

Kontrola wycieku informacji

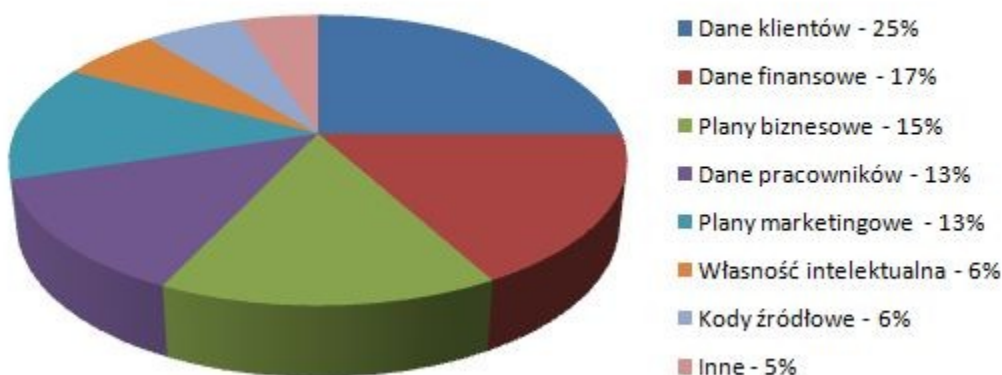
Dane firmowe

Kwestia niekontrolowanego wypływu ważnych informacji firmowych stała się w ostatnim czasie jednym z najpoważniejszych problemów związanych z bezpieczeństwem danych. Ciągłe rosnąca popularność coraz tańszych i zapewniających coraz większą pojemność przenośnych, podręcznych nośników danych niesie ze sobą cały szereg zagrożeń. Urządzenia takie jak pamięci USB Flash, telefony komórkowe, odtwarzacze MP3, karty SD itp. potrafią dziś przechowywać wiele gigabajtów danych, nie wspominając już o przenośnych twardych dyskach, w które wyposażane są urządzenia takie jak iPod (nawet 160 GB). Ich niewielkie rozmiary i łatwość, z jaką można podłączyć je do komputera, zarówno przez porty USB, jak i poprzez Bluetooth czy IrDA, sprawiają, że coraz większe stają się możliwości swobodnego przenoszenia dużych ilości danych, ale także coraz większe ryzyko dostania się ich w niepowołane ręce.

Jak wynika z badań przeprowadzonych w marcu 2008 roku przez firmę SanDisk, jednego z największych producentów pamięci zewnętrznych, aż 77% pracowników przyznaje się do wykorzystywania prywatnych napędów Flash do celów związanych ze swoją pracą¹. Znamiennym jest, że kadra zarządzająca IT oceniła, iż odsetek ten jest o ponad połowę niższy!

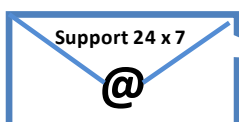
Jakie dane firmowe pracownicy przedsiębiorstw najczęściej przechowują na swoich pendrivach? Według informacji SanDisk, są to informacje, które stanowią w najwyższym stopniu tajemnicę przedsiębiorstwa, tj. dane klientów i innych pracowników, informacje finansowe, plany biznesowe i marketingowe, własność intelektualna oraz kody źródłowe.

Dane firmowe na napędach USB Flash



(wg raportu SanDisk - kwiecień 2008)

¹ <http://www.sandisk.com/Corporate/PressRoom/PressReleases/PressRelease.aspx?ID=4179>



Global:

www.advansysperu.com
info@advansysperu.com
51-1 247-6868

Polska:

www.usblock.pl
usblock@marken.com.pl
058 667-49-49

Oczywiście, należy mieć świadomość, że korzystanie z prywatnych nośników danych przez pracowników nie zawsze musi wiązać się z przechowywaniem na nich danych firmowych – pracownicy mogą używać ich w pracy do kopiowania muzyki, czy pokazywania zdjęć. Jednak z punktu widzenia administratora odpowiedzialnego za bezpieczeństwo danych w sieci firmowej, już to stanowi potencjalne zagrożenie wywołania infekcji szkodliwym oprogramowaniem lub świadomego (bądź nie) wycieku informacji poza firmę.

Polityka bezpieczeństwa

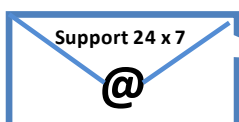
Nadal niewystarczająca jest świadomość zagrożeń związanych z wyciekiem informacji. Jak pokazują wspomniane wcześniej badania firmy SanDisk, ponad dwie trzecie firm, które wprowadziły, bądź wprowadzają politykę bezpieczeństwa oraz program edukacji pracowników, zdecydowały się na ten krok w wyniku wycieku lub naruszenia bezpieczeństwa danych, czyli de facto dopiero po zaistnieniu sytuacji krytycznej.

