Informacje o technologii

Dyski samoszyfrujące do serwerów i macierzy dyskowych NAS i SAN

Przegląd

W tym dokumencie omówiono problemy związane z ochroną danych na dyskach twardych, które zazwyczaj nie zawsze pozostają pod kontrolą właściciela. Przedstawiono dyski samoszyfrujące (SED, Self-Encrypting Drives) wykorzystywane na dwa sposoby: szybkie bezpieczne wymazywanie (kryptograficzne kasowanie lub uniemożliwianie odczytu danych) i automatyczne blokowanie w celu zabezpieczenia aktywnych danych w przypadku zaginięcia lub kradzieży dysku z systemu podczas użytkowania. Uwzględniono dwa załączniki. W pierwszym porównano dyski SED z innymi technologiami szyfrowania używanymi do ochrony danych na dyskach. W drugim przedstawiono szczegółową analizę szybkiego bezpiecznego wymazywania i technologii automatycznego blokowania SED oraz zastosowania dysków SED w serwerach, macierzach NAS i SAN, środowiskach wirtualnych, macierzach RAID i JBOD oraz indywidualnych dyskach.

Wprowadzenie

Gdy dyski twarde są wycofywane z użytku i przekazywane poza fizycznie izolowane, chronione centra danych do rąk innych osób, dane znajdujące się na tych dyskach są narażane na znaczne ryzyko. Działy IT rutynowo wycofują dyski z użytku między innymi z następujących powodów:

- zwrot dysków zgodnie z umową gwarancyjną, w celu wykonywania napraw lub po wygaśnięciu umów dzierżawy
- usuwanie i likwidacja dysków
- wykorzystanie dysków do innych zastosowań związanych z pamięcią masową

Prawie wszystkie dyski w końcu opuszczają centrum danych i nie pozostają pod kontrolą właścicieli. Firma Seagate szacuje, że około 50 000 dysków jest codziennie wycofywanych z użytku w centrach danych. Dane firmowe są przechowywane na dyskach tego typu i mogą być odczytane z większości dysków usuniętych z centrum danych. 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 zawierać setki nazwisk i numerów identyfikacyjnych.

Dyski samoszyfrujące do serwerów i macierzy dyskowych NAS i SAN

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. W przypadku aktualnych procedur wycofywania z użytku, ukierunkowanych na uniemożliwienie odczytu danych, konieczne jest zatrudnianie wielu pracowników, dlatego występuje zagrożenie związane z błędami technicznymi i ludzkimi.

Wady aktualnych procedur wycofania dysków z użytku są liczne i związane z poważnymi skutkami w dłuższej perspektywie czasowej:

- 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 są narażone.
- Rozmagnesowanie lub fizyczne niszczenie dysku jest kosztowne. Trudno jest zapewnić optymalizację siły rozmagnesowania zgodnie z typem dysku, dlatego na dysku mogą nadal pozostać czytelne dane. Fizyczne niszczenie dysku jest niebezpieczne dla środowiska, a żadna z tych metod nie umożliwia zwrócenia dysku w związku z umową gwarancyjną lub 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 uniknąć zagubienia lub kradzieży niektórych z nich.
- Inne firmy korzystają z profesjonalnych usług związanych z likwidacją dysków. W tym wypadku należy jednak uwzględnić koszty pozyskania usług oraz przygotowania wewnętrznych raportów i inspekcji. Ponadto transport dysku do firmy świadczącej odpowiednie usługi powoduje zagrożenie danych znajdujących się na dyskach. Utrata tylko jednego dysku może być źródłem strat na poziomie milionów dolarów, związanych z naruszeniem przepisów dotyczących ochrony danych.

Uwzględniając powyższe wady, można było przewidzieć rezultaty studium przeprowadzonego przez firmę IBM. Ustalono, że 90 procent dysków zwróconych do IBM zawierało czytelne dane. Jaki z tego wniosek? Problemem nie jest dysk usuwany z centrum danych, ale dane przechowywane na dysku.

Szyfrowanie

Codziennie tysiące terabajtów danych jest usuwanych z centrów danych w związku z wycofywaniem przestarzałych systemów z użytku. Czy ten problem występowałby, gdyby wszystkie dane na tych dyskach twardych były automatycznie szyfrowane, co umożliwiałoby natychmiastowe i bezpieczne wymazywanie? W większości stanów USA obecnie obowiązują przepisy dotyczące ochrony danych, które wykluczają szyfrowane dane z obowiązku rejestrowania wypadków ujawniania danych osobom nieupoważnionym. Należy również zauważyć, że koszt ujawnienia danych jest wysoki — przeciętnie 6,6 miliona USD[1].

Problemy związane z wydajnością, skalowaniem i złożonością doprowadziły jednak działy IT do odrzucania strategii wymagających szyfrowania. Ponadto szyfrowanie uważane jest za ryzykowne przez firmy nie znające dobrze procesu zarządzania kluczami, który decyduje o zdolności firmy do odszyfrowania własnych danych. Dyski samoszyfrujące umożliwiają rozwiązanie wszystkich powyższych problemów, zapewniając łatwe i ekonomiczne szyfrowanie danych i wycofywanie dysków.

Omówimy dwa scenariusze zabezpieczeń:

- dyski SED zapewniające szybkie bezpieczne wymazywanie danych bez konieczności zarządzania kluczami
- automatycznie blokowane dyski SED ułatwiające ochronę aktywnych danych przed kradzieżą z zarządzaniem kluczami w całym cyklu użytkowania

[1] Studium roczne 2008: Cost of a Data Breach, Ponemon Institute, luty 2009

Dyski samoszyfrujące do serwerów i macierzy dyskowych NAS i SAN

Szybkie bezpieczne wymazywanie danych bez zarządzania kluczami

Dysk samoszyfrujący zapewnia szybkie niszczenie danych przy użyciu metody wymazywania kryptograficznego. Podczas korzystania z dysku SED właściciel nie musi zarządzać kluczami uwierzytelniania (zwanymi również poświadczeniami lub hasłami), aby uzyskać dostęp do danych znajdujących się na dysku. Dysk SED szyfruje zapisywane dane i odszyfrowuje odczytywane dane, nie wymagając od właściciela klucza uwierzytelniania.

Jeżeli konieczne jest wycofanie z użytku lub wykorzystanie dysku do innych celów, właściciel wysyła do dysku polecenie w celu kryptograficznego wymazania danych. Wymazywanie kryptograficzne polega po prostu na zastąpieniu klucza szyfrowania wewnątrz dysku i uniemożliwieniu odszyfrowania danych zabezpieczonych przy użyciu usuniętego klucza. (Bezpieczne wymazywanie bardziej szczegółowo omówiono w załączniku A.)

Dyski samoszyfrujące umożliwiają redukcję kosztów operacyjnych dzięki zwolnieniu personelu IT z obowiązku kontrolowania i likwidacji dysków. Technologia ochrony danych SED na poziomie wymaganym w przypadku agencji rządowych zapewnia zgodność z przepisami bez ograniczania efektywności personelu IT. 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 w związku z umową gwarancyjną lub wygaśnięciem dzierżawy
- możliwość bezpiecznego wykorzystania dysków do innych celów

Automatycznie blokowane dyski samoszyfrujące z zarządzaniem kluczami w całym cyklu użytkowania

Oprócz wykorzystania dysku samoszyfrującego do szybkiego bezpiecznego wymazywania po wycofaniu z użytku właściciel dysku może również wykorzystać dysk SED w trybie automatycznego blokowania w celu zabezpieczenia aktywnych danych przed kradzieżą. Kradzieże wewnętrzne lub ginięcie dysków to poważny problem dla firm niezależnie od ich wielkości. Ponadto w przypadku biur oddziałów i małych firm, które nie dysponują silnymi fizycznymi zabezpieczeniami, dyski są bardziej narażone na kradzież zewnętrzną.

Wykorzystanie dysku SED w trybie automatycznego blokowania wymaga tylko zabezpieczenia dysku podczas normalnego użytkowania kluczem uwierzytelniania.

