PIERWSZY FILAR RODO

Wiele wrażliwych danych, choć nie powinno, jest przechowywanych i przetwarzanych na stacjach roboczych i laptopach. Podstawowym działaniem w kierunku spełnienia wymagań RODO wydaje się zatem zaszyfrowanie dysków w komputerach pracowników oraz innych używanych przez nich nośników danych. Oto najlepsze darmowe i płatne narzędzia do szyfrowania danych.

Artur Pęczak

W maju 2018 roku wchodzi w życie Rozporządzenie o Ochronie Danych Osobowych (RODO), jakie istotnie zmienia zasady ochrony danych osobowych, rozszerza zakres podmiotów, których te przepisy dotyczą oraz podnosi wysokość kar za ich naruszenie. Choć RODO nie wskazuje wprost konkretnych rozwiązań technicznych i organizacyjnych, które należy podjąć, aby zapewnić wymagany poziom bezpieczeństwa systemów i danych przedsiębiorstwa, jedno ze sformułowań pojawia się w kilku miejscach unijnego rozporządzenia. Mowa tutaj o pseudonimizacji, czyli zastąpieniu jednego atrybutu danych innym (np. nazwiska – liczbą) i szyfrowaniu danych, które w artykule 32. („Bezpieczeństwo przetwarzania") wymieniane jest na pierwszym miejscu jako najważniejszy środek ochrony wrażliwych informacji.

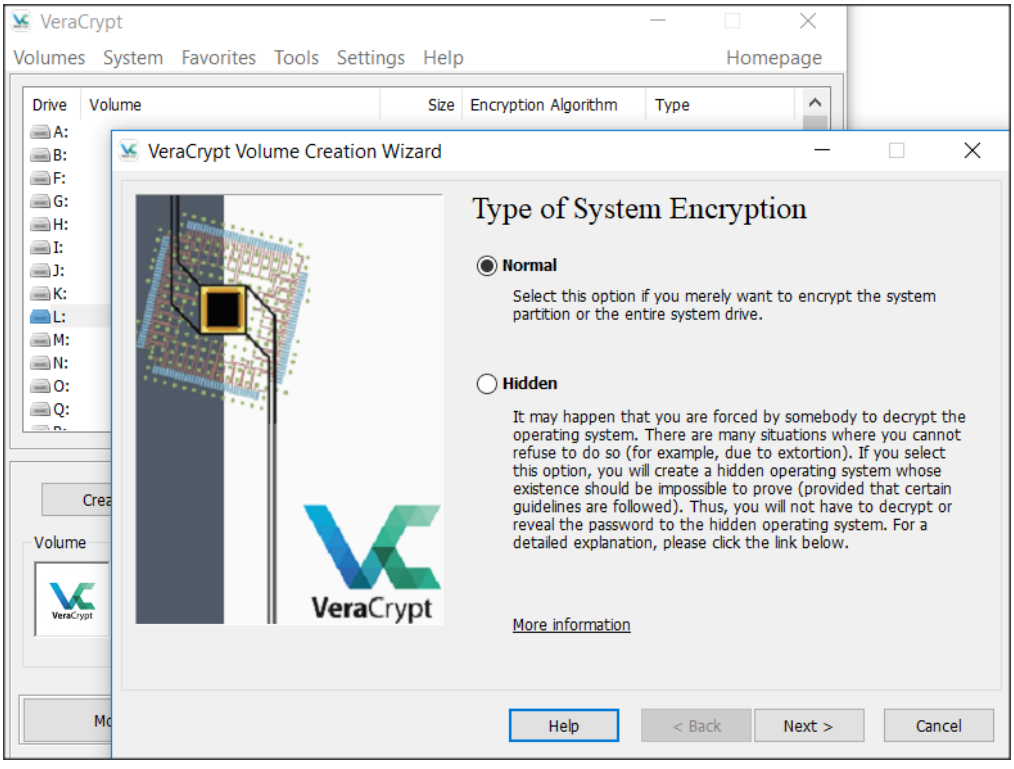
Punktem wyjścia powinno być założenie, że żadne wrażliwe informacje przedsiębiorstwa, a w szczególności dane osobowe objęte ochroną z mocy prawa, nie powinny być przechowywane i przetwarzane na komputerach osobistych pracowników. Ich miejsce jest na serwerach instalowanych w dobrze zabezpieczonych fizycznie, technicznie i organizacyjnie centrach danych. Problem w tym, że spełnienie tych wymagań nie zawsze jest możliwe, a ze względu na charakter stanowiska pracy – niekoniecznie uzasadnione. Dane osobowe to nie tylko bazy danych klientów i pracowników w systemie kadrowo-płacowym, ale również umowy o pracę czy CV przesyłane e-mailem i zapisywane na dyskach użytkowników. Czym zabezpieczyć komputery pracowników, którzy mają styczność z danymi osobowymi i innymi wrażliwymi informacjami przedsiębiorstwa?

