Informacje o technologii

Opcje wdrożenia funkcjonalności Instant Secure Erase firmy Seagate

Wprowadzenie

Gdy dyski twarde są wycofywane z użytku i opuszczają centra danych, trafiając do rąk osób trzecich, dane znajdujące się na tych dyskach są narażane na znaczne ryzyko. Niemniej jednak, działy informatyczne nadal muszą rutynowo usuwać i pozbyć się dysków z różnych powodów, takich jak:

- zmiana przeznaczenia dysków do innych zastosowań związanych z pamięcią masową,
- zwrot dysków zgodnie z umową gwarancyjną, w celu dokonania naprawy lub po wygaśnięciu umów dzierżawy.

Prawie każdy dysk twardy trafia poza kontrolę właściciela po jego ostatecznym usunięciu z centrum danych; w rzeczywistości, firma Seagate szacuje, że codziennie z centrów danych wycofuje się z użytkowania 50 000 dysków. Dane firmowe i osobiste są przechowywane na tego typu dyskach, a po ich usunięciu z centrum danych mogą zostać odczytane z większości dysków. Nawet dane rozmieszczone na wielu dyskach w macierzach RAID mogą zostać skradzione, ponieważ rozmiar typowego pojedynczego modułu we współczesnych macierzach o dużej pojemności jest dostatecznie duży, aby pomieścić setki nazwisk i numery ubezpieczenia społecznego.

Opcje wdrożenia funkcjonalności Instant Secure Erase firmy Seagate

Problemy związane z kontrolą nad dyskami i kosztami likwidacji

Aby uniknąć kradzieży danych i konieczności powiadamiania klientów, wymaganego zgodnie z przepisami dotyczącymi ochrony danych, firmy korzystają z niezliczonej liczby metod wymazywania danych na dyskach wycofywanych z użytku przed przekazaniem ich do odbiorców zewnętrznych i ewentualnie osób nieupoważnionych. Aktualne procedury wycofywania dysku z użytkowania, nastawione na uniemożliwienie odczytu danych, zmuszają do zatrudniania wielu pracowników, powodując występowanie zagrożenia związanego z błędami technicznymi i ludzkimi.

W aktualnych procedurach wycofania dysków z użytkowania istnieje mnóstwo wad w aktualnych procedurach wycofania dysków z użytkowania o dalekosiężnych skutkach:

- zastępowanie danych na dyskach jest kosztowne i wiąże się z wykorzystaniem cennych zasobów systemowych przez wiele dni. Żadne powiadomienie o zakończeniu nie jest generowane przez dysk, a podczas zastępowania nie są uwzględniane ponownie przydzielane sektory, przez co dane zostają wyeksponowane;
- rozmagnesowanie lub fizyczne zniszczenie dysku jest kosztowne. Trudno jest zapewnić siłę rozmagnesowania optymalną dla danego typu dysku, dlatego na dysku mogą nadal pozostać czytelne dane. Fizyczne niszczenie dysku jest niebezpieczne dla środowiska, a żadna z tych metod nie umożliwia zwrotu dysku na gwarancji lub w związku z wygaśnięciem dzierżawy;
- niektóre firmy uznały, że jedyną metodą bezpiecznego wycofania dysków z użytku jest zachowanie ich pod własną kontrolą, tzn. przechowywanie bezterminowo w magazynach. Ta metoda nie zapewnia jednak pełnej ochrony, ponieważ w przypadku znacznej liczby dysków nie można wykluczyć ryzyka utraty lub kradzieży części z nich;
- inne firmy korzystają z profesjonalnych usług związanych z utylizacją dysków, co stanowi drogie rozwiązanie obejmujące koszty wykonania usług i sporządzenie wewnętrznych protokołów i koszty kontroli. Ponadto transport dysku do firmy świadczącej odpowiednie usługi powoduje zagrożenie danych znajdujących się na dyskach. Utrata zaledwie jednego dysku może być źródłem strat na poziomie milionów dolarów, związanych z naruszeniem przepisów dotyczących ochrony danych.

Problemy związane z wydajnością, skalowaniem i złożonością zmusiły jednak działy informatyczne do odrzucenia strategii wymagających szyfrowania. Ponadto szyfrowanie jest uważane za ryzykowne przez tych, którzy nie znają dobrze procesu zarządzania kluczami, decydującego o zdolności firmy do odszyfrowania własnych danych. Dyski samoszyfrujące (SED) umożliwiają rozwiązanie wszystkich powyższych problemów, zapewniając łatwe i oszczędne szyfrowanie danych i wycofywanie dysków z użytkowania.