Po zabezpieczeniu w ten sposób klucz szyfrowania danych przechowywanych na dysku jest blokowany zawsze po wyłączeniu zasilania dysku. Mówiąc inaczej, wyłączenie zasilania dysku SED powoduje automatyczne zablokowanie znajdujących się na nim danych.

Po ponownym włączeniu zasilania dysku SED wymagane jest uwierzytelnianie przed odblokowaniem klucza szyfrowania i odczytaniem danych znajdujących się na dysku. Zapewnia to ochronę danych w wypadku zgubienia lub kradzieży dysku przez pracowników lub osoby spoza firmy.

Cykl użytkowania kluczy uwierzytelniania może być zarządzany przez program IBM Tivoli Key Lifecycle Manager (dotychczas Encryption Key Manager), zgodny z technologią Java, który generuje, chroni i przechowuje klucze uwierzytelniania w centralnej lokalizacji i wykonuje kopie zapasowe kluczy. Ujednolicona usługa zarządzania kluczami może być odpowiedzią na wymagania dotyczące zarządzania kluczami dla wszystkich form pamięci masowej (oraz innych zabezpieczeń). Firmy IBM, LSI i Seagate zapewniają zgodność z protokołem współdziałania w zarządzaniu kluczami (Key Management Interoperability Protocol), przekazanym organizacji OASIS w celu rozpowszechnienia w procesie wprowadzania otwartych standardów. Dzięki niezależności od platformy program IBM Tivoli Key Lifecycle Manager umożliwia proste i efektywne zarządzanie coraz większą liczbą kluczy szyfrowania w przedsiębiorstwie.

Tryb automatycznego blokowania dysków samoszyfrujących i program IBM Tivoli Key Lifecycle Manager szczegółowo omówiono w załączniku A.

Właściciel dysku samoszyfrującego może wykorzystać najpierw technologię SED tylko w trybie bezpiecznego wymazywania danych, a następnie przełączyć dysk do trybu automatycznego blokowania. Później po wykonaniu szybkiego bezpiecznego wymazywania danych i przeznaczeniu dysku do innego celu można ponownie przełączyć dysk do trybu bezpiecznego wymazywania danych. Początkowo właściciel dysku może więc pozostawić dysk SED w trybie bezpiecznego wymazywania danych podczas normalnej eksploatacji i kasować dane tylko wówczas, gdy jest to konieczne. Później, na przykład w przypadku wyższego poziomu zagrożenia kradzieżą, właściciel może przełączyć dysk SED do trybu automatycznego blokowania na pozostałą część okresu jego eksploatacji, tworząc po prostu klucz uwierzytelniania obudowujący istniejący klucz szyfrowania. Następnie, po pomyślnym wymazaniu danych i przystosowaniu dysku SED do innego zastosowania, nowy właściciel może zrezygnować z automatycznego blokowania i przełączyć dysk do trybu bezpiecznego wymazywania danych, aby bezpiecznie oczyścić dysk po zakończeniu okresu użytkowania.

Dyski samoszyfrujące do serwerów i macierzy dyskowych NAS i SAN

Wykorzystanie dysków samoszyfrujących w trybie szybkiego bezpiecznego wymazywania danych jest bardzo efektywną i skuteczną metodą ochrony dysków wycofywanych z użytku. Jednak korzystanie z dysków SED w trybie automatycznego blokowania ma jeszcze większe zalety. Mówiąc krótko, od chwili usunięcia dysku lub systemu z centrum danych (legalnie lub bez autoryzacji) dysk jest blokowany. Administrator centrum danych nie musi planować lub podejmować żadnych dodatkowych działań w celu ochrony tych danych. Takie rozwiązanie ułatwia zapobieganie naruszeniu przepisów dotyczących ochrony danych w przypadku nieprawidłowego obchodzenia się z dyskiem i zabezpieczenie danych w wypadku kradzieży dysku przez pracowników lub inne osoby.

Porównanie technologii ochrony danych na dyskach twardych

Żadna technologia szyfrowania nie zapewnia skutecznej ochrony wszystkich danych przed wszelkimi zagrożeniami. Różne technologie są używane do ochrony przed poszczególnymi zagrożeniami. Na przykład dyski samoszyfrujące ułatwiają zabezpieczanie danych przed zagrożeniami występującymi wówczas, gdy dysk nie znajduje się pod kontrolą właściciela, jednak nie zawsze mogą chronić dyski w centrum danych. Na przykład osoba, która bez autoryzacji uzyska dostęp do serwera korzystającego z niezablokowanego dysku, może odczytać niezaszyfrowany tekst zapisany na dysku. Należy więc koniecznie pamiętać, że technologia szyfrowania SED nie zastępuje kontroli dostępu do centrum danych, a raczej uzupełnia te zabezpieczenia.

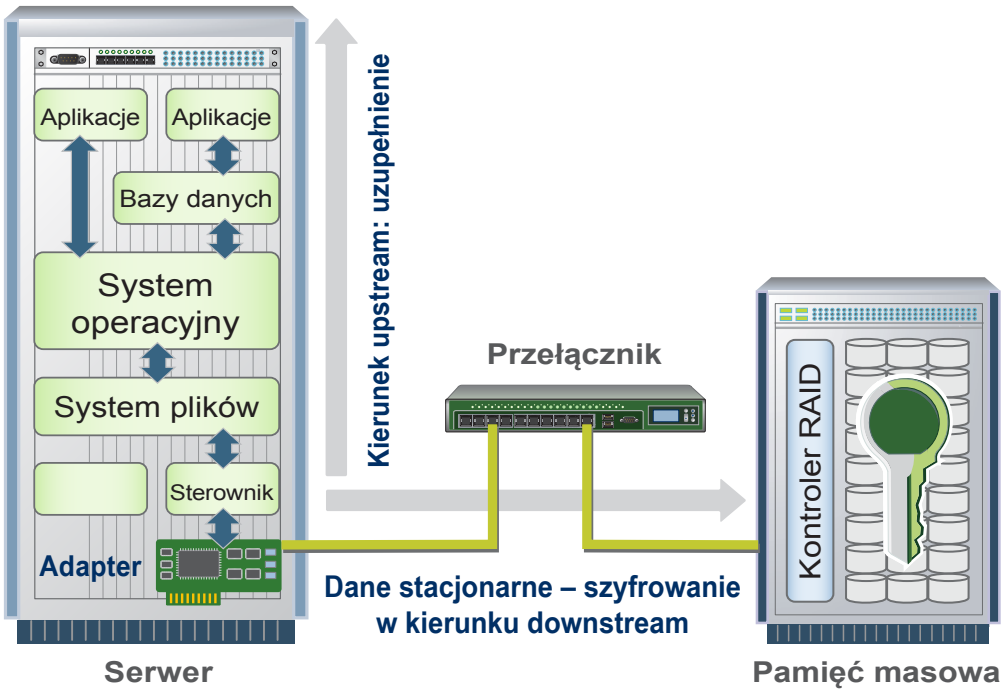
Zabezpieczanie danych stacjonarnych również powinno być uzupełnieniem, a nie zastępstwem ochrony danych mobilnych. Większość danych mobilnych jest przekazywanych kablami w kierunku downstream za pośrednictwem sieci Ethernet (macierze NAS) lub na poziomie bloków (macierze SAN) i pozostaje fizycznie pod kontrolą administratora pamięci masowej w dziale IT, dlatego jest uważana za prawidłowo chronioną. W przypadku danych mobilnych, które nie pozostają pod kontrolą administratora, najbardziej powszechnie akceptowaną i przyjętą metodą szyfrowania jest użycie protokołu IPSec lub FC over IP, w którym krótkotrwałe klucze sesji są wykorzystywane do szyfrowania niewielkich ilości danych. Może wydawać się, że lepszym rozwiązaniem niż ta technika zabezpieczeń sesji jest szyfrowanie w infrastrukturze w celu ochrony danych na dysku twardym: dane są szyfrowane nie tylko na dysku twardym, ale również podczas przekazywania przez infrastrukturę. Ta metoda ma jednak fundamentalną wadę: zamiast podwyższać poziom bezpieczeństwa w rzeczywistości jest przyczyną dodatkowych zagrożeń i wyższego stopnia złożoności na skutek narażenia długotrwałych kluczy szyfrowania. W takich okolicznościach zagrożone są znaczne ilości tekstu chronionego przy użyciu pojedynczego klucza szyfrowania. Jeżeli konieczne jest szyfrowanie danych na dysku mobilnych, należy korzystać z protokołu IPSec lub FC over IP. Szyfrowanie danych na dysku powinno być wykonywane przez sam dysk z przyczyn opisanych poniżej.