Szyfrowanie całych dysków

Oprogramowanie do szyfrowania całych dysków i nośników wymiennych (z ang. full disk encryption, FDE) to kategoria aplikacji zasadniczo odmiennych od narzędzi pozwalających na zabezpieczenie wskazanych plików i folderów (z ang. file level encryption, FLE).

Do wyboru jest bezpłatne oprogramowanie (VeraCrypt, DiskCryptor) wbudowane w Windows narzędzie BitLocker oraz komercyjne rozwiązania skierowane do firm różnej wielkości, np. DESlock+, moduł szyfrowania w programie Kaspersky Endpoint Security, Dell Data Protection I Encryption I inne. Dwa pierwsze produkty łączą cechy narzędzi FDE i FLE, oferując użytkownikom

▼ VeraCrypt kontynuuje tradycje programu TrueCrypt 7.1a. Kolejne wersje programu usuwały słabości zauważone w algorytmach szyfrowania oryginału.



pełne spektrum narzędzi do zabezpieczania danych.
Bezpłatne oprogramowanie całkiem nieźle sprawdza się w zabezpieczaniu pojedynczych komputerów. Administratorzy w większych firmach docenią możliwość zarządzania bezpieczeństwem punktów końcowych z centralnej konsoli, zaawansowane mechanizmy autoryzacji i uwierzytelniania z zastosowaniem kart kryptograficznych oraz czytników odcisków palca, integrację z usługą katalogową Active Directory i branżowe certyfikacje algorytmów zaimplementowanych w oprogramowaniu do szyfrowania, np. FIPS 140-2 dla algorytmu AES w programie DESlock+.

Żadne wrażliwe informacje przedsiębiorstwa, zwłaszcza dane osobowe objęte ochroną z mocy prawa, nie powinny być przechowywane i przetwarzane na komputerach osobistych pracowników. Ich miejsce jest na serwerach instalowanych w dobrze zabezpieczonych fizycznie, technicznie i organizacyjnie centrach danych.

VeraCrypt

TrueCrypt, chyba najbardziej znany program do szyfrowania dysków, w maju 2014 roku przestał być nagle rozwijany. Mimo to wiele osób używa jego ostatniej „zaufanej" wersji w domu i małych firmach. Nic dziwnego, bo to znakomity program, a wydanie oznaczone numerem 7.1a działa prawidłowo również z Windows 10. Wystarczy dobrze poszperać w sieci, a jeszcze lepiej poszukać plików instalacyjnych aplikacji w archiwach.
Na bazie TrueCrypt 7.1a szybko powstało kilka odgałęzień, które kontynuują rozwój programu. Najbardziej znanym odgałęzieniem okazał się VeraCrypt, również rozwijany na zasadach open source. W kolejnych wydaniach tej aplikacji usunięto kilka słabości zauważonych w trakcie audytu błędów w zabezpieczeniach TrueCrypta oraz dokonano zmian w algorytmach szyfrujących, aby lepiej opierały się atakom siłowym. Mowa głównie o zwiększonej liczbie iteracji dla wybranych algorytmów mieszających. Nowa funkcja PIM pozwala użytkownikowi samodzielnie wskazać liczbę iteracji wykonywanych przez funkcję generującą klucz szyfrowania. Od wersji 1.0f VeraCrypt pozwala na montowanie wolumenów TrueCrypta. W ten sposób zachowano wsteczną kompatybilność z oryginałem.
Zasadniczo zmiany wprowadzone w VeraCrypt są „kosmetyczne", a zatem program oferuje w dużej mierze to, za co użytkownicy doceniali TrueCrypta. Program umożliwia szyfrowanie całych dysków, w tym partycji systemowych lub wybranych woluminów i pamięci przenośnych. W pierwszym przypadku odblokowanie dostępu do dysku wymaga wprowadzenia hasła zaraz po uruchomieniu komputera (pre-boot). VeraCrypt umożliwia również szyfrowanie danych w kontenerach. Na dysku kontener przechowywany jest w postaci pojedynczego pliku, który po tzw. zamontowaniu staje się widoczny w systemie jako kolejny dysk twardy komputera. Wszystkie dane zapisane na takim dysku, a w rzeczywistości w kontenerze, pozostają zaszyfrowane.
Analogicznie do oryginału VeraCrypt szyfruje dane w czasie rzeczywistym. Dzięki wsparciu sprzętowego szyfrowania w procesorach, funkcji parallelization (program korzysta z wielu procesorów i wielu rdzeni procesora jednocześnie) oraz pipelining (dane są szyfrowane i deszyfrowane do pamięci RAM) działanie programu nie ma zauważalnego wpływu na wydajność komputera. Aplikacja obsługuje ukryte wolumeny, które stanowią odzwierciedlenie idei steganografii do ukrycia ważnych danych wewnątrz innych, nieistotnych.

