Teknoloji Belgesi

Sunucular için Kendiliğinden Şifrelenen Diskler, NAS ve SAN Dizileri

Genel Bakış

Bu belge, sabit disklerde bulunan ve disk sahibinin kontrolünden kaçınılmaz olarak çıkan verileri emniyete almanın zorluklarını ele almaktadır. Belgede, Kendiliğinden Şifrelenen Diskler (SED) tanıtılmaktadır; bu diskler iki şekilde kullanılabilir: anlık güvenli silme sağlamak (kriptografik silme veya verileri okunmaz hale getirme) ve bir diskin kullanım sırasında sistemden çıkarılması veya çalınması halinde, aktif verileri emniyete almak için oto-kilitleme özelliğini etkinleştirmek için. Bunları iki ek takip etmektedir: İlk ek, SED'leri disk verilerinin emniyete alınmasında kullanılan diğer şifreleme teknolojileriyle karşılaştırmaktadır. İkincisiyse, anlık güvenli silme ve SED teknolojisinin oto-kilitleme özelliğine ilişkin ayrıntılı bir analiz yaparak, SED'lerin sunucularda, NAS ve SAN dizilerinde, sanallaştırılmış ortamlarda, RAID'lerde, JBOD'larda ve gizli disklerde nasıl kullanıldığını açıklamaktadır.

Giriş

Sabit diskler kullanımdan kaldırılıp, fiziksel olarak korunan veri merkezinden çıkarılarak başka kişilerin eline geçtiğinde, bu disklerde saklanan veriler ciddi bir risk altına girer. BT departmanları, diskleri rutin olarak kullanımdan kaldırırlar; bunun çeşitli sebepleri vardır:

- Disklerin garanti, onarım veya süresi dolan kira anlaşmaları sebebiyle geri götürülmesi;
- Disklerin çıkarılması ve atılması;
- Disklerin başka depolama görevleri için kullanılması.

Neredeyse tüm diskler, en sonunda veri merkezinden ve sahiplerinin kontrolünden çıkarlar; Seagate, veri merkezlerinden günde yaklaşık 50.000 diskin çıkarıldığını tahmin etmektedir. Kurumsal veriler, bu disklerde mevcut kalır ve çoğu disk, veri merkezini, içerdikleri veriler hala okunabilir durumdayken terk eder. Bir RAID dizinindeki birçok diskten geçmiş veriler bile, veri hırsızlığına karşı korumasızdır; çünkü günümüzün yüksek kapasiteli dizinlerindeki tipik bir disk birimi bile, yüzlerce ismi ve sosyal güvenlik numarasını barındıracak kadar geniştir.

Sunucular için Kendiliğinden Şifrelenen Diskler, NAS ve SAN Dizileri

Disk Kontrolündeki Zorluklar ve Atma Maliyetleri

Kurumsal şirketler, veri ihlallerini ve bunları izleyecek, veri gizliliği kanunlarınca öngörülen müşteri bildirimlerini önlemek amacıyla, kullanımdan çıkarılan disklerdeki verilerin, diskler şirket binasından ayrılmadan önce silinerek, yanlış kişilerin eline geçmesini engellemek için binlerce yol denemişlerdir. Verileri okunmaz hale getirmek için tasarlanan mevcut kullanımdan çıkarma uygulamaları, bu işlemde insanların önemli ölçüde yer almasını gerektirerek, hem teknik hem de insana özgü hataların oluşmasına zemin hazırlar.

Günümüzün diskleri kullanımdan çıkarma uygulamalarının dezavantajları, hem çok sayıdadır hem de oldukça kapsamlıdır:

- Disk verilerinin üzerine yazılması pahalıdır ve değerli sistem kaynaklarının günlerce bloke olmasına sebep olur. Disk tarafından herhangi bir tamamlanma bildirimi verilmez ve üzerine yazma işlemi, yeniden tahsis edilen sektörleri kapsamadığı için, ilgili verileri korumasız bırakır;
- Bir diski manyetikliğinden arındırmak veya fiziksel olarak parçalamak da maliyetli işlemlerdir. Manyetikliği giderme gücünün disk tipine göre optimize edildiğinden emin olmak zordur; dolayısıyla, disk üzerinde okunabilir durumda veriler kalabilir. Diski fiziksel olarak parçalamaksa, çevreye zarar verir; iki uygulama da, diskin garanti veya süresi dolan kira anlaşmaları sonucu geri döndürülmesini mümkün kılmaz;
- Bazı kurumsal şirketler, diskleri güvenli bir şekilde kullanımdan kaldırmanın tek yolunun, onları kontrol altında tutarak, süresiz olarak depolarda saklamak olduğu sonucuna varmışlardır. Fakat bu yöntem de tam olarak güvenli değildir; çünkü, insanların bulunduğu bir ortamda yüksek miktarda disk bulunması, kaçınılmaz olarak kimi disklerin kaybolmasına veya çalınmasına yol açar;
- Bazı şirketlerse, profesyonel elden çıkarma hizmetleri tutmayı seçerler, ancak bu hizmeti tutmanın maliyetini ve dahili raporlar ile denetim gibi gereklilikleri de beraberinde getiren, yüksek maliyetli bir seçenektir. Bir diskin söz konusu hizmete aktarılmasının diskteki verileri riske atması da, bu yöntemin bir başka sorunlu özelliğidir. Kaybedilen tek bir disk, şirkete veri ihlalinin tazminatı olarak milyonlarca dolara mal olabilir.