Szyfrowanie aplikacji, baz danych, systemu operacyjnego i plików (zob. rysunek 1) to techniki uwzględniające zagrożenia danych przechowywanych na dysku (związane z administratorami baz danych, plików lub systemu albo hakerami), występujące w centrum danych. Ze względu na znaczne ograniczenie wydajności i konieczność wprowadzenia zmian w chronionej aplikacji, bazie danych, systemie operacyjnym lub systemie plików, bez możliwości skalowania, szyfrowanie większych ilości danych jest jednak rozwiązaniem niepraktycznym. Z powodu tego ograniczenia administratorzy rezerwują szyfrowanie tylko dla najważniejszych danych.

Administratorzy są więc zmuszeni do klasyfikacji danych w celu identyfikacji i lokalizacji ważnych danych. Niestety powszechnie wiadomo, że ten proces nie umożliwia identyfikacji wszystkich ważnych danych. Klasyfikacja danych jest uciążliwym, pracochłonnym i trudnym zadaniem zwłaszcza wówczas, gdy ważne informacje mogą być kopiowane z chronionego źródła do niezabezpieczonej lokalizacji docelowej. Ze względu na problemy tego typu na dysku jest zapisywanych zbyt wiele ważnych i niezaszyfrowanych danych, które prawdopodobnie pozostaną na dysku twardym na długo po zakończeniu okresu użytkowania dysku.

Oznacza to, że technologie szyfrowania w kierunku downstream muszą zapewnić pełną ochronę dysku i wyeliminować lukę utworzoną przez nieskuteczną klasyfikację ważnych danych. Te technologie zwalniają osoby chroniące dane z obowiązku klasyfikacji poufności informacji, które nie pozostają pod kontrolą centrum danych (jest to zadanie trudne w zarządzaniu i pociągające dodatkowe koszty). Szyfrowanie w infrastrukturze, kontrolerze macierzy RAID (serwer lub podsystem pamięci masowej) lub na dysku twardym to dostępne opcje. Jednak gdzie należy wykonywać szyfrowanie?

Dyski samoszyfrujące do serwerów i macierzy dyskowych NAS i SAN



Rysunek 1

Kilka lat temu, zanim w firmie Seagate rozpoczęto prace nad szyfrowaniem dysków, pracownicy amerykańskiej Agencji Bezpieczeństwa Narodowego (NSA) przeanalizowali problem bezpieczeństwa danych i doszli do wniosku, że szyfrowanie powinno odbywać się na poziomie dysku twardego. Zgodnie z powszechnie znaną ogólną zasadą strażnicy powinni znajdować się jak najbliżej chronionego obiektu. Podobnie szyfrowanie w dysku twardym jest optymalnym rozwiązaniem, ponieważ właśnie tam znajdują się dane. Dyski SED udostępniają zaawansowaną technologię zapewniającą pełne szyfrowanie dysku i obniżenie całkowitego kosztu posiadania pamięci masowej połączonej bezpośrednio z serwerami oraz macierzą SAN i NAS, oferując równocześnie następujące korzyści:

- **Uproszczone zarządzanie kluczami:** Dysk SED eliminuje konieczność śledzenia klucza szyfrowania danych lub zarządzania nim. W trybie bezpiecznego wymazywania danych śledzenie klucza uwierzytelniania lub zarządzanie nim również nie jest konieczne.
- **Redukcja kosztów dzięki standardowej technologii:** Zastosowanie technologii zgodnej ze standardami branżowymi umożliwia zmniejszenie kosztów i gwarantuje, że jednolita technologia jest używana w odniesieniu do macierzy SAN, NAS, serwerów, komputerów stacjonarnych, notebooków i przenośnych platform pamięci masowej.
- **Optymalna efektywność pamięci masowej:** W przeciwieństwie do niektórych technologii szyfrowania dysk SED umożliwia kompresję danych i eliminację duplikatów w celu maksymalizacji pojemności pamięci masowej.
- **Wyższy poziom integralności danych:** Technologia SED umożliwia wykorzystanie informacji dotyczących ochrony (Protection Information), które będą w przyszłości zapewniać integralność danych, a ponadto nie wpływa na niezawodność lub gwarancję dysku twardego.
- **Maksymalna wydajność i skalowalność:** Technologię SED można wykorzystać przy pełnej szybkości dysku, a ponadto jest przystosowana do skalowania liniowego i automatycznego.
- **Brak klasyfikacji danych:** Kosztowna, czasochłonna klasyfikacja danych nie jest wymagana do uzyskania maksymalnej wydajności.
- **Ograniczone ponowne szyfrowanie:** W przypadku technologii SED można zmniejszyć liczbę cyklów ponownego tworzenia kluczy i szyfrowania, ponieważ klucz szyfrowania danych nigdy nie jest zagrożony.
- **Doskonałe zabezpieczenia:** Agencja NSA zatwierdziła pierwszy model SED. Technologia SED nie osłabia zabezpieczeń na skutek zbędnego szyfrowania w infrastrukturze, które powoduje narażenie długotrwałych bloków zaszyfrowanego tekstu i kluczy. Dyski SED pozostawiają szyfrowanie łączy transmisyjnych (OTW, Over-The-Wire) technologiom służącym do ochrony danych mobilnych.

Dyski samoszyfrujące do serwerów i macierzy dyskowych NAS i SAN

Standaryzacja dysków samoszyfrujących pozwala również mieć nadzieję na obniżenie kosztów zakupu. Sześciu wiodących dostawców dysków twardych współpracowało w celu opracowania ostatecznej specyfikacji zrzeszeniowej opublikowanej przez organizację TCG (Trusted Computing Group). Ta specyfikacja, utworzona jako standard opracowania dysków samoszyfrujących i zarządzania nimi, umożliwia współdziałanie dysków SED oferowanych przez różnych dostawców. Współdziałanie tego typu zapewni prawidłową konkurencję na rynku oraz obniżenie cen zarówno dla integratorów systemów, jak i użytkowników końcowych. Z doświadczeń wynika, że w przypadku produkcji dysków twardych standardy branżowe wielokrotnie przyczyniły się do zwiększenia produkcji i obniżenia kosztów. Ta redukcja kosztów jednostkowych wynikająca ze zwiększenia produkcji gwarantuje, że dodatkowe układy logiczne w kontrolerze ASIC pozostają nieznaczną częścią kosztów materiałowych dysku. (W załączniku B szczegółowo porównano technologie szyfrowania dysków i omówiono zalety technologii SED.)

Podsumowanie

Administratorzy serwerów i macierzy dysków SAN i NAS mają wszelkie powody do szyfrowania swoich danych. Dyski samoszyfrujące (SED) są odpowiednim rozwiązaniem w tym wypadku, a ponadto eliminują czynniki zniechęcające dotychczas niektórych specjalistów IT do szyfrowania danych.

Zalety dysków samoszyfrujących są ewidentne. Szybkie bezpieczne wymazywanie danych umożliwia redukcję kosztów operacyjnych działów IT wycofujących dyski z użytku bez konieczności zarządzania kluczami. Ponadto zachowuje wartość dysku wycofanego z użytku, ponieważ umożliwia bezpieczne przekazanie dysku do innych zastosowań albo zwrot w związku z serwisem, gwarancją lub wygaśnięciem dzierżawy. W trybie automatycznego blokowania dyski SED ułatwiają ochronę danych w przypadku kradzieży lub zgubienia dysku po odłączeniu dysku od systemu. Dysk można przejąć, ale nie oznacza to przejęcia danych.