DiskCryptor

W kategorii wolnego oprogramowania konkurentem TrueCrypta i pochodnych programów pozostaje DiskCryptor. Ostatnia wersja tej aplikacji została wydana w połowie 2014 roku i chociaż poprawnie działa z Windows 10, swoje najlepsze lata ma już za sobą. DiskCryptor szyfruje całe dyski i nośniki wymienne, nie obsługuje zaś kontenerów, interfejsu UEFI oraz partycji GTP. Przed zaszyfrowaniem partycji systemowej (rozruchowej) należałoby więc zmienić interfejs UEFI na przestarzały BIOS i przekonwertować układ dysku z GPT do MBR.
DiskCryptor działa niezauważalnie dla użytkownika, obsługuje algorytmy AES, Twofish i Serpent oraz ich kombinacje, a także sprzętowe wspomaganie szyfrowania dla AES. Zaletą programu, w szczególności dla osób, które instalują na komputerach także Linuksa, jest możliwość integracji z menedżerem rozruchu GRUB. Starsze LILO jest również wspierane. Inną opcją jest zapisanie programu rozruchowego (bootloader) na zewnętrznym nośniku i wykorzystanie dodatkowej metody autoryzacji w postaci klucza cyfrowego. DiskCryptor umożliwia też stworzenie zaszyfrowanego obrazu płyty CD/DVD.

BitLocker

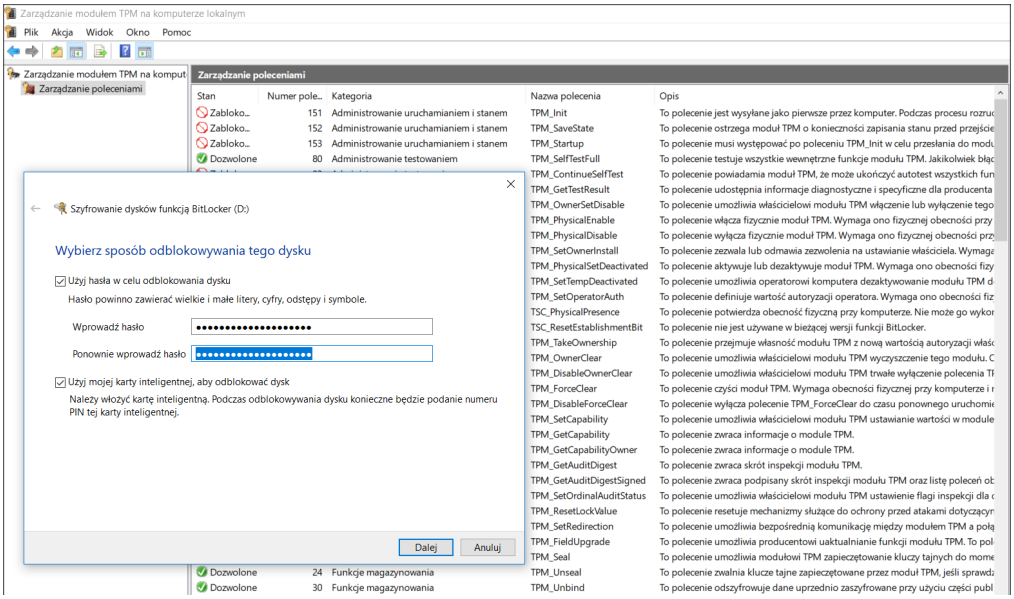
BitLocker to wbudowane w Windows narzędzie do szyfrowania całych dysków. Problem w tym, że jest dostępne wyłącznie w wersjach systemu skierowanych dla firm. W Windows 10 z funkcji tej mogą skorzystać posiadacze licencji Pro i Enterprise. W Windows 7 narzędzie jest dostępne w wydaniach Ultimate i Enterprise.
Działanie funkcji BitLocker opiera się na module Trusted Platform

