Test: szyfrowanie danych za pomocą DESlock+ s. 52

Przyszłość telefonii komórkowej s. 74

5
2014

Miesięcznik informatyków i menedżerów IT

www.it-professional.pl

IT professional

Nr 5 (30) maj 2014 — Cena 29,00 zł (w tym 5% VAT)

ROZWIĄZANIA MICROSOFT DLA MŚP

s. 12

- **Serwer dla małych firm**
  Możliwości Windows Server 2012 R2 Essentials
- **Bezpieczeństwo IT w małej firmie**
  Mechanizmy ochrony infrastruktury IT
- **Usługi chmurowe Microsoft**
  Pakiet usług biznesowych udostępnianych w ramach chmury publicznej
- **Windows 8.1 Update**
  Nowe funkcje systemu

s. 56

Stalking, pomówienia i kradzież tożsamości

Prawne możliwości ochrony przed przestępstwami internetowymi

s. 42

Uwierzytelnianie za darmo

Centralne zarządzanie dostępem do sieci bezprzewodowej. Serwer FreeRADIUS

s. 30

Ochrona dostępu do sieci

Sprawdzanie kondycji stacji roboczych i konfiguracja DHCP

ISSN 2083-9588
9 772083 958004

Serwery ▪ Stacje robocze ▪ Bezpieczeństwo ▪ Infrastruktura i sieci ▪ Zarządzanie i prawo IT ▪ Technologie mobilne

Sprawdzamy funkcje i możliwości zabezpieczania danych firmowych oferowane przez DESlock+ – narzędzie do szyfrowania plików, folderów, dysków twardych komputerów i pamięci przenośnych.

OCHRONA DANYCH

SZYFROWANIE DLA MŚP

Artur Cieślik

Szukając narzędzia pozwalającego zabezpieczać dane zapisane na komputerach stacjonarnych oraz przenośnych używanych w małej lub średniej wielkości firmie, mamy do wyboru albo rozwiązania wymagające sporych nakładów finansowych, albo dostępne praktycznie bez żadnych opłat. Jak się można łatwo domyślić, każde z tych rozwiązań ma zarówno zalety, jak i wady. Problemem tych pierwszych jest ogromna liczba funkcji wykorzystywanych często wyłącznie w dużych firmach (przyjmijmy, że określenie „duże" odnosi się tu do polskich realiów). Funkcje te wymagają skonfigurowania osobnych serwerów zarządzających i infrastruktury co najmniej klastrowej. Z drugiej strony są rozwiązania open source, oferujące dużą elastyczność konfiguracji i wysoki poziom bezpieczeństwa. Darmowe rozwiązania pozwalają zabezpieczać dane na różnego rodzaju nośnikach: dyskach twardych, pamięciach USB i płytach CD/DVD/Blu-Ray. Mogą oferować dużo ułatwień, jednak dla wielu administratorów firmowych sieci największą wadą będzie brak możliwości zdalnego zarządzania wieloma instancjami za pomocą centralnej konsoli, której najczęściej nie ma w tego typu aplikacjach.

> MOŻLIWOŚCI DESLOCK+

Przetestowaliśmy rozwiązanie w wersjach serwerowej (2.4.5) oraz klienckiej (4.5.7). W zależności od wersji użytkownik może korzystać wyłącznie z klienta standalone lub wersji centralnie zarządzalnej. Aplikację można pobrać ze strony **deslock.com/downloads.php**.

Podstawową wersją rozwiązania jest Personal Edition, pozwalająca na szyfrowanie plików oraz folderów i oferująca wtyczkę do Outlooka. Ponadto pozwala na szyfrowanie schowka oraz dysków wirtualnych i archiwów. Pomimo braku możliwości zabezpieczania kryptograficznego zewnętrznych nośników oraz całych dysków twardych ma jedną dużą zaletę – jest dostępna za darmo. Jednak brak możliwości scentralizowanego zarządzania może być problematyczny dla firm mających potrzebę instalacji rozwiązania na większej liczbie stanowisk.