Dyski samoszyfrujące oferują również atrakcyjne korzyści. Śledzenie klucza szyfrowania lub zarządzanie nim w celu odzyskania danych nie jest konieczne, ponieważ klucz pozostaje w dysku, a właściciel może zawsze odszyfrować swoje dane. Konieczne jest tylko śledzenie klucza uwierzytelniania lub zarządzanie nim. Ten klucz można bezpiecznie zapisywać w kopii zapasowej, replikować i dublować w centrach awaryjnego odzyskiwania danych. Wprowadzanie klucza i zarządzanie nim nie jest w ogóle konieczne, jeżeli dysk SED jest używany tylko w trybie szybkiego bezpiecznego wymazywania danych.

Szyfrowanie SED jest automatyczne i niewidoczne, dzięki czemu nie wymaga kosztownych zmian w procesie zarządzania pamięcią masową, w systemie operacyjnym, aplikacjach i bazach danych. Gwarantowane są znaczne oszczędności wynikające z efektywnego kompresowania i usuwania duplikatów danych w systemie pamięci masowej. Ponadto wydajność jest skalowana liniowo i automatycznie, a wszystkie dane można szyfrować bez ograniczania wydajności, dlatego kosztowna i czasochłonna klasyfikacja danych nie jest konieczna.

Dyski samoszyfrujące są zgodne ze standardami, dlatego umożliwiają optymalne zarządzanie, współdziałanie i efektywność kosztową, a wszyscy wiodący producenci dysków twardych uczestniczyli w opracowaniu tych standardów. Zarządzanie kluczami jest również ujednolicane po przyjęciu przez wiodących dostawców pamięci masowych protokołu współdziałania w zarządzaniu kluczami (Key Management Interoperability Protocol) zaproponowanego przez organizację OASIS. Dyski SED są przystosowane do integracji w standardowych produktach implementowanych zgodnie z typowym harmonogramem uaktualnień pamięci masowej.

Mówiąc prosto, szyfrowanie w dysku jest bardziej ekonomiczne, zapewnia większą wydajność oraz lepsze zarządzanie i ochronę w porównaniu z innymi technologiami szyfrowania. Wielu wybitnych analityków, producentów systemów i szereg agencji rządowych, takich jak NSA, ustaliło, że szyfrowanie powinno być wykonywane w dysku. Wniosek z tego taki: dyski SED są istotnym krokiem w kierunku lepszych zabezpieczeń i niższego całkowitego kosztu posiadania na globalnym rynku serwerów oraz macierzy dysków SAN i NAS.

Uwzględniając, że technologia SED umożliwia obniżenie kosztów wycofania dysków z użytku i rozwiązanie problemów IT, wiele korporacji rozważa wykorzystanie dysków SED w swojej strategii zabezpieczeń. Twórcy strategii zabezpieczeń powinni rozważyć możliwość aktualizacji zasad, tak aby wszystkie nabywane w przyszłości dyski twarde były zgodne z dostępną technologią SED. Firmy IBM i LSI są pionierami uwzględniającymi dyski samoszyfrujące w swoich rozwiązaniach, a firma Seagate szybko wprowadza technologię SED w całej ofercie dysków twardych. Inni dostawcy dysków twardych również wprowadzili technologię SED i wkrótce wszystkie dyski będą oferowane z technologią samoszyfrowania.

Dyski samoszyfrujące do serwerów i macierzy dyskowych NAS i SAN

Załącznik A: Technologia dysków samoszyfrujących (SED)

Nowo zakupione dyski samoszyfrujące

Każdy dysk SED losowo generuje fabryczny klucz szyfrowania, który jest zapisywany na dysku. Technologia SED zapewnia automatyczne pełne szyfrowanie dysku. Przed zapisem na dysku tekst jest szyfrowany (przy użyciu wbudowanego klucza szyfrowania). Podczas operacji odczytu zaszyfrowane dane są odszyfrowywane, zanim opuszczą dysk. Podczas normalnej pracy dysk SED jest bez ograniczeń dostępny dla systemu, podobnie jak każdy niezaszyfrowany dysk. Dysk SED nieustannie wykonuje operacje szyfrowania — nie można przypadkowo wyłączyć tej funkcji.

Po zakupie dysku przez właściciela ten wbudowany klucz jest zapisany w formie zwykłego tekstu do chwili, kiedy dysk zostanie przełączony do trybu automatycznego blokowania, w którym wprowadzany jest klucz uwierzytelniania. Dysk szyfruje i odszyfrowuje wszystkie zapisywane i odczytywane dane, jednak jeżeli klucz uwierzytelniania nie zostanie utworzony, każdy może zapisać na dysku i odczytać dane.

Konfiguracja systemu nie jest skomplikowana. Właściciel musi zdecydować, czy dysk SED będzie używany w trybie automatycznego blokowania czy szybkiego bezpiecznego wymazywania danych. Poniżej omówiono poszczególne tryby.

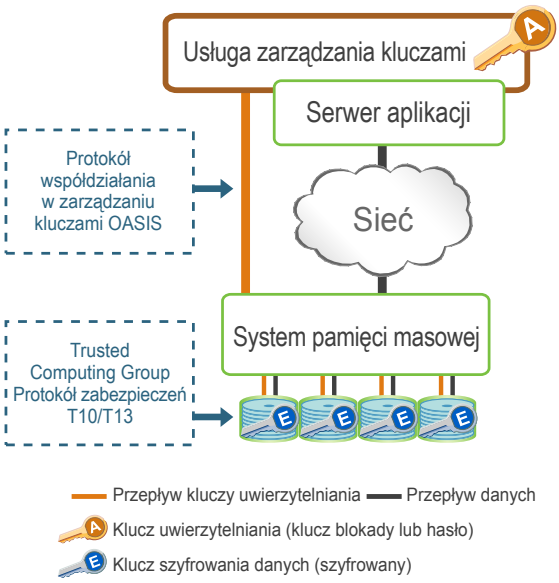
Technologia szybkiego bezpiecznego wymazywania danych

Jeżeli właściciel zamierza używać dysku tylko w trybie szybkiego bezpiecznego wymazywania danych, może po prostu rozpocząć korzystanie z dysku. W trybie szybkiego bezpiecznego wymazywania danych właściciel nie musi używać klucza uwierzytelniania lub hasła do odszyfrowania i odczytywania danych. Takie rozwiązanie eliminuje zagrożenie związane z nieprawidłowym zarządzaniem kluczem uwierzytelniania, które może być przyczyną utraty danych.

Technologia SED znacznie upraszcza przekazanie dysku do innych zastosowań i likwidację zużytego dysku. Właściciel, który zamierza przekazać dysk do innego zastosowania, po prostu kasuje i zastępuje klucz szyfrowania. Dysk usuwa klucz szyfrowania i zastępuje go nowym kluczem generowanym losowo. Po skasowaniu klucza nie można odczytać danych zapisanych na dysku — dane zaszyfrowane przy użyciu poprzedniego klucza są nieczytelne i nie mogą być odszyfrowane przy użyciu nowego klucza (zob. rysunek 2). Dysk jest w stanie, w jakim znajdował się po dostarczeniu z zakładu produkcyjnego, gotowy do przekazania nowemu właścicielowi i wykorzystania w trybie szybkiego bezpiecznego wymazywania danych lub automatycznego blokowania.

Rysunek 2

Dyski samoszyfrujące do serwerów i macierzy dyskowych NAS i SAN



Rysunek 3

Zarządzanie kluczami i dyskami SED w trybie automatycznego blokowania

Jeżeli dysk SED jest używany w trybie automatycznego blokowania, wymagany jest klucz uwierzytelniania ze źródła zewnętrznego, umożliwiający odblokowanie w celu wykonania operacji odczytu/zapisu. Centrum danych zawierające dyski SED w trybie automatycznego blokowania korzysta z: — usługi zarządzania kluczami, która przechowuje i udostępnia klucze uwierzytelniania oraz zarządza nimi, — systemu pamięci masowej, który przekazuje te klucze do odpowiedniego dysku (zob. rysunek 3). Firmy Seagate, IBM i LSI współpracowały w celu konsolidacji swoich technologii i opracowania rozwiązań z pełnym samoszyfrowaniem, takich jak IBM System Storage DS8000 i IBM System Storage DS5000.