Module (wymagana wersja 1.2 lub wyższa). To sprzętowy układ scalony na płycie głównej komputera, w którym przechowywane są klucze szyfrowania. W przypadku BitLockera moduł TPM wykorzystywany jest również do sprawdzania integralności procesu uruchamiania systemu. Złodziej, który ukradnie laptopa, nie uzyska dostępu do danych, nawet jeśli uruchomi własny system z płyty LiveCD lub USB albo przełoży nośnik do innego komputera. To najbardziej neutralny sposób szyfrowania dysków. Poziom bezpieczeństwa można istotnie zwiększyć poprzez wymuszenie na pracowniku dodatkowego uwierzytelnienia w trakcie uruchamiania komputera. Urządzenie może zostać zabezpieczone hasłem, kartą inteligentną z kodem PIN lub oboma tymi składnikami uwierzytelniania jednocześnie.

Szyfrowanie dysków funkcją BitLocker możliwe jest również na komputerach bez modułu TPM. Wówczas BitLocker przechowuje klucze szyfrowania na pamięci USB, którą należy umieścić w urządzeniu w momencie uruchamiania komputera lub wybudzaniu go z hibernacji. Od Windows 8 Microsoft dodał również możliwość odblokowywania komputera hasłem. Co zrozumiałe, w obu przypadkach traci się ochronę zapewnianą przez moduł TPM.

BitLocker nie wymaga instalacji dodatkowego oprogramowania na komputerze, a przy tym na laptopie z TPM jest łatwy do wdrożenia. W menu kontekstowym dysku komputera wystarczy wybrać opcję Włącz funkcję BitLocker. Wbudowany kreator poprowadzi przez kolejne etapy zabezpieczania nośnika. Firmowym administratorom przyda się możliwość włączenia szyfrowania na etapie wdrażania systemu z wykorzystaniem mechanizmu WinPE oraz szeroka integracja ze środowiskiem Windows Server, w tym możliwość sterowania działaniem funkcji za pomocą Zasad grupy (np. czy program ma szyfrować cały dysk, czy tylko obszary zajęte przez dane). BitLocker integruje się również z usługami katalogowymi Active Directory w zakresie centralnego zarządzania kluczami odzyskiwania.

Microsoft udostępnił także narzędzie Microsoft BitLocker Administration and Monitoring (MBAM), które umożliwia centralne zarządzanie chronionymi punktami końcowymi. MBAM pozwala na wdrażanie polityk szyfrowania na podstawie szablonów oraz monitorowanie zgodności komputerów z tymi politykami na poziomie pojedynczego komputera lub całej organizacji. Administrator ma dostęp do kluczy odzyskiwania w przypadku, gdy użytkownik zapomni haseł lub rekord startowy komputera zostanie zmieniony. Co więcej, BitLocker może być zarządzany za pomocą narzędzi firm trzecich, np. produktów antywirusowych Kaspersky, Dell Data Protection | Encryption, Symantec Endpoint Encryption czy Sophos SafeGuard Enterprise.



▲ Rdzeniem systemu zabezpieczeń funkcji BitLocker jest sprzętowy układ Trusted Platform Module montowany w nowoczesnych komputerach. Dodatkowo do odblokowania komputera może być wymagane podanie hasła lub włożenie karty inteligentnej.

DESlock+

DESlock+ to narzędzie szyfrowania przeznaczone dla różnej wielkości firm. Program umożliwia szyfrowanie powierzchni całych dysków, nośników wymiennych, pojedynczych plików, wiadomości e-mail i tekstu. Wspiera najnowsze wersje Windows, interfejs UEFI oraz układ partycji GPT. Program dostępny jest w trzech wersjach, przy czym wszystkie opcje szyfrowania dostępne są w wydaniu DESlock+ Pro.