Jak okazało się w trakcie dalszych badań, samo wprowadzenie polityki bezpieczeństwa również nie do końca rozwiązuje kwestię bezpieczeństwa informacji. Badanie wiedzy pracowników wykazało, że prawie połowa z nich (44%) uważa, iż w firmie nie funkcjonuje żadna polityka bezpieczeństwa zakazująca zapisywania danych firmowych na prywatnych nośnikach, 16% pracowników przyznało się do niezajomości zasad polityki bezpieczeństwa, dopiero kolejnych 40% przyznało, że zakaz jest im znany. Poziom świadomości pracowników kształtuje się na tak niskim poziomie, pomimo deklarowania przez personel zarządzający licznych szkoleń (tylko 3% przyznało, że szkolenia dla pracowników dotyczące bezpieczeństwa informacji nie są wcale przeprowadzane). Potwierdza to opinia 41% administratorów odpowiedzialnych za bezpieczeństwo danych IT, którzy wyrażają zaniepokojenie wysokim poziomem potencjalnego ryzyka związanego z masowym wykorzystywaniem przenośnych pamięci w firmach.

Łącząc to z faktem, że jeden na dziesięciu badanych użytkowników przyznał, iż zdarzyło mu się znaleźć pendrive w miejscu publicznym, otrzymujemy obraz poważnego zagrożenia przed jakim, nie do końca świadomie, staje większość przedsiębiorstw.

„Nasze badanie wykazuje, iż pomimo istnienia pewnej świadomości potencjalnych zagrożeń związanych z korzystaniem z niezabezpieczonych napędów Flash USB, korporacyjne zasady bezpieczeństwa IT wymagają bardziej efektywnych polityk, edukacji i rozwiązań technologicznych w celu obniżenia ryzyka. Jedynie włożenie szczególnego wysiłku, obejmującego inteligentne zarządzanie urządzeniami, monitorowanie danych oraz scentralizowane wymuszenie polityki bezpieczeństwa będzie w stanie dostatecznie zredukować ryzyko, jednocześnie pozwalając organizacjom na czerpanie korzyści z rozszerzonej mobilności.”

Gil Mildworth, Senior Director of Marketing for SanDisk's Enterprise Division



Global:

www.advansysperu.com
info@advansysperu.com
51-1 247-6868

Polska:

www.usblock.pl
usbblock@marken.com.pl
058 667-49-49

Scentralizowana ochrona programem USB Lock RP

Wychodząc naprzeciw potrzebom rynku bezpieczeństwa informatycznego, firma Advanced Systems International stworzyła swój sztanarowy produkt – oprogramowanie USB Lock. Program występuje w dwóch wersjach: ST (Standard) przeznaczonej dla pojedynczych komputerów, oraz RP (Remote Protect) służącej do zdalnego zarządzania ochroną w sieci.

USB Lock RP jest rozwiązaniem niezwykle prostym, łatwym do instalacji i wdrożenia w firmie. Składa się z dwóch plików instalacyjnych: konsoli zarządzającej i klienta. Jego funkcje ochrony obejmują blokowanie dostępu do napędów USB (na przykład nośników Pendrive, odtwarzaczy MP3, iPod), czytników kart pamięci (SD, CF, MMC), napędów CD/DVD, Zip, dyskietek itp. USB Lock umożliwia także blokowanie połączeń IrDA i Bluetooth.

Działanie programu nie ma wpływu na normalnie wykorzystywane urządzenia podłączone przez porty USB, jak na przykład myszki, klawiatury czy skanery.

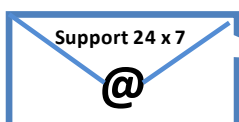
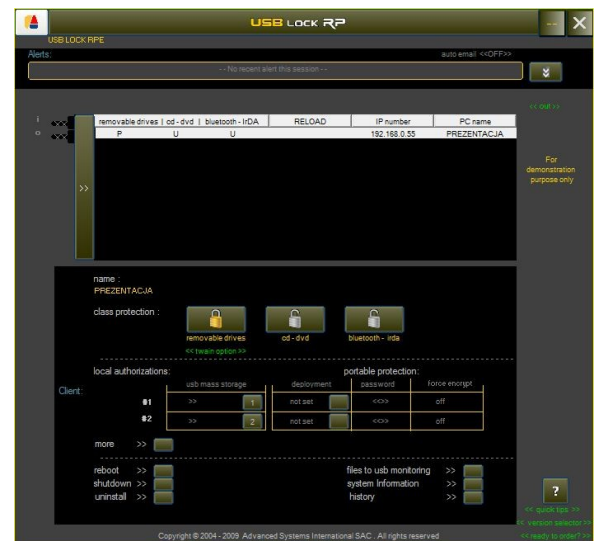
Wszystkie opcje ochrony uruchamia się z poziomu konsoli zarządzającej zainstalowanej na jednym z komputerów w sieci. Administrator konsoli otrzymuje również dostęp do alertów informujących o zdarzeniach związanych z użyciem podlegających kontroli urządzeń, takich jak podłączanie i odłączanie autoryzowanych lub nie posiadających autoryzacji nośników USB. W przypadku zakupu rozszerzonej wersji USB Lock Plus, wyposażonej w moduł USB Aware, administrator będzie posiadał także możliwość podglądu listy plików kopiowanych na nośnik USB.