Funkcjonalność Seagate Instant Secure Erase [natychmiastowego usuwania danych] umożliwia bezpieczne, szybkie i oszczędne wycofanie dysku z użytkowania lub zmianę jego przeznaczenia

Dyski SED szyfrują wszystkie dane użytkownika w momencie wprowadzenia ich na dysk za pomocą klucza szyfrowania danych przechowywanego bezpiecznie w napędzie. W związku z tym wszystkie dane zapisane na dysku SED są szyfrowane domyślnie. W przypadku konieczności wycofania z użytku lub zmiany przeznaczenia dysku, właściciel wysyła do dysku polecenie w celu realizacji funkcji natychmiastowego usuwania danych (Seagate Instant Secure Erase - ISE). Funkcjonalność Seagate ISE wykorzystuje możliwość dysku SED kryptograficznego wymazywania w celu zmiany klucza szyfrowania danych[1]. Wymazywanie kryptograficzne bezpiecznie zastępuje klucz szyfrowania na dysku SED, tak jak pokazano na rysunku 1. W przypadku zmiany klucza pierwotnie użytego do zaszyfrowania danych, wszelkie dane zaszyfrowane tym kluczem stają się nieczytelne, a ich odzyskanie w przyszłości będzie niemożliwe. W ten sposób, funkcjonalność Seagate ISE natychmiast, bezpiecznie i skutecznie niszczy dane zapisane na urządzeniu, umożliwiając wycofanie dysku z użytkowania, bądź jego ponowne wykorzystanie lub odsprzedaż. Niezależnie od zastosowanych metod wdrożenia, dyski SED zmniejszają koszty operacyjne działu informatycznego, uwalniając go od problemów związanych z kontrolowaniem napędów i kosztami utylizacji. Dyski SED firmy Seagate wykorzystują technologię ochrony danych na poziomie wymaganym przez agencje rządowe, zapewniając bezpieczeństwo w zakresie zgodności z ochroną prywatności, bez ograniczania skuteczności działu informatycznego. Ponadto dyski SED upraszczają likwidację sprzętu i chronią jego wartość w przypadku zwrotów i wykorzystania do innych celów:

- eliminacja konieczności zastępowania danych lub niszczenia dysku,
- ochrona dysków zwracanych na gwarancji lub w związku z wygaśnięciem dzierżawy,
- możliwość bezpiecznej zmiany przeznaczenia lub odsprzedaży dysków.

Rysunek 1. Proces wdrożenia funkcji Seagate Instant Secure Erase

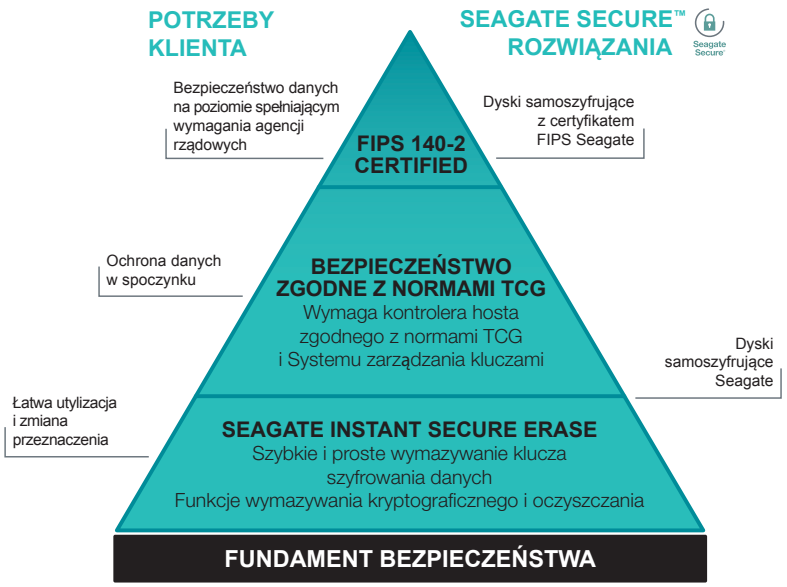
[1] Firma Seagate współpracuje z wieloma liderami w branży i agencjami rządowymi nad opracowaniem standaryzacji niszczenia danych za pomocą wymazywania kryptograficznego; odbywa się to w ramach ISO (Międzynarodowej Organizacji Normalizacyjnej) na podstawie normy ISO/IEC WD 27040.