Aplikacja jest prosta we wdrożeniu i użyciu. Może być używana przez użytkowników indywidualnych, choć siła tego rozwiązania tkwi w centralnej konsoli, która z jednego miejsca pozwala zarządzać grupami użytkowników i ich stacjami roboczymi. Licencje, polityki zabezpieczeń i klucze szyfrujące mogą być dostarczane i zarządzane z jednego centralnego miejsca. Serwer proxy obsługiwany w chmurze producenta zapewnia płynną komunikację między komputerami pracowników, a serwerem zarządzającym, bez konieczności konfigurowania połączeń VPN do sieci wewnętrznej przedsiębiorstwa. Co ważne, DESlock+ oferuje zaawansowane funkcje zarządzania kluczami szyfrowania. Program umożliwia dodawanie i usuwanie kluczy, w tym zmianę polityki

szyfrowania, zdalnie i w sposób niewidoczny dla użytkownika.
Bezpieczny folder to interesująca alternatywa dla użytkowników, którzy nie potrzebują ochrony dla całego dysku. Wszystkie pliki umieszczone w takim folderze zostaną automatycznie zaszyfrowane i pozostaną należycie chronione przed dostępem osób trzecich. Dzięki integracji z Microsoft Outlook program pozwala również na szyfrowanie wiadomości e-mail. Tak zabezpieczoną wiadomość będzie mogła odczytać osoba, która posiada taki sam klucz szyfrujący jak nadawca. Jeśli na komputerze nie zainstalowano programu DESlock+, w celu „odblokowania" wiadomości adresat może po prostu wprowadzić hasło szyfrowania. Mocną stroną programu jest narzędzie DESlock+GO, które pozwala na odczytanie zaszyfrowanego nośnika wymiennego na dowolnej stacji. DESlock+ poza zabezpieczaniem klasycznych pamięci przenośnych umożliwia również szyfrowanie płyt CD i DVD.

Kaspersky Endpoint Security

W kwestii bezpieczeństwa komputerów wiele do powiedzenia mają dostawcy oprogramowania antywirusowego. W zaawansowanych wariantach swoich pakietów Internet Secyrity oferują oni funkcje szyfrowania w ramach aplikacji zabezpieczających. ESET oferuje w ten sposób użytkownikom opisany wcześniej DESlock+. Funkcje szyfrowania dysków w produktach Kaspersky dla średniej wielkości firm są włączone w pakiet Kaspersky Endpoint Security for Business Advanced lub stanowią dodatek do licencji Select. Połączenie kilku technologii zabezpieczeń w jednym produkcie ułatwia zarządzanie bezpieczeństwem, pozwalając stworzyć spójną politykę ochrony w ramach całej organizacji.
Moduł szyfrowania w programie Kaspersky umożliwia szyfrowanie całych dysków lub plików zarówno w wypadku nośników umieszczonych na stałe w komputerze, jak i pamięci przenośnych. Polityki zabezpieczeń mogą być centralnie zarządzane z poziomu jednolitej konsoli administratora. Narzędzie obsługuje uwierzytelnienie dwuskładnikowe przy użyciu kart inteligentnych i tokenów, co podnosi bezpieczeństwo dostępu do danych na komputerze. Moduł ma jeszcze jedną ciekawą funkcję. Chcąc udostępnić poufne dane drugiej osobie, która nie dysponuje produktem Kaspersky, można utworzyć chronione hasłem, zaszyfrowane i samorozpakowujące się archiwum plików.
Kaspersky integruje się z BitLockerem. Na urządzeniach z Windows szyfrowanie dysków może być realizowane z użyciem rozwiązania Microsoft, a zarządzane z poziomu konsoli administracyjnej Kaspersky.