Bütün bu dezavantajlara bakıldığında, bir IBM çalışmasının IBM'e geri döndürülen disklerin yüzde 90'ının hala okunabilir durumda olduğunu ortaya çıkarması pek de şaşırtıcı değildir. Buradan çıkarmamız gereken ders nedir? Söz konusu olan sadece veri merkezinden çıkarılan disk değil, aynı zamanda diskte saklanan verilerdir.

Şifreleme

Her gün, eski sistemler kullanımdan kaldırıldıkça, veri merkezlerinden binlerce terabaytlık veri çıkmaktadır. Peki bütün bu sabit diskler otomatik ve saydam olarak bu verileri şifreleyip, anında ve güvenli bir şekilde silinmelerini sağlasaydı? Bugün, ABD eyaletlerinin çoğunda, şifrelenmiş verileri zorunlu veri ihlali bildirimlerinden muaf kılan veri gizliliği kanunları mevcuttur. Sakın yanlış anlamayın, verilerin açığa çıkmasının maliyeti, ortalama 6,6 milyon ABD doları olmak suretiyle, oldukça yüksektir[1].

Performans, ölçeklendirilebilirlik ve karmaşıklık gibi güçlükler, BT departmanlarının şifreleme kullanımını öngörülen güvenlik politikalarına karşı çıkmasına yol açmıştır. Bununla birlikte, şifreleme, bir şirketin kendi verileri üzerindeki şifreleri her zaman kaldırabilmesini sağlayan bir işlem olan anahtar yönetimine alışık olmayanlar tarafından riskli görülmektedir. Kendiliğinden Şifrelenen Diskler, bu sorunları büyük ölçüde gidererek, disklerin kullanımdan kaldırılması sırasındaki şifreleme işlemini hem kolay hem de uygun maliyetli bir hale getirmiştir.

İki güvenlik senaryosu üzerinde duracağız:

- Anahtar yönetimi gerektirmeden anlık güvenli silme sağlayan SED'ler;
- Anahtar yaşam çevrimi yönetimi sayesinde aktif verilerin hırsızlığa karşı korunmasını sağlayan otomatik olarak kilitlenen SED'ler.

[1] 2008 Yıllık Çalışma: Veri İhlali Maliyeti, Ponemon Institute, Şubat 2009

Sunucular için Kendiliğinden Şifrelenen Diskler, NAS ve SAN Dizileri

Anahtar Yönetimi Olmadan Anlık Güvenlik Silme

Kendiliğinden Şifrelenen Diskler, kriptografik silme yoluyla, verilerin hızla yok edilmesini sağlar. SED normal kullanımdayken, sahibinin diskteki verilere erişmek için doğrulama anahtarlarına (şifre veya parola olarak da bilinir) ihtiyacı olmaz. SED, diske yazılan verileri şifreler ve diskten okunan verilerin şifresini kaldırır; bütün bu işlemler, disk sahibinin bir doğrulama anahtarı girmesine gerek kalmadan yapılır.

Diskin kullanımdan kaldırılma veya bir başka amaçla kullanılma zamanı geldiğinde, disk sahibi diske kriptografik silme işlemi yapması için bir komut gönderir. Kriptografik silme, şifrelenmiş disk içindeki şifreleme anahtarının yerine yenisini koyar ve şifrelenmiş verilerin şifrelerinin silinmiş anahtarı kullanarak çözülmesini imkansız kılar. (Güvenli silme işleminin nasıl yürüdüğüne ilişkin daha ayrıntılı bir açıklamayı Ek A'da bulabilirsiniz.)

Kendiliğinden Şifrelenen Diskler, BT departmanını hem disk kontrolü sorunlarından hem de elden çıkarma masraflarından kurtararak, BT çalışma giderlerini azaltır. SED'lerin devlet seviyesindeki veri güvenliği, BT verimliliğinden ödün vermeksizin, veri gizliliği uyumu için bir Güvenli Bölge oluşturulmasını sağlar. Ayrıca, SED'ler aşağıdaki özellikleri sayesinde kullanımdan kaldırma işlemini kolaylaştırır ve geri dönüş veya başka amaçla kullanım için donanım değerini korur:

- Üzerine yazma veya diski yok etme ihtiyacını ortadan kaldırır;
- Garanti ve süresi dolan kira dönüşlerini güvenceye alır;
- Disklerin güvenle bir başka amaç için kullanılmasını sağlar.