Poza tradycyjnymi funkcjami system pamięci masowej udostępnia funkcje definiowania grup bezpiecznych woluminów, pobierania kluczy uwierzytelniania z usługi zarządzania kluczami oraz przesyłania klucza do odpowiedniego dysku. Operację tę przedstawia pomarańczowa linia na rysunku 3. W ten sposób system pamięci masowej ukrywa funkcję szyfrowania przed hostami, systemem operacyjnym, bazami danych i aplikacjami.

Po zakończeniu uwierzytelniania podczas włączania zasilania szyfrowanie nie jest widoczne dla systemu pamięci masowej, który wykonuje tradycyjne funkcje w normalnym trybie. Na rysunku 3 ciemnoszara linia reprezentuje przepływ niezaszyfrowanych danych tekstowych. Systemy pamięci masowej są optymalizowane dla niezaszyfrowanych danych pod względem kompresji danych i eliminacji duplikatów.

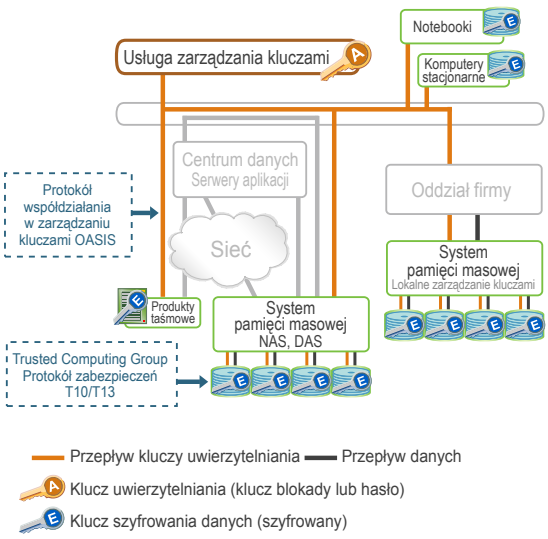
Usługa zarządzania kluczami może wykorzystywać programowe lub sprzętowe magazyny kluczy w celu tworzenia i przypisywania odpowiednich kluczy uwierzytelniania i szyfrowania oraz zarządzania nimi w całym przedsiębiorstwie. Efektywne zarządzanie kluczami powinno być sprawnie zintegrowane z istniejącą strategią zabezpieczeń organizacji, aby zapewniać prawidłową ochronę zarówno usługi, jak i kluczy przed nieautoryzowanym dostępem.

Ponadto efektywny system zarządzania kluczami powinien uwzględniać kopie zapasowe, synchronizację, zarządzanie cyklem użytkowania, inspekcje i przechowywanie długoterminowe. Wdrażanie usługi zarządzania kluczami jest znacznie uproszczone wówczas, gdy można wykorzystać istniejące organizacyjne rozwiązanie zapewniające wysoki poziom dostępności i odzyskiwanie awaryjne.

Program IBM Tivoli Key Lifecycle Manager (dotychczas Encryption Key Manager), zgodny z technologią Java, generuje, chroni, przechowuje i obsługuje klucze uwierzytelniania używane w przypadku samoszyfrujących stacji taśm IBM i systemu IBM System Storage DS8000 z pełnym szyfrowaniem dysków. Jako aplikacja Java IBM Tivoli Key Lifecycle Manager może funkcjonować w systemach operacyjnych z/OS, i5/OS, AIX, Linux, HP-UX, Sun Solaris i Windows, a ponadto może pełnić funkcję udostępnianego zasobu wdrażanego w kilku lokalizacjach w przedsiębiorstwie w celu zapewnienia wysokiego poziomu dostępności tej aplikacji.

Dzięki niezależności od platformy i możliwości wykorzystania istniejących zasad zabezpieczeń oraz środowiska o wysokim poziomie dostępności na najbardziej bezpiecznej platformie serwerowej organizacji program IBM Tivoli Key Lifecycle Manager umożliwia proste i efektywne zarządzanie coraz większą liczbą kluczy szyfrowania w przedsiębiorstwie.

Dyski samoszyfrujące do serwerów i macierzy dyskowych NAS i SAN



Rysunek 4

Program IBM Tivoli Key Lifecycle Manager dostarcza klucze w odpowiednim czasie i umożliwia przechowywanie kluczy w bezpiecznej centralnej lokalizacji. Jest to unikatowe rozwiązanie obsługujące wiele protokołów dostarczania kluczy i zarządzające certyfikatami oraz kluczami symetrycznymi i asymetrycznymi. Użytkownicy mogą również centralnie tworzyć, importować, rozpowszechniać, zapisywać w kopiach zapasowych i archiwizować informacje dotyczące cyklu użytkowania tych kluczy i certyfikatów oraz zarządzać nimi przy użyciu dostosowywanego graficznego interfejsu użytkownika (GUI). Ponadto niewidoczna implementacja szyfrowania w programie IBM Tivoli Key Lifecycle Manager oznacza, że klucze są generowane i dostarczane z centralnej lokalizacji i nigdy nie są wysyłane lub przechowywane w formacie „zwykłego tekstu”.

Ta technologia może być wykorzystana w całym centrum danych w sposób przedstawiony na rysunku 4. Dyski samoszyfrujące mogą być instalowane w macierzach pamięci masowej, macierzach SAN i NAS, serwerach, centrach danych, biurach oddziałów i małych firmach. Ujednolicona usługa zarządzania kluczami może być odpowiedzią na wymagania dotyczące zarządzania kluczami dla wszystkich form pamięci masowej (oraz innych zabezpieczeń).

Technologia dysków SED w trybie automatycznego blokowania

Aby przełączyć dysk SED do trybu automatycznego blokowania, właściciel dysku może najpierw zmienić klucz szyfrowania dla zwiększenia poziomu bezpieczeństwa, korzystając z funkcji bezpiecznego wymazywania nowego dysku SED. Takie rozwiązanie zabezpiecza również dysk przed atakiem w magazynie. Właściciel musi następnie utworzyć klucz uwierzytelniania, wprowadzając najpierw identyfikator SID (Security ID, dowód własności) z zewnętrznej etykiety dysku. Klucz uwierzytelniania będzie używany przez dysk do ochrony klucza szyfrowania. Po wykonaniu powyższych czynności dysk SED jest przełączony do trybu automatycznego blokowania. W tym stanie dysk jest chroniony. Po wyłączeniu zasilania dysk zostanie zablokowany, a po ponownym włączeniu zasilania wymagane będzie uwierzytelnianie w celu usunięcia blokady. W trybie automatycznego blokowania dysku SED klucz szyfrowania i klucz uwierzytelniania współdziałają w celu zapewnienia dostępu do danych przechowywanych na dysku.

W trybie automatycznego blokowania dysku SED, skonfigurowanym do uwierzytelniania, nie istnieje tajne hasło, którego odkrycie umożliwiłoby nieautoryzowany dostęp do zaszyfrowanych danych. Wyjaśnia to prosty opis procesu odblokowywania dysku. Proces odblokowywania jest jednym z etapów uruchamiania dysku, który umożliwia dostęp do zaszyfrowanych danych. Dysk oczekuje poświadczeń (klucz uwierzytelniania) umożliwiających weryfikację tożsamości uprawnionego użytkownika uzyskującego dostęp do dysku.

Dyski samoszyfrujące do serwerów i macierzy dyskowych NAS i SAN

Poniżej opisano kroki występujące podczas procesu uwierzytelniania uprzednio zabezpieczonego dysku (zob. rysunek 5):

Rysunek 5

1. Uwierzytelnianie

- System pamięci masowej pobiera klucz uwierzytelniania z usługi zarządzania kluczami i wysyła go do odpowiedniego zablokowanego dysku.
- Dysk przetwarza klucz uwierzytelniania i porównuje wynik z danymi klucza uwierzytelniania zapisanymi w bezpiecznym obszarze dysku.
- Jeżeli obie wartości klucza nie są zgodne, proces uwierzytelniania zostaje zakończony i nie można odczytać danych z dysku. Dysk pozostaje zablokowany. Zaszyfrowany tekst nigdy nie jest wysyłany z dysku.