Kolejna wersja Essential Edition oferuje dokładnie te same funkcje bezpieczeństwa co darmowy odpowiednik, jednak pozwala już na centralne zarządzanie za pomocą serwera DESlock+ Enterprise. Z kolei Standard Edition pozwala dodatkowo na zabezpieczanie zewnętrznych nośników danych, a komplet opcji umieszczono w wersji DESlock+ Pro. Jest to jedyny rodzaj klienta DESlock+, który umożliwia zaszyfrowanie całego dysku łącznie z systemem operacyjnym.

DESlock+ to rozwiązanie polecane szczególnie średniej wielkości organizacjom o rozproszonej infrastrukturze komputerów mobilnych, na których przechowywane są firmowe dane wymagające solidnego zabezpieczenia (szyfrowanie AES, Blowfish oraz 3DES).

Klient obsługuje systemy operacyjne z rodziny Microsoft Windows od XP SP3 do wersji 8 (zarówno 32-, jak i 64-bitowe). Niestety DESlocka+ nie zainstalujemy na maszynach z systemami Linux i Max OS X. Na liście obsługiwanych klientów DESlock+ znajdziemy natomiast mobilny system iOS (wersja 6.0 lub wyższa). DESlock+ Enterprise Server jest centralną usługą opartą na silniku bazy danych MS SQL oraz serwerze Apache, które wymagają do prawidłowego działania Windows XP SP3, 7, 8 lub wersji serwerowych od Windows 2003 Server.

> PLANOWANIE I INSTALACJA

Przed rozpoczęciem procesu instalacji usługi serwera warto przeanalizować kilka scenariuszy implementacji rozwiązania. Opisywany system składa się z czterech głównych składników: konsoli administratora dostępnej przez przeglądarkę Internet Explorer lub Firefox (Admin User Interface), serwera bazy danych (Enterprise Server), proxy wykorzystywanego do pośredniczenia w komunikacji klient–serwer (Enterprise Server Proxy) oraz klienta instalowanego na końcówkach (Client PC). Za pomocą konsoli administracyjnej możemy konfigurować polityki bezpieczeństwa, wysyłać instalacje do klientów i monitorować stan komponentów. Enterprise Server jest

częścią DESlocka+, która może być zainstalowana zarówno na stacji roboczej np. z Windows 7, jak i serwerze Windows w wersji 2008.

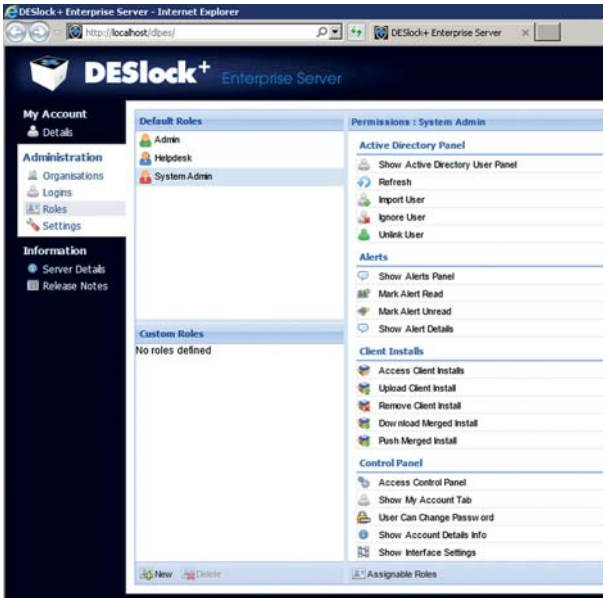
Na szczególną uwagę zasługuje Enterprise Server Proxy – komponent systemu będący interfejsem komunikacyjnym pomiędzy Enterprise Server a klientami zainstalowanymi na stacjach roboczych i laptopach. Usługa może zostać zainstalowana w naszej sieci wewnętrznej lub strefie DMZ albo zostać wdrożona jako usługa chmurowa oferowana przez producenta rozwiązania. Producent deklaruje, że wszystkie dane serwera proxy DESlock+ są szyfrowane. Podobnie wygląda scenariusz, gdy proxy znajduje się pod naszą kontrolą. Usługa w tej konfiguracji jest uruchamiana w naszym DMZ i podobnie jak rozwiązanie chmurowe pośredniczy w połączeniach z klientami.