Opcje wdrożenia funkcjonalności Instant Secure Erase firmy Seagate

Różne rozwiązania firmy Seagate dla różnych potrzeb w zakresie bezpieczeństwa

Wszystkie dyski SED klasy korporacyjnej firmy Seagate zapewniają funkcjonalność Seagate ISE. Sposób, w jaki się to osiąga, zależy od tego, jaki został ustalony poziom bezpieczeństwa po wprowadzeniu dysku do użytkowania. Każdy poziom obejmuje funkcje ochrony poprzednich poziomów.

- Ochrona danych w stanie spoczynku i w postaci zamknięcia wskazującego na próbę otwarcia (FIPS 140-2 Level 2)
- Ochrona danych w stanie spoczynku
- Tylko ochrona związana ze zmianą przeznaczenia (Seagate ISE)



Rysunek 2. Rozwiązania Seagate Secure™ dla każdego poziomu wdrożenia bezpieczeństwa

Odpowiednie metody wymazywania dla każdej z tych wstępnych konfiguracjach wyszczególniono w tabeli 1. Dla klientów firmy Seagate posiadających gruntowną wiedzę w zakresie poleceń SCSI lub ATA i kodowania możliwe jest również stworzenie autorskiego rozwiązania do użytkowania dysków SED firmy Seagate z zestawami poleceń i specyfikacji TCG Storage, T10, T13. Aby uzyskać dodatkowe informacje skontaktuj się z przedstawicielem handlowym firmy Seagate.

Jak dyski samoszyfrujące Seagate realizują funkcjonalność Instant Secure Erase

Dyski SED firmy Seagate wykorzystują jedną lub więcej metod realizacji funkcjonalności Seagate ISE w zależności od zestawu poleceń interfejsu i konfiguracji napędu. Na przykład, urządzenie z interfejsem SATA może dysponować różnymi możliwościami wymazywania w porównaniu z urządzeniem z interfejsem SAS. Ponadto, dodatkowe zabezpieczenia i możliwości wymazywania są dostępne za pośrednictwem protokołu bezpieczeństwa w specyfikacji TCG Storage obsługiwanego przez dyski SED. W każdych okolicznościach kontroler hosta musi implementować obsługę funkcjonalności Seagate ISE poprzez obsługiwane polecenie.

1. Napędy skonfigurowane z ochroną danych w stanie spoczynku, posiadające lub nieposiadające ochrony w postaci zamknięcia wskazującego na próbę otwarcia, są włączane przy użyciu protokołów TCG klasy korporacyjnej.

   Urządzenie zarządzane poprzez protokół w specyfikacji TCG Storage obsługuje funkcjonalność Seagate ISE na poziomie pasma. Poza ochroną danych użytkownika podczas użytkowania dysku, funkcjonalność Seagate ISE na poziomie pasma pozwala wymazywać część lub wszystkie dane przechowywane na urządzeniu bez wpływu na inne pasma danych na dysku. W ten sposób wymazywanie danych odbywa się za pomocą protokołu zabezpieczeń w specyfikacji TCG Storage (metoda Erase) w każdym paśmie, co wymaga oprogramowania firm trzecich.

   Urządzenie zarządzane za pomocą protokołu w specyfikacji TCG Storage można również natychmiast wymazać, wywołując metodę RevertSP protokołu zabezpieczeń. Tego rodzaju bezpieczne wymazywanie wymaga posiadania urządzenia do odczytywania 32-znakowego identyfikatora PSID (Physical Secure ID), wydrukowanego na etykiecie i bezpiecznie wymazuje dysk, przywracając go do oryginalnego stanu fabrycznego.

2. Napędy konfigurowane w trybie wyłącznie ochrony łatwego kasowania i zmiany przeznaczenia są włączane za pomocą komend ATA Security.

   Dysk SED firmy Seagate realizujący zestaw poleceń ATA zostaje wymazany, przywołując polecenia ATA Security Erase Prepare oraz Security Erase Unit. Należy pamiętać, że jest to unikalne wdrożenie funkcjonalności Seagate ISE firmy Seagate.

Opcje wdrożenia funkcjonalności Instant Secure Erase firmy Seagate

Tabela 1 prezentuje w zarysie różne metody wdrożenia funkcjonalności ISE firmy Seagate na dyskach SED. Patrz uwagi w poniższej tabeli.