2. Odszyfrowywanie klucza szyfrowania

- Jeżeli oba klucze są identyczne, dysk zostaje odblokowany i za pomocą klucza uwierzytelniania pobranego z systemu pamięci masowej odszyfrowuje kopię klucza szyfrowania (zaszyfrowanego wcześniej za pomocą klucza uwierzytelniania) zapisanego w bezpiecznym obszarze dysku. Po pomyślnym ukończeniu procesu uwierzytelniania dysk pozostaje odblokowany do momentu wyłączenia. Ten proces uwierzytelniania występuje tylko wówczas, gdy zasilanie dysku zostanie włączone po raz pierwszy i nie jest powtarzany przy każdej operacji odczytu lub zapisu.

3. Klucz szyfrowania w formacie zwykłego tekstu szyfruje i odszyfrowuje dane

- Klucz szyfrowania w formacie zwykłego tekstu jest następnie wykorzystywany do zaszyfrowania danych, które mają być zapisane na dysku oraz odszyfrowania danych, które mają być z niego odczytane.
- Transfer danych odbywa się w sposób standardowy; szyfrowanie i odszyfrowywanie danych przebiega niezauważalnie w tle.

Po przełączeniu dysku do trybu automatycznego blokowania można go ponownie przełączyć do trybu szybkiego bezpiecznego wymazywania danych dopiero po wykonaniu operacji bezpiecznego wymazywania. Właściciel, który zamierza przekazać dysk do innego zastosowania lub wycofać dysk z użytku (tj. przełączyć dysk z trybu automatycznego blokowania do bezpiecznego wymazywania danych w celu przekazania innej osobie), po prostu wykonuje operację bezpiecznego wymazania i zastąpienia klucza szyfrowania.

Dyski samoszyfrujące do serwerów i macierzy dyskowych NAS i SAN

Załącznik B: Porównanie technologii ochrony danych na dyskach twardych

Nie istnieje pojedyncza uniwersalna metoda szyfrowania uwzględniająca wszystkie zagrożenia danych stacjonarnych. W przypadku każdej metody należy uwzględnić zagadnienia związane z kosztami, współdziałaniem, wydajnością i opóźnieniem, dlatego należy rozważnie wybrać lokalizację szyfrowania. Dostępne są między innymi następujące opcje szyfrowania:

- oprogramowanie hosta
- sprzętowe urządzenia szyfrujące
- szyfrujące układy ASIC znajdujące się w adapterze, przełączniku, kontrolerze RAID lub dysku twardym

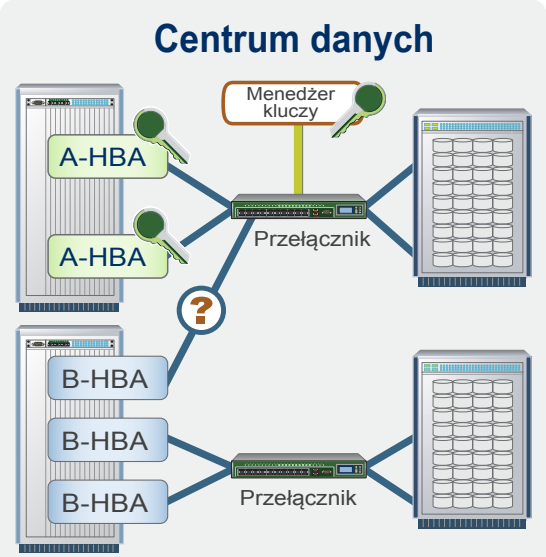
Rozważając metody ochrony i lokalizację szyfrowania danych stacjonarnych w macierzach SAN i NAS lub pamięci masowej podłączonej bezpośrednio do serwera, należy wybrać rozwiązanie umożliwiające szyfrowanie jak najbliżej pamięci masowej – najlepiej na dysku twardym.

Ułatwione zarządzanie kluczami i współdziałanie

Dyski SED znacznie ułatwiają zarządzanie kluczami, ponieważ klucz szyfrowania zawsze pozostaje na dysku, dlatego śledzenie klucza szyfrowania i zarządzanie nim nie jest konieczne. Ponadto administrator centrum danych nie musi przechowywać klucza szyfrowania w celu ewentualnego odzyskania danych, ponieważ zaszyfrowane kopie kluczy szyfrowania znajdują się w wielu miejscach na dysku.

Tylko dyski SED eliminują konieczność korzystania z depozytu klucza szyfrowania, ponieważ w przypadku utraty wszystkich kopii klucza na dysku można przypuszczać, że dysk uległ awarii, tzn. dane i tak nie zostałyby odczytane. Dodawanie dodatkowych kluczy szyfrowania odbywa się z zachowaniem zasady nadmiarowości danych — w momencie tworzenia dysku lustrzanego z funkcją samoszyfrowania na dysku tym również utworzony zostanie zestaw zaszyfrowanych kluczy szyfrowania. Natomiast w przypadku szyfrowania w infrastrukturze i kontrolerze mogą występować problemy ze śledzeniem, zarządzaniem i deponowaniem kluczy szyfrowania w celu umożliwienia odczytu/zapisu danych w punktach końcowych.

W przypadku szyfrowania sprzętowego występują poważne problemy w przełączniku lub adapterze. Rozdzielenie szyfrowania i lokalizacji danych powoduje podwyższenie stopnia złożoności rozwiązania i zwiększenie prawdopodobieństwa wystąpienia błędu. Na przykład prawidłowy klucz może być niedostępny wówczas, gdy jest wymagany do odszyfrowywania danych w środowisku wirtualnym. Większa ilość udostępnianego wyposażenia powoduje zwiększenie liczby modułów,



Rysunek 6

które muszą korzystać z określonego klucza, a śledzenie większej liczby kluczy przemieszczających się w infrastrukturze powoduje problemy z bezpieczeństwem, złożonością i wydajnością.

Adaptery ze zintegrowanymi kontrolerami szyfrowania ASIC powodują problemy ze współdziałaniem adapterów różnych dostawców, które nie obsługują zintegrowanych modułów szyfrujących. Dane zaszyfrowane przez sprzęt zamocowany na adapterze może odczytać tylko zgodny sprzęt korzystający z tego samego algorytmu szyfrowania oraz tej samej infrastruktury zarządzania kluczami. Na przykład na rysunku 6 niebieski moduł HBA (Host Bus Adapter) w dolnym serwerze nie może odczytać danych zaszyfrowanych w obiekcie docelowym lub uwierzytelnić się w menedżerze kluczy lub przełączniku szyfrowania, ponieważ nie może uzyskać dostępu do menedżera kluczy lub dysponuje niezgodnym sprzętem szyfrującym.

Dyski SED nie stwarzają problemów z zarządzaniem, ponieważ klucz szyfrowania zawsze pozostaje na dysku. Ponadto można łatwo dodać dyski z różnymi silnikami szyfrującymi do istniejącej macierzy. W centrach danych mogą być używane różne silniki szyfrujące w tej samej macierzy, gdyż algorytm szyfrowania jest niewidoczny dla systemu. Ponieważ modele dysków zmieniają się, a w dyskach twardych stosowane są coraz nowsze technologie szyfrowania, można dodać nowe dyski do starych w systemie pamięci masowej obsługującym funkcję szyfrowania bez konieczności zmian związanych z wyższym poziomem zabezpieczeń nowych dysków.

Dyski samoszyfrujące do serwerów i macierzy dyskowych NAS i SAN

Wprowadzane jest również współdziałanie w zarządzaniu kluczami. Firmy IBM, LSI i Seagate zapewniają zgodność z protokołem współdziałania w zarządzaniu kluczami (Key Management Interoperability Protocol), przekazanym organizacji OASIS w celu rozpowszechnienia w procesie wprowadzania otwartych standardów.