Po zainstalowaniu usług DESlock+ w wybranym scenariuszu można połączyć się z serwerem za pomocą interfejsu WWW. Przy pierwszym uruchomieniu system poprosi o podanie nazwy organizacji i użytkownika oraz hasła administracyjnego.

> OPCJE KLUCZY

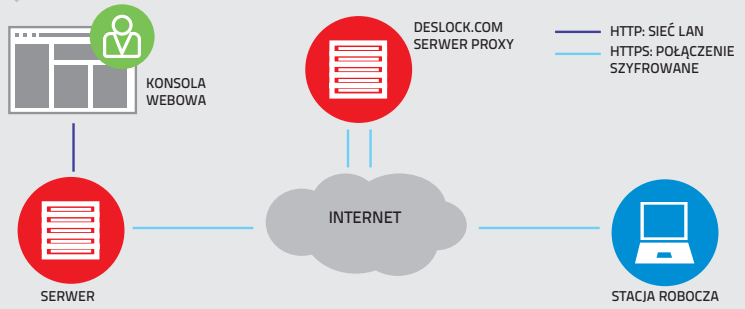
Okno interfejsu jest podzielone na panel boczny oraz główny z paskiem zakładek, w którym prezentowane są opcje konfiguracyjne. Użytkowników możemy pogrupować w folderach przypisywanych do danej organizacji (w przypadku dużych wdrożeń możliwe jest utworzenie wielu organizacji, których klientami zarządzamy). Podobnie jak w Active Directory do określonych folderów możemy przypisywać wybrane polityki oraz grupy kluczy szyfrujących, które następnie można powiązać z grupami klientów. W oprogramowaniu DESlock+ obiekty organizujące klientów w grupy nazywane są Teams. Jednocześnie w tych grupach klientów można definiować grupy kluczy używane później w danym zespole klientów. Klucze szyfrujące mogą być przyporządkowywane do grup, a następnie wykorzystywane przez klientów należących do wskazanych kontenerów (zespołów). Typy kluczy mogą korzystać z trzech rodzajów algorytmów: AES, Blowfish oraz 3DES (Triple Data Encryption Standard). Pierwszy z nich jest zaakceptowanym standardem o nazwie Rijndael, którego skuteczność pozwala na stosowanie go do zabezpieczenia nawet ściśle tajnych informacji. DESlock+ wykorzystuje wersję AES o długości klucza 256 bitów. Ten tryb został zaakceptowany zarówno przez National Institute of Standards and Technology (NIST), jak i Institute of Electrical and Electronics Engineers (IEEE) jako standard szyfrowania dla urządzeń o zapisie blokowym. Z tego powodu w przypadku korzystania z opcji FDE (Full Disk Encryption) tylko ten algorytm może być wykorzystany do zabezpieczenia całego dysku.