Tabela 1. Opcje funkcjonalności Seagate Instant Secure Erase

Wstępna konfiguracja	**Ochrona danych w stanie spoczynku z ochroną lub bez ochrony w postaci zamknięcia wskazującego na próbę otwarcia**		**Tylko ochrona w zakresie zmiany przeznaczenia**	**Brak włączonego zabezpieczenia**
Metoda wymazywania	**Protokół zabezpieczeń TCG** Erase	**Protokół zabezpieczeń TCG** RevertSP	**ATA Security** Polecenia Security Erase Prepare i Security Erase Unit	**Sanitize** Zestaw funkcji/polecenie Sanitize
Obsługiwana konfiguracja	Dyski SED firmy Seagate z pamięcią masową zgodną ze specyfikacją TCG	Dyski SED firmy Seagate z pamięcią masową zgodną ze specyfikacją TCG	Dyski SED firmy Seagate z interfejsem SATA	Obsługiwane dyski SED firmy Seagate z interfejsami SATA i SAS
Zakres wymazywania	Wymazywanie kryptograficzne na poziomie pasma	Cały dysk zostaje kryptograficznie wymazany	Cały dysk zostaje kryptograficznie wymazany	Cały dysk zostaje kryptograficznie wymazany
Efekt uboczny	Odblokowuje pasmo i resetuje hasło pasma	Dysk SED powraca do stanu fabrycznego	Odblokowuje dysk i wyłącza funkcję trybu bezpieczeństwa ATA	Brak początkowego bezpieczeństwa zapobiegającego przypadkowemu wymazaniu
Kontrola dostępu	Wymagane jest uwierzytelnianie za pomocą hasła zarządzanego przez hosta lub domyślnego	Wymagane jest uwierzytelnianie za pomocą wydrukowanego hasła (w postaci kodu kreskowego) na etykiecie napędu	Wymagane jest uwierzytelnianie za pomocą hasła zarządzanego przez hosta	Nieuwierzytelnione przez konstrukcję (jeśli dysk jest zablokowany, użytkownik musi odblokować dysk przed wykonaniem operacji)
Zalety	Ochrona danych w stanie spoczynku Walidacja zgodna ze standardem FIPS 140-2 Level 2 W pełni funkcjonalny interfejs zarządzania bezpieczeństwem oparty o specyfikację pamięci masowej zgodnej ze specyfikacją TCG	Ochrona danych w stanie spoczynku Walidacja zgodna ze standardem FIPS 140-2 Level 2 W pełni funkcjonalny interfejs zarządzania bezpieczeństwem oparty o specyfikację pamięci masowej zgodnej ze specyfikacją TCG	Zabezpieczenie na poziomie napędu z interfejsem ATA Wykorzystuje standardowe polecenia ATA Security	Zapewnia bezpieczne wymazywanie bez obciążenia związanego zarządzaniem (tj. zarządzanie hasłem nie jest wymagane)
Uwagi	Wymaga sprzętu lub oprogramowania zgodnego ze specyfikacją TCG	Wymaga fizycznego posiadania dysku SED do odczytania kodu zabezpieczającego dysk	Wykorzystuje standardowe polecenia ATA Security	Możliwość błędnego lub umyślnego wymazania danych ze względu na polecenie o niezabezpieczonym charakterze

Uwagi

1. W większości przypadków, metoda bezpiecznego wymazywania dysku w wyższych konfiguracjach zabezpieczeń będzie działać również w przypadku stosowania jej przy niższych ustawieniach bezpieczeństwa, na przykład, protokół RevertSP będzie działać na dysku skonfigurowanym w trybie ATA, przy założeniu, że napęd obsługuje również zestaw poleceń TCG (obsługa zabezpieczeń może różnić się w zależności od modelu dysku).
2. Termin *ochrona danych w stanie spoczynku* odnosi się do zdolności zapewnienia przez dysk samoszyfrujący (SED) bardzo silnej ochrony przed ujawnieniem danych na dysku, który został skonfigurowany tak, aby zablokować interfejs danych przed nieautoryzowanym dostępem w funkcjonującym otoczeniu komputerowym.
3. Publikacja Federal Information Processing Standard (FIPS) 140-2 to ustanowiony przez rząd amerykański standard bezpieczeństwa komputerowego stosowany do akredytacji modułów kryptograficznych. Nosi tytuł *Security Requirements for Cryptographic Modules (FIPS PUB 140-2)* (Wymogi bezpieczeństwa dla modułów kryptograficznych) i jest publikowany przez Narodowy Instytut Standardów i Technologii (NIST). Ten standard określa wymogi bezpieczeństwa, które zostaną spełnione przez moduł kryptograficzny stosowany w ramach systemu bezpieczeństwa chroniącego dane klasy *Sensitive but Unclassified* (Wrażliwe, ale nie tajne) i *Protected* (Chronione). Dyski w standardzie FIPS firmy Seagate posiadają certyfikat bezpieczeństwa 2. poziomu (zamknięcie wskazujące na próbę otwarcia); więcej informacji dostępnych jest na stronie: www.seagate.com/docs/pdf/whitepaper/mb605_fips_140_2_faq.pdf