Anahtar Yaşam Çevrimi Yönetimli Oto-Kilitlemeli Kendiliğinden Şifrelenen Diskler

Disk sahibi, kullanımdan kaldırma sırasında, anlık güvenli silme işlemi için Kendiliğinden Şifrelenen Disk kullanımının yanı sıra, aynı SED'yi aktif verilerin hırsızlığa karşı korunmasını sağlamak amacıyla oto-kilitleme modunda kullanmayı da tercih edebilir. İç hırsızlık veya yanlış yerleştirme, her ölçekten işletmeler için gittikçe ciddileşen bir sorundur; ayrıca, güçlü bir fiziksel güvenliği olmayan şube ve küçük işletme yöneticileri, dış hırsızlıklara karşı daha fazla savunmasızdırlar.

SED'nin oto-kilitleme modunda kullanılması, diskin normal kullanım sırasında bir doğrulama anahtarıyla güvenceye alınmasını gerektirir. Bu şekilde güvenceye alınan diskin veri şifreleme anahtarı, disk her kapatıldığında kilitlenir. Başka bir deyişle, SED kapatıldığında veya fişten çekildiğinde, diskteki verileri otomatik olarak kilitler.

SED yeniden açıldığında, şifreleme anahtarının kilidinin açılması ve diskteki herhangi bir verinin okunabilmesi için bir doğrulama isteyerek, yanlış yerleştirme ve iç veya dış hırsızlıklara karşı koruma sağlar.

Doğrulama anahtarlarının ömrü, IBM Tivoli Anahtar Yaşam Çevrimi Yöneticisi (eski Şifreleme Anahtarı Yöneticisi) ile yönetilebilir; bu program, doğrulama anahtarlarını merkezi olarak oluşturan, koruyan, saklayan ve yedekleyen Java tabanlı bir yazılım programıdır. Bu program, tüm depolama biçimlerinin (ve diğer güvenlik uygulamalarının) anahtar yönetimi koşullarını destekleyen birleştirilmiş bir anahtar yönetimi hizmetidir. IBM, LSI ve Seagate, OASIS'e açık standartlar işleminde ilerleme için beyan edilen Anahtar Yönetimi Ortak Çalışabilirlik Protokolü'nü destekleyecektir. IBM Tivoli Anahtar Yaşam Çevrimi Yöneticisi, platform tarafsızlığı sayesinde, işletmelerde sayısı gittikçe artan şifreleme anahtarlarının yönetimi için basit ve etkili bir yöntem sunmaktadır.

Kendiliğinden Şifrelenen Disklerin oto-kilitleme modu ve IBM Tivoli Anahtar Yaşam Çevrimi Yöneticisi, Ek A'da ayrıntılarıyla ele alınmaktadır.

Bir Kendiliğinden Şifrelenen Disk sahibi, SED'yi öncelikle sadece güvenli silme modunda kullanabilir, ardından SED'yi oto-kilitleme moduna geçirebilir. Bundan sonra, bir anlık güvenli silme işlemini ve diskin yeni bir amaca göre ayarlanmasını takiben, disk yeniden sadece güvenli silme modunda kullanıma geri döndürülebilir. Böylelikle, disk sahibi öncelikle, gerektiği zaman bir anlık güvenli silme işlemi yapmak için, SED'yi normal çalışma sırasında sadece güvenli silme modunda bırakabilir. Sonrasındaysa, hırsızlığa ilişkin artan endişeler sebebiyle, disk sahibi, mevcut şifreleme anahtarını gizleyen bir doğrulama anahtarı oluşturarak, SED'yi diskin bundan sonraki kullanımı için oto-kilitleme modunda kullanmayı seçebilir. Buna bağlı olarak, SED güvenli bir şekilde silinip yeni bir amaca göre ayarlandıktan sonra, diskin yeni sahibi diski oto-kilitleme moduna geçirmeyip, kullanım ömrünün sonunda güvenli bir şekilde silmek için, sadece güvenli silme modunda kullanabilir.

Sunucular için Kendiliğinden Şifrelenen Diskler, NAS ve SAN Dizileri

Kendiliğinden Şifrelenen Diskleri sadece anlık güvenli silme işlemi için kullanmak, bir diskin kullanımdan kaldırılması için son derece verimli ve etkili bir yol sağlar. Fakat SED'lerin oto-kilitleme modunda kullanılması, daha çok avantaj arz etmektedir. Kısacası, disk veya sistem veri merkezinden çıkarıldığı andan itibaren (doğrulama olsun ya da olmasın), disk kilitlenmiş olur. Bu verileri koruması için veri merkezi yöneticisinin önceden yapması gereken hiçbir eylem veya işlem yoktur. Bu özellik, diskin yanlış kullanımı halinde veri ihlali olasılığını önler ve verilerin iç veya dış hırsızlık tehdidine karşı korunmasını sağlar.

Sabit Disklerdeki Verileri Koruma Teknolojilerinin Karşılaştırılması

Tek bir şifreleme teknolojisi, tüm verileri bütün tehditlere karşı verimli ve etkili bir şekilde koruyamaz. Farklı tehditlere karşı koruma