Drugim algorytmem jest Blowfish o długości klucza od 32 do 448 bitów oraz bloku 64-bit. Jest znacznie szybszy niż DES i bezpieczniejszy. Nie są znane skuteczne ataki poza jednym, który można przeprowadzić tylko dla słabych kluczy i wyłącznie w przypadku korzystania z Blowfisha czteroprzebiegowego. Trzeci z obsługiwanych algorytmów szyfrujących to 3DES. Algorytm wykorzystuje trzy klucze DES, co w efekcie daje nam trzykrotne szyfrowanie algorytmem



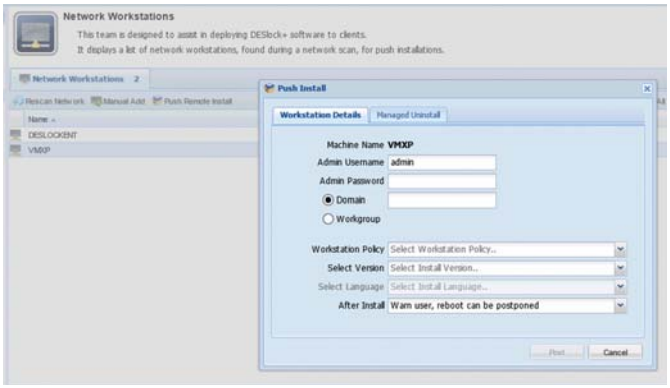
Rozbudowane ustawienia uprawnień dla administratorów umożliwiają dokładne wskazanie ról poszczególnych osób zarządzających infrastrukturą DESlocka.

KOMUNIKACJA Z ENTERPRISE SERVER PROXY



Domyślną konfiguracją jest serwer proxy działający jako usługa chmurowa. Enterprise Server Proxy można również zainstalować w sieci wewnętrznej.

DES za pomocą trzech odrębnych kluczy szyfrujących o długości 56 bitów. Dzięki takiemu podejściu otrzymujemy 168-bitowy klucz szyfrujący. Każda operacja z potrójnej enkrypcji szyfruje blok o długości 64 bitów. 3DES podatny jest na atak na klucz, jednak wymaga sporych nakładów związanych z dostarczeniem odpowiedniej mocy obliczeniowej i pamięci. Sprawia to, że taki atak przy obecnym stanie technologii jest nieskuteczny.



DESlock pozwala na wypychanie zdalnej instalacji do przygotowywanych stacji roboczych.

> POLITYKI ZABEZPIECZEŃ

Kolejnym krokiem wdrożenia jest utworzenie polityk. W oprogramowaniu DESlock+ możemy konfigurować dwa rodzaje polityk: użytkownika (Group Policy) oraz stacji roboczej (Workstation Policy). Pierwsza z nich określa poziom dostępu do funkcji klienta przez użytkownika stacji roboczej, liczbę wymaganych znaków w haśle, jego złożoność i zasady reagowania na wielokrotne podanie błędnego ciągu znaków. Osobna grupa funkcji pozwala określać polityki zabezpieczeń dla zewnętrznych nośników danych. Za pomocą dostępnych w tym miejscu opcji można np. wymusić na użytkownikach korzystanie tylko z szyfrowanych pamięci USB lub przynajmniej szyfrowanych plików i katalogów. W tym miejscu można również uruchomić proces szyfrowania całego dysku komputera, na którym pracuje wskazany użytkownik zalogowany do klienta DESlock+.

Drugim typem zbioru zasad są polityki stacji roboczej. W tym miejscu możemy określić reakcję systemu na nieaktywność użytkownika oraz znaleźć funkcje odpowiedzialne za komunikację z serwerem proxy i uwierzytelnianie do tej usługi. Wśród zasad znajdziemy również parametry dotyczące kluczy szyfrujących, w tym zasad ich przechowywania na stacji roboczej. Dostępne są też opcje administracyjne odpowiedzialne za określenie automatycznego wykonywania aktualizacji aplikacji klienta DESlock+.