Opcje wdrożenia funkcjonalności Instant Secure Erase firmy Seagate

Jak wykorzystać funkcjonalność Instant Secure Erase na dysku SED firmy Seagate

W zależności od rodzaju dysku SED i opcji wybranej w celu bezpiecznego wymazania urządzenia, dane można usunąć rzeczywiście na różne sposoby. Dostępne są następujące rozwiązania:

- oprogramowanie Seagate SeaTools™ dla systemu operacyjnego Windows: darmowe narzędzie dla komputerów PC służące do diagnozowania zarówno wewnętrznie jak i zewnętrznie podłączonych urządzeń pamięci masowej. Oprogramowanie SeaTools obsługuje funkcjonalność Seagate ISE. Oprogramowanie SeaTools znajduje się pod adresem www.seagate.com w zakładce Support and Downloads, pod SeaTools – Diagnosis Software;
- standardowe rozwiązania stron trzecich: używanie kontrolerów RAID firm LSI i Intel lub rozwiązania do zarządzania pełnym kluczem firmy IBM (Tivoli Key Lifecycle Manager), Wave, Winmagic itp;
- niestandardowe/wbudowane rozwiązanie: (własna) opracowana możliwość zintegrowana w systemie lub aplikacji hosta zapewniająca obsługę funkcjonalności Seagate ISE. Aby uzyskać dodatkowe informacje, skontaktuj się z przedstawicielem handlowym firmy Seagate.

Bibliografia

Specyfikacje TCG Storage –
www.trustedcomputinggroup.org/developers/storage/specifications

Specyfikacje ATA –
www.t13.org/

Specyfikacje SCSI –
www.t10.org/

Oprogramowanie Seagate SeaTools –
http://www.seagate.com/pl/pl/support/downloads/seatools/

www.seagate.com

Seagate Secure®

AMERYKA PŁN. I PŁD. Seagate Technology LLC 10200 South De Anza Boulevard, Cupertino, California 95014, USA, +1 408 658 1000
AZJA/PACYFIK Seagate Singapore International Headquarters Pte. Ltd. 7000 Ang Mo Kio Avenue 5, Singapur 569877, +65 6485 3888
EUROPA, BLISKI WSCHÓD I AFRYKA Seagate Technology SAS 16-18 rue du Dôme, 92100 Boulogne-Billancourt, Francja, +33 1 41 86 10 00

© 2012 Seagate Technology LLC. Wszelkie prawa zastrzeżone. Wydrukowano w USA. Seagate, Seagate Technology i logo Wave są zastrzeżonymi znakami towarowymi firmy Seagate Technology LLC w Stanach Zjednoczonych i/lub innych krajach. Seagate Secure i logo Seagate Secure są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Seagate Technology LLC lub jednej z jej firm zależnych w Stanach Zjednoczonych i/lub innych krajach. Logo FIPS jest znakiem certyfikacyjnym instytutu NIST, co nie oznacza faworyzowania produktu przez instytut NIST ani rządy Stanów Zjednoczonych lub Kanady. Wszystkie pozostałe znaki towarowe i zastrzeżone znaki towarowe należą do odpowiednich właścicieli. Eksport i reeksport sprzętu lub oprogramowania szyfrującego może podlegać regulacjom prawnym Biura Przemysłu i Bezpieczeństwa Departamentu Handlu Stanów Zjednoczonych (więcej informacji znajduje się w witrynie www.bis.doc.gov), a import do krajów i użytkowanie poza terenem Stanów Zjednoczonych może podlegać ograniczeniom. Firma Seagate zastrzega sobie prawo do wprowadzania zmian w ofercie produktów lub w ich parametrach bez powiadomienia. TP627.1-1203PL, marzec 2012