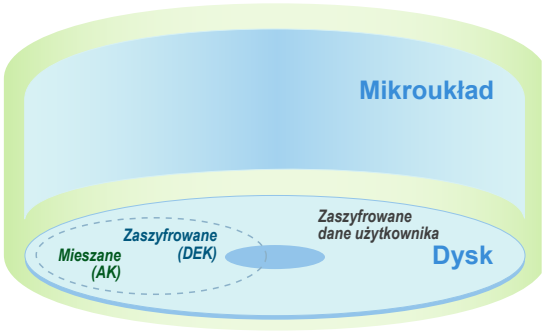
Zabezpieczenia na poziomie wymaganym w agencjach rządowych

Dyski SED zapewniają lepsze zabezpieczenia, ograniczając prawdopodobieństwo, że konieczne będzie zastąpienie rozwiązania w zakresie ochrony danych w przyszłości na skutek bardziej restrykcyjnych przepisów. Jak już zauważono, dyski SED nie osłabiają zabezpieczeń na skutek zbędnego szyfrowania w infrastrukturze i narażania zaszyfrowanego tekstu i kluczy przechowywanych przez dłuższy czas. Dyski SED oferują również wiele dodatkowych korzyści przyczyniających się do wzmocnienia zabezpieczeń w porównaniu z innymi technologiami pełnego szyfrowania dysków.

Amerykańska Agencja Bezpieczeństwa Narodowego (NSA) zatwierdziła pierwszy dysk samoszyfrujący (dysk twardy Momentus® 5400 FDE) do ochrony informacji w komputerach wdrażanych przez agencje rządu USA i kontrahentów dla celów związanych z bezpieczeństwem narodowym. Ponadto implementacja algorytmu szyfrowania w tym pierwszym modelu jest zgodna ze standardem NIST AES FIPS-197. Firma Seagate aktualnie ubiega się o podobną akceptację przyszłych dysków SED.

Na rysunku 7 przedstawiono sytuację, w której znajdowałyby się osoby, które bez autoryzacji weszły w posiadanie zabezpieczonego dysku SED zablokowanego po wyłączeniu zasilania. Klucz szyfrowania zawsze pozostaje w dysku, jest unikatowy dla dysku i jest generowany przez ten dysk. Ponadto klucz szyfrowania w formacie zwykłego tekstu nie jest dostępny — tylko zaszyfrowana wersja klucza jest przechowywana na dysku. Na dysku nie ma danych w formacie zwykłego tekstu, tylko przetworzony klucz uwierzytelniania. Ponadto dyski twarde nie wykorzystują pamięci nieodpornej na atak typu „zimny rozruch".

Zarówno dane, jak i klucz szyfrowania są zaszyfrowane za pomocą algorytmu AES 128, zaaprobowanego przez rząd amerykański do ochrony informacji poufnych. Projektując firma Seagate uwzględniła fakt, że osoba



Rysunek 7

atakująca może mieć informacje na temat jego konstrukcji i lokalizacji wymaganych danych. Brak wskazówek na dysku umożliwiających odszyfrowanie danych powoduje, że szczegółowe informacje na temat konstrukcji dysku są bezużyteczne dla hakerów. Podobnie złamanie zabezpieczeń jednego dysku nie ułatwi w żaden sposób złamania zabezpieczeń innych dysków.

Generalnie ujawnienie zaszyfrowanego tekstu może być użyteczne dla osoby atakującej. Jeżeli na przykład system plików na dysku ma powszechnie znaną strukturę, haker może wykorzystać wiedzę, że wartości w niektórych sektorach są stałe i znane, i spróbować złamać szyfr. Powszechnie znane są także struktury baz danych. Istotną unikatową zaletą dysków SED jest fakt, że zaszyfrowany tekst nie jest przesyłany. Utrudnia to skutecznie atak tego typu.

Dyski SED mogą blokować się nieodwracalnie po wstępnie określonej liczbie prób uwierzytelnienia zakończonych niepowodzeniem. Natomiast osoba atakująca dysponująca dyskiem, który nie wykorzystuje technologii SED i który został zaszyfrowany inną metodą, może w nieskończoność ponawiać próby uwierzytelnienia, ponieważ dysk nie jest zabezpieczony. Ponadto pobierane pliki oprogramowania układowego dysku SED są zabezpieczone; osoba atakująca nie może wprowadzić zmodyfikowanego oprogramowania układowego do dysku. Na zakończenie należy zauważyć, że aby dodatkowo zminimalizować luki zabezpieczeń umożliwiające atak, firma Seagate nie wprowadziła awaryjnych metod uzyskania dostępu do dysku SED (tzw. tylnych drzwi).

Dyski samoszyfrujące do serwerów i macierzy dyskowych NAS i SAN

Praca przy pełnej szybkości dysku; mniejsza potrzeba klasyfikacji danych

Dysk samoszyfrujący jest wyposażony w dedykowany silnik obsługujący szyfrowanie przy pełnej szybkości interfejsu. Silnik szyfrujący SED wykorzystuje moduły sprzętowe i znajduje się w kontrolerze ASIC. Każdy port dysku korzysta z dedykowanego silnika szyfrującego zgodnego z maksymalną szybkością portu. Szyfrowanie nie spowoduje więc spowolnienia pracy dysku.

Wydajność dysku SED można skalować liniowo i automatycznie. Dodanie kolejnych dysków powoduje proporcjonalne zwiększenie przepustowości systemu szyfrowania. Administratorzy centrów danych nie muszą zajmować się równomiernym rozkładaniem obciążenia związanego z szyfrowaniem podczas dodawania nowych dysków do macierzy lub większej liczby macierzy do centrum danych.

Administratorzy centrów danych mogą szyfrować wszystkie dane bez ograniczenia wydajności, dlatego klasyfikacja danych jest konieczna w dużo mniejszym stopniu. Jak już zauważono, próby identyfikacji wszystkich poufnych informacji są pracochłonne i czasochłonne. Utrudniona jest również obsługa i aktualizacja danych tego typu zwłaszcza wówczas, gdy mogą być w łatwy sposób kopiowane z chronionego źródła do niezabezpieczonej lokalizacji docelowej. Ograniczenie konieczności klasyfikacji danych znacznie upraszcza proces planowania i zarządzania szyfrowaniem w centrum danych.

Pełna efektywność kompresji i eliminacji duplikatów

Kompresja danych i eliminacja duplikatów w systemie pamięci masowej umożliwia znaczną redukcję kosztów przechowywania danych, jednak tylko wówczas, gdy dane nie są szyfrowane, ponieważ systemy pamięci masowej są optymalizowane dla danych w formacie zwykłego tekstu w przypadku kompresji i eliminacji duplikatów. Dyski SED zapewniają pełną efektywność kompresji i eliminacji duplikatów w systemie pamięci masowej.

Pełna zgodność ze standardem ochrony integralności danych (PI)

Technologia SED oferuje nowatorskie rozwiązanie w zakresie ochrony integralności danych PI (Protection Information), zwane również funkcją Data Integrity Feature, zgodne ze specyfikacją pełnej ochrony danych T-10 i protokołu SCSI. Implementacja tego standardu protokołu SCSI w systemach SAS i kanałów światłowodowych (Fibre Channel) umożliwia każdemu elementowi na ścieżce danych sprawdzanie danych i wykrywanie uszkodzeń. Ta operacja jest wykonywana przy użyciu specjalnego dodatku do danych, jednak nie jest dostępna, jeżeli dane przekazywane przez dany element zostały zaszyfrowane.

Dysk SED wykonuje szyfrowanie na końcu ścieżki danych (tzn. na dysku używanym do przechowywania danych), dlatego jest jedynym rozwiązaniem zgodnym ze specyfikacją Protection Information na całej ścieżce danych. Zapewniając tę doskonałą integralność danych, technologia SED nie wpływa jednak na niezawodność, dostępność lub użyteczność/gwarancję dysku twardego.

