ponad 1 000 stanowisk). Pełne wyniki badania B2B International są dostępne TUTAJ.

Źródło: Kaspersky Lab Polska