Polityki bezpieczeństwa pozwalają również na korzystanie z szyfrowania wskazanych plików lub katalogów na dyskach. Za wybór szyfrowanych zasobów odpowiada jednak użytkownik. Administrator może jedynie udostępnić taką opcję lub ją zablokować. Ta zasada dotyczy generalnie wszystkich funkcji z wyjątkiem opcji szyfrowania całego dysku. O uruchomieniu procesu FDE (Full Disk Encryption) decyduje administrator DESlocka+, który może rozpocząć szyfrowanie, wybierając właściwą opcję w obiekcie użytkownika. Aby proces mógł się rozpocząć, użytkownik jest zobowiązany do wpisania kodu aktywacyjnego rozpoczynającego szyfrowanie całego dysku. Administrator może też wyłączyć możliwość szyfrowania dysku dla wskazanego komputera w Workstation Policy, wyłączyć możliwość zalogowania się użytkownika do zaszyfrowanego systemu oraz zdalnie usunąć dane uwierzytelniające również administratora (!). Skutkiem wybrania tej opcji jest zdalne zablokowanie dostępu do systemu bez możliwości odzyskania danych. Opcja ta jest przydatna np. w przypadku kradzieży sprzętu.

WERSJE DESLOCK+

	Personal Edition	Essential Edition	Standard Edition	DESlock+ PRO
Szyfrowanie całej powierzchni dysku (transparentna autoryzacja w fazie pre-boot)	○	○	○	●
Szyfrowanie dysków wymiennych (na podstawie polityk tworzonych w konsoli centralnego zarządzania)	○	○	●	●
DESlock+Go – szyfrowanie nośników wymiennych (dostęp do danych na stacjach bez zainstalowanego programu DESlock)	○	○	●	●
Szyfrowanie plików i folderów	●	●	●	●
Szyfrowanie poczty i załączników (wtyczka dla MS Outlook)	●	●	●	●
Szyfrowanie tekstu oraz schowka	●	●	●	●
Tworzenie zaszyfrowanych woluminów oraz archiwów samorozpakowujących się	●	●	●	●
Centralne zarządzanie (zaszyfrowanymi stacjami, użytkownikami oraz kluczami szyfrującymi)	○	●	●	●

> INSTALACJA KLIENTÓW

Konfigurację powinniśmy zacząć od ustalenia ustawień wysyłanych do klientów. Dla wybranego obiektu (zespołu), będącego po prostu katalogiem użytkowników lub stacji roboczych, ustalamy odpowiednie zasady lub korzystamy z dziedziczenia obiektu nadrzędnego. Następnym krokiem jest dodanie klienta poprzez podanie adresów e-mail naszych użytkowników oraz przypisanie do poszczególnych osób licencji (generowany jest klucz niezbędny do aktywacji klienta DESlock+ zainstalowanego

na stacji roboczej użytkownika). Klucz dostępny jest w postaci ciągu znaków, które można przesłać mailem lub wpisać osobiście podczas przygotowywania sprzętu dla pracownika. Następnie użytkownikowi należy przypisać grupę kluczy szyfrujących.

W celu instalacji oprogramowania na komputerze użytkownika można skorzystać z opcji push, która wysyła instalator do klientów widocznych w sieci i automatycznie łączy z serwerem proxy, który pośredniczy w połączeniach z serwerem polityk. Możliwe jest również przygotowanie instalatora, który będzie uruchamiany na wskazanych komputerach lub instalowany za pomocą Group Policy Objects znajdujących się w usłudze Active Directory. Trzeba pamiętać, że instalacja klienta wymaga dostępu sieciowego do serwera proxy, w celu jego aktywacji po instalacji. Jeżeli naszym serwerem proxy jest usługa dostępna w internecie, wystarczy zapewnić dostęp do globalnej sieci aktywowanego komputera.

Po instalacji i aktywacji klient DESlock+ pobiera polityki z serwera Enterprise Server za pośrednictwem proxy. Użytkownik może skorzystać z funkcji udostępnionych przez administratora systemu. Sam administrator może w tym momencie przejść do szczegółów użytkownika w konsoli DESlock+ i uruchomić proces szyfrowania całego dysku (FDE). Po wybraniu tej funkcji można określić hasła administratora oraz użytkownika, które będą niezbędne do uruchomienia systemu operacyjnego i dostępu do danych zapisanych na danym komputerze.