Redukcja kosztów dzięki standardowej technologii

Sześciu wiodących dostawców dysków twardych (Fujitsu, Hitachi, Samsung, Seagate, Toshiba i Western Digital) współpracowało w celu opracowania ostatecznej specyfikacji opublikowanej ostatnio przez organizację TCG (Trusted Computing Group). Ta specyfikacja, utworzona jako standard projektowania dysków samoszyfrujących i zarządzania nimi, umożliwia współdziałanie dysków SED oferowanych przez różnych dostawców. Współdziałanie tego typu zapewni prawidłową konkurencję na rynku oraz obniżenie cen zarówno dla integratorów systemów, jak i użytkowników końcowych.

Ostatecznie wszystkie dyski oferowane przez wszystkich dostawców będą samoszyfrujące (połowa dostawców oferuje już dyski SED). Można więc przewidywać, że zostanie wyeliminowane zagrożenie związane z naruszaniem bezpieczeństwa danych wówczas, gdy dyski nie pozostają pod kontrolą właścicieli.

Dyski samoszyfrujące do serwerów i macierzy dyskowych NAS i SAN

Samoszyfrujące pamięci masowe będą więc dostępne we wszystkich punktach końcowych, włącznie z następującymi urządzeniami:

- serwery, macierze SAN i NAS (wirtualne lub nie), macierze RAID, JBOD lub indywidualne dyski
- napędy taśmowe
- dyski typu SSD
- dyski do komputerów stacjonarnych
- dyski do notebooków
- dyski przenośne

Mniejsza potrzeba ponownego szyfrowania

Rozdzielenie kluczy uwierzytelniania i kluczy szyfrowania zapewnia właścicielom dysków szereg korzyści związanych z zarządzaniem. Ponieważ klucz szyfrowania jest zaszyfrowany i zawsze pozostaje na dysku, administrator centrum danych nie musi zmieniać go okresowo, tak jak zwykle zmienia się hasło ze względów bezpieczeństwa. Eliminuje to potrzebę odszyfrowywania i ponownego szyfrowania danych, co jest procesem uciążliwym i pracochłonnym.

Klucz uwierzytelniania można zmieniać tak często, jak jest to konieczne, na przykład w przypadku odejścia administratora z firmy, bez konieczności ponownego szyfrowania. W przypadku odejścia administratorów pamięci masowej lub pojawienia się nowych operatorów ich prawa dostępu do urządzeń pamięci masowej można uwzględnić bez wpływu na szyfrowane dane.

Natomiast w przypadku szyfrowania w kontrolerze lub infrastrukturze klucze szyfrowania danych są przenoszone między menedżerem kluczy (miejsce bezpiecznego przechowywania) a punktem szyfrowania i konieczny jest depozyt klucza. Klucze szyfrowania danych nie są wówczas lepiej zabezpieczone niż klucze uwierzytelniania, dlatego powinny być okresowo zmieniane. Oznacza to konieczność ponownego szyfrowania danych (znaczne ograniczenie wydajności).

Ochrona danych mobilnych przy użyciu metod fizycznych lub szyfrowania sesji

Większość danych mobilnych jest przekazywanych kablami w kierunku downstream za pośrednictwem sieci Ethernet (macierze NAS) lub na poziomie bloków (macierze SAN) i pozostaje fizycznie pod kontrolą administratora pamięci masowej w dziale IT, dlatego jest uważana za prawidłowo chronioną.

W przypadku danych przekazywanych kablami w kierunku downstream, które nie znajdują się pod kontrolą administratora pamięci masowej w dziale IT, najbardziej powszechną i przyjętą metodą szyfrowania przesyłanych danych jest użycie krótkotrwałego klucza szyfrowania sesji. Pojedyncza transmisja może być szyfrowana przy użyciu klucza sesji odrzucanego niezwłocznie po zakończeniu transmisji — kolejna transmisja będzie chroniona nowym, innym kluczem sesji. Te krótkotrwałe klucze minimalizują zagrożenie danych w przeciwieństwie do długotrwałych kluczy używanych do szyfrowania danych przechowywanych na dysku twardym.

Rozważmy trzy scenariusze szyfrowania sesji:

Scenariusz pierwszy

Występują potencjalne zagrożenia związane z łączami infrastruktury kanału światłowodowego (FC, Fibre Channel), wychodzącymi z centrum danych i rozszerzającymi zakres macierzy SAN do biur zdalnych, innych ośrodków lub zdalnych lokalizacji (odzyskiwanie awaryjne). W takich okolicznościach zabezpieczenia zapewniają łącza FC over Internet Protocol (IP), a dane są chronione przy użyciu zabezpieczeń protokołu IP.

Scenariusz drugi

Routery i przełączniki wykorzystują technologie takie jak IPSec do ochrony i łączenia macierzy SAN za pośrednictwem sieci WAN. W przypadku zagrożenia tego typu szyfrowanie host/adapter nie jest wymagane pod warunkiem, że przełączniki i routery obsługują szyfrowanie danych IPSec. Technologia kanału światłowodowego (FC, Fibre Channel) ma zasięg tylko około 10 km, jednak menedżerowie IT muszą udostępniać, chronić i przenosić dane na odległość znacznie większą (czasami poza granice geograficzne). Firma QLogic oferuje routery i przełączniki umożliwiające przekazywanie ruchu sieciowego SAN za pośrednictwem protokołu IP i łączenie macierzy SAN poprzez sieci WAN.

Dyski samoszyfrujące do serwerów i macierzy dyskowych NAS i SAN

Scenariusz trzeci

Jeżeli protokół IP rozszerza macierz SAN za pośrednictwem Internetu lub dedykowanych linii, zabezpieczenia IPSec są używane w odniesieniu do tych łączy zdalnych w celu ochrony ważnych danych mobilnych na znacznych odległościach i obsługi replikacji danych, udostępniania urządzeń danych SAN oraz zapewniania kopii zapasowych i ciągłości działalności firmy. Sesje SSL (Secure Sockets Layer) są używane do ochrony łączy WAN (klucze krótkotrwałe) i ukrywania kluczy przez dłuższy czas.

Niezależnie od tego, czy dostępne są fizyczne zabezpieczenia infrastruktury, konieczna jest ochrona danych na dyskach twardych, które nie pozostają pod kontrolą właściciela. Zamiast opisanych wyżej technik zabezpieczeń sesji dobrym długoterminowym rozwiązaniem może wydawać się szyfrowanie w infrastrukturze w celu ochrony danych na dysku twardym: dane są szyfrowane nie tylko na dysku twardym, ale również podczas przesyłania w infrastrukturze. Ta metoda ma jednak fundamentalną wadę: zamiast podwyższać poziom bezpieczeństwa w rzeczywistości jest przyczyną dodatkowych zagrożeń i wyższego stopnia złożoności na skutek narażenia długotrwałych kluczy szyfrowania. W takich okolicznościach zagrożone są znaczne ilości tekstu chronionego przy użyciu pojedynczego klucza szyfrowania.

Jeżeli konieczne jest szyfrowanie danych mobilnych, należy korzystać z protokołu IPSec lub FC over IP. Szyfrowanie danych na dysku powinno być wykonywane przez sam dysk z przyczyn omówionych w powyższych sekcjach.

Dodatkowe informacje

Dodatkowe informacje dotyczące zabezpieczeń pamięci masowej są dostępne w witrynie organizacji Trusted Computing Group: www.trustedcomputinggroup.org

oraz utworzonym przez organizację SNIA (Storage Networking Industry Association) forum SSIF (Storage Security Industry Forum): www.snia.org/forums/ssif/knowledge_center.

Opracowania, emisje internetowe i demonstracyjne filmy wideo na temat dysków samoszyfrujących są dostępne w witrynie: www.SEDSecuritySolutions.com.

AMERYKA PŁN. I PŁD. Seagate Technology LLC 920 Disc Drive, Scotts Valley, California 95066, USA, +1 831 438 6550
AZJA/PACYFIK Seagate Technology International Ltd. 7000 Ang Mo Kio Avenue 5, Singapur 569877, +65 6485 3888
EUROPA, BLISKI WSCHÓD I AFRYKA Seagate Technology SAS 130-136, rue de Silly, 92773 Boulogne-Billancourt Cedex, Francja, +33 1 41 86 10 00