Oprogramowanie daje możliwość wyznaczenia określonych pamięci USB, które system dopuści do funkcjonowania, w przeciwieństwie do wszystkich innych tego rodzaju urządzeń

(autoryzacja napędów usb). Pozwala to na korzystanie z konkretnych, firmowych nośników pomimo zastosowania rygorystycznej polityki bezpieczeństwa w tym zakresie.

Najnowsze rozszerzenie oprogramowania - USB Lock RPE - pozwala dodatkowo na szyfrowanie zawartości określonych nośników USB.

Oprogramowanie klienckie działa na poziomie systemu operacyjnego. Uruchamiane jest jako usługa systemowa i działa w tle nie wpływając na obciążenie systemu (0% CPU). Próba użycia urządzenia nie posiadającego autoryzacji powoduje zablokowanie komputera i wyświetlenie komunikatu zmuszającego użytkownika do odłączenia zakazanego nośnika. Dzięki oprogramowaniu USB Lock RP chronić można nawet ponad tysiąc stacji roboczych. Program przeznaczony jest dla sieci złożonych z komputerów z systemami Windows 2000, XP, Server 2003 lub Vista (32 lub 64 bit).

**Global:**

www.advansysperu.com
info@advansysperu.com
51-1 247-6868

Polska:

www.usblock.pl
usblock@marken.com.pl
058 667-49-49

Indywidualne zabezpieczenie programem USB Lock ST

Nie w każdym przypadku dobrze sprawdza się scentralizowany system ochrony. W oczywisty sposób dotyczy to użytkowników indywidualnych, ale także części pracowników firm, którzy są uprawnieni do samodzielnej kontroli bezpieczeństwa posiadanych danych, np. użytkowników laptopów, którzy muszą chronić zawartość swoich komputerów, ale na co dzień korzystają z wszelkiego rodzaju nośników i połączeń.

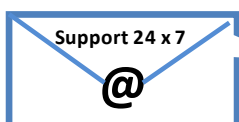
Idealnym rozwiązaniem w tym wypadku będzie program USB Lock w wersji Standard (ST). Program ten pozwala na ochronę przed nieautoryzowanym użyciem nośników USB, Smart Card, dyskietek, płyt CD/DVD oraz połączeń Irda i Bluetooth, podobnie jak czyni to USB Lock RP – jedyną różnicą jest możliwość ustawiania opcji zabezpieczeń na komputerze lokalnym. USB Lock ST posiada jednak dodatkowe możliwości: moduł USB Aware (który jest opcjonalny w przypadku USB Lock RP) oraz bardzo przydatną funkcjonalność – ochronę przenośnych nośników USB, polegającą na zabezpieczeniu zawartości nośników pendrive za pomocą 128-bitowego klucza szyfrującego. Zaszifrowane dane mogą być następnie odczytane także na komputerach, na których nie zostało zainstalowane oprogramowanie USB Lock, jednak czterokrotne podanie nieprawidłowego hasła spowoduje automatyczne zniszczenie chronionych plików.



USB Lock ST pracować może w trybie ręcznym, w którym opcje ochrony ustawia się indywidualnie, oraz w trybie automatycznym. Polega on na tym, że określony nośnik USB wykorzystywany jest jako token (klucz USB). Podłączenie takiego tokena skutkuje automatycznym wyłączeniem ochrony, pozwalającym na natychmiastowe korzystanie z urządzeń. Odłączenie tokena powoduje wznowienie ochrony.

USB Lock ST pracuje bez wpływu na wydajność komputera oraz na inne, normalnie używane peryferia (myszki, klawiatury itp.). Program chroni wszystkie konta użytkowników komputera. Przeznaczony jest dla systemu Windows XP lub Vista (32 lub 64 bit).

O przydatności USB Lock można łatwo przekonać się dzięki udostępnieniu przez producenta wersji demonstracyjnych tego oprogramowania. Wkrótce po jego zainstalowaniu może okazać się, że wdrożenie i egzekwowanie polityki bezpieczeństwa przechowywania oraz przenoszenia danych niekoniecznie musi oznaczać wielkie nakłady finansowe, organizacyjne i czasowe, nawet dla małych firm.

**Global:**

www.advansysperu.com
info@advansysperu.com
51-1 247-6868

Polska:

www.usblock.pl
usblock@marken.com.pl
058 667-49-49