Dell Data Protection | Encryption

W obszarze szyfrowania danych firma Dell proponuje rozwiązanie Dell Data Protection | Encryption. Producent chwali się zgodnością oprogramowania z najwyższym komercyjnie dostępnym certyfikatem IPS 140-2, poziom 3 w zakresie szyfrowania dysków systemowych. Wybrane notebooki z linii Latitude, komputery OptiPlex oraz stacje robocze Precision mają wbudowany sprzętowy moduł Hardware Crypto Accelerator, który oferuje zabezpieczenie danych klasy wojskowej na poziomie całych dysków twardych. Istnieje możliwość zamówienia komputera w fabryce z wdrożonym systemem szyfrowania dysku.
Dell Data Protection dostępny jest w wersji Personal dla użytku osobistego i mniejszych organizacji oraz Enterprise dla większych przedsiębiorstw z centralną konsolą oferującą funkcje zdalnego wdrażania, zarządzania i inspekcji zasad zabezpieczeń na punktach końcowych. W wariancie Mobile Edition produkt Della służy do zabezpieczania urządzeń mobilnych. W wersji Cloud niezauważalnie szyfruje i deszyfruje dane zapisywane na dyskach chmurowych takich jak Box, czy Dropbox.
Dell Data Protection oferuje różne opcje szyfrowania – od funkcji, Bit-Locker oferując spójne mechanizmy zarządzania, raportowania i audytu, po własne algorytmy szyfrowania potwierdzone certyfikatami. Oprogramowanie wyposażono w wiele mechanizmów autoryzacji i uwierzytelniania pracowników w dostępie do urządzenia, w tym wsparcie dla układów TPM, kontrolę dostępu za pomocą czytników kart inteligentnych i linii papilarnych po uwierzytelnianie z wykorzystaniem haseł Windows.
Spośród innych aplikacji klasy korporacyjnej do szyfrowania całych dysków warto wymienić również produkty Symantec Endpoint Encryption (oparte na technologii PGP), Sophos SafeGuard, Check Point Full Disk Encryption Software Blade, WinMagic SecureDoc Disk Encryption i McAfee Complete Data Protection—Advanced z integracją do konsoli ePolicy Orchestrator (ePO) używanej do zarządzania innymi produktami McAfee na punktach końcowych. ■

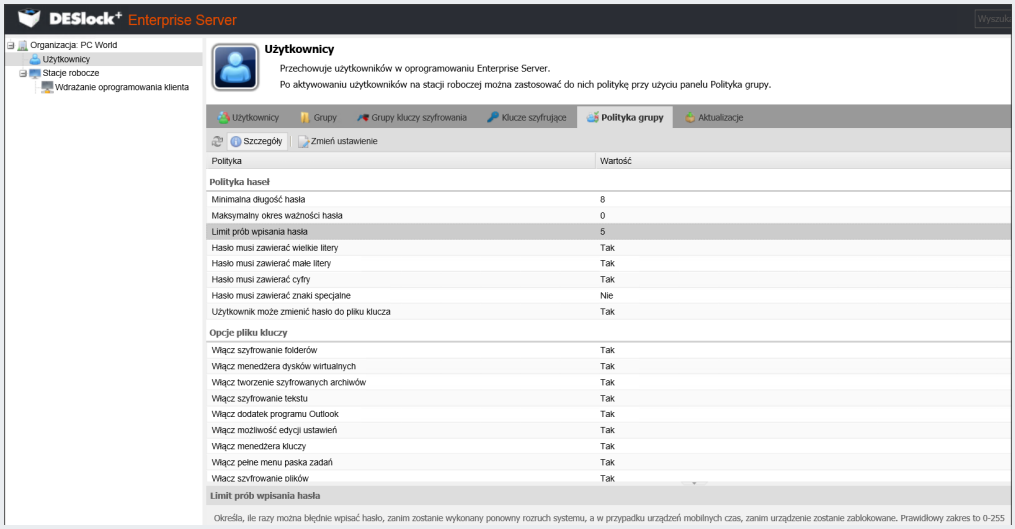
Artur Pęczak

DESlock+ jest kompletnym i uniwersalnym narzędziem do szyfrowania danych, poczty i dysków dla małych i dużych firm. Na polskim rynku aplikacja całkiem nieźle wypełnia lukę między darmowym oprogramowaniem szyfrującym a drogimi rozwiązaniami przeznaczonymi dla największych przedsiębiorstw i korporacji.
DESlock+ doskonale sprawdzi się jako samodzielne narzędzie instalowane na kilku firmowych komputerach. Z drugiej strony rozwiązanie oferuje funkcje klasy korporacyjnej, które z powodzeniem pozwalają je wdrażać w większych organizacjach. Mowa o konsoli centralnego zarządzania, szerokiej integracji z Active Directory, rozbudowanych opcjach administracji, narzędziach odzyskiwania zaszyfrowanych danych oraz ochrony poczty elektronicznej.
W zależności od wersji (Essential, Standard i Pro) program oferuje wiele metod szyfrowania – tekstu i schowka, wiadomości i załączników Microsoft Outlook, pojedynczych plików i folderów, danych w kontenerach (analogicznie do TrueCrypta) oraz powierzchni całych dysków i nośników wymiennych (FDE). W rezultacie program wykorzystasz do ochrony danych zapisanych na dyskach komputerów, ale także informacji wymienianych między pracownikami, np. e-mailami. W tym ujęciu DESlock+