Podstawową funkcją FDE jest szyfrowanie całych dysków łącznie z systemem operacyjnym Windows. Wybierając taką formę zabezpieczenia, mamy możliwość skorzystania tylko z algorytmu AES, a szyfrowanie całego dysku wraz z partycją systemową wykonywane jest w locie.

> PRZYDATNE DODATKI

W DESlock+ znajdziemy jeszcze kilka innych przydatnych opcji. Oprócz całego dysku, podłączanych do komputera napędów zewnętrznych i pamięci przenośnych możemy zaszyfrować nośniki CD oraz DVD. Kolejnymi elementami, które można zaszyfrować, są wiadomości e-maili. Tworzona wiadomość może być zaszyfrowana w całości lub w części za pomocą klucza lub hasła (dostępny plug-in do Outlooka; odbiorca maila powinien zaopatrzyć się w darmową aplikację DESlock+ Reader dostępną na stronie producenta). Kolejne zabezpieczenie służy do szyfrowania wskazanego tekstu wyświetlanego w oknie aplikacji lub zapisanego do schowka Windows. Na szczególną uwagę zasługuje opcja tworzenia dysków wirtualnych. Jest to rozwiązanie pozwalające na przygotowanie szyfrowanego woluminu mającego postać pojedynczego pliku przechowywanego na dysku. Za pomocą DESlock+ Virtual Disk Managera plik może zostać zamontowany w systemie Windows pod wskazaną literą i być dostępny jako kolejny napęd. Tego typu woluminy są bardzo wygodne w użyciu i mogą być stosowane do przechowywania poufnych plików bez konieczności szyfrowania całego systemu operacyjnego. IT

PODSUMOWANIE

Testowany DESlock+ jest płatnym rozwiązaniem do zabezpieczania danych przechowywanych na różnego rodzaju nośnikach: dyskach twardych, pamięciach zewnętrznych, płytach CD/DVD. Dużą zaletą rozwiązania jest system zdalnego, centralnego zarządzania dostosowany do rozproszonej infrastruktury stacji roboczych i laptopów. Użytkownicy nie muszą dostarczać urządzeń do pracowników działu IT w celu zabezpieczenia danych, a administratorzy mają możliwość wykonywania praktycznie wszystkich czynności łącznie ze zdalną instalacją klienta. Rozwiązanie pozwala na użycie sprawdzonych algorytmów szyfrowania: AES, Blowfish oraz 3DES. Oferuje również szeroką gamę ułatwień dla użytkowników, łącznie z możliwością szyfrowania wiadomości e-mail i komunikacji z klientami mającymi dostęp tylko do darmowej wersji aplikacji. Rozwiązanie polecamy szczególnie średniej wielkości organizacjom o rozproszonej infrastrukturze komputerów mobilnych, na których przechowywane są firmowe dane wymagające solidnego zabezpieczenia.

Werdykt

DESlock+

Zalety

- ⊕ Darmowa wersja klienta
- ⊕ Możliwości centralnego zarządzania
- ⊕ Wysoki poziom bezpieczeństwa
- ⊕ Liczba przydatnych funkcji
- ⊕ Polska wersja interfejsu
- ⊕ Dokumentacja (dostępna na stronie WWW)

Wady

- ⊖ Brak wsparcia dla systemów Linux
- ⊖ Brak wsparcia sprzętowego dla szyfrowania AES

Ocena 8/10

Autor specjalizuje się w realizacji audytów bezpieczeństwa informacji, danych osobowych i zabezpieczeń sieci informatycznych. Był wieloletnim menedżerem Działu Integracji Systemów. Prowadzi szkolenia z zakresu bezpieczeństwa informacji i ochrony danych osobowych oraz audytów zabezpieczeń systemów informatycznych.