RECENZJA

DESLOCK+. SZYFROWANIE NA MIARĘ CZASÓW

Szyfrowanie dysków, nośników wymiennych, plików oraz wiadomości e-mail programem DESlock+ skutecznie zabezpiecza wrażliwe dane przed ujawnieniem.



staje się narzędziem zarówno dla administratorów odpowiedzialnych za ochronę danych przechowywanych na dyskach komputerów, jak i pracowników, którzy sami mogą decydować o tym, jak zabezpieczyć poufne i wrażliwe informacje przed ich przekazaniem na zewnątrz.

Instalacja i wdrożenie

Zaletą programu jest szybkie wdrożenie. Instalacja konsoli zarządzania, w tym wgranie licencji, ustawienie podstawowych polityk zabezpieczeń i założenie użytkowników, aż do momentu rozpoczęcia zdalnego szyfrowania dysków na jednej z testowych maszyn, zajęła nam mniej niż godzinę i to bez przeszukiwania kolejnych stron dokumentacji i kontaktowania się z helpdeskiem producenta.

Nie byłoby to możliwe, gdyby nie jeden z ważniejszych elementów oprogramowania, a mianowicie serwer pośredniczący (proxy) w chmurze producenta, który zapewnia płynną komunikację między stacjami roboczymi a serwerem zarządzania. Dzięki temu polityki zabezpieczeń, zadania do wykonania i licencje mogą być dostarczane użytkownikom mobilnym bez konieczności zestawiania przez nich połączeń VPN do sieci firmowej. Oczywiście istnieje możliwość uruchomienia lokalnego serwera proxy, jeśli polityka bezpieczeństwa firmy zabrania przesyłania informacji do chmury. Właściwa konsola zarządzania może zostać zainstalowana na serwerze Windows, a w przypadku najmniejszych firm również na zwykłym komputerze z Windows. Ciekawym kierunkiem rozwoju tego narzędzia byłoby udostępnienie wersji konsoli zarządzania w chmurze, co jeszcze bardziej uprościłoby proces wdrożenia i późniejszego utrzymania. Na razie ta opcja jest niedostępna.

Integracja z Active Directory umożliwia m.in. zdalne dostarczanie agentów usługi na komputery pracowników, wystawianie i aktywowanie licencji oraz używanie tych samych poświadczeń do odblokowania dysku, co w przypadku logowania do komputera. Dane użytkowników są synchronizowane z usługą katalogową firmy.

Funkcjonalność

DESlock+ oferuje szereg mechanizmów odzyskiwania dostępu do zaszyfrowanego dysku w sytuacji, gdy chodzi o komputer byłego pracownika lub gdy użytkownik zapomni hasło. Program umożliwia zdefiniowanie wielu użytkowników, dzięki czemu konto administratora odblokowuje dostęp do komputera. Na żądanie użytkownika administrator może wygenerować jednorazowy kod odblokowujący (funkcja challenge & response), a w ostateczności, np. jeśli uszkodzono system operacyjny, skorzystać z płyty ratunkowej. W programie brakuje nieco wsparcia dla certyfikatów cyfrowych, tokenów sprzętowych albo czytników biometrycznych, które mogłyby stanowić alternatywną metodę uwierzytelniania dla standardowych haseł i kluczy. Mimo to DESlock+ pozostaje bardzo dobrym programem do szyfrowania danych, który robi to, co do niego należy, a więc wszechstronnie zabezpiecza stacje robocze Windows i informacje przekazywane między pracownikami. ■

DESlock+ Pro

Plusy:

- łatwe i szybkie wdrożenie,
- wiele opcji szyfrowania, w tym całych powierzchni dysków (FDE),
- serwer proxy w chmurze,
- wtyczka do Microsoft Outlook.

Minusy:

- brak wsparcia dla biometrii, tokenów i certyfikatów cyfrowych,
- brak konsoli zarządzania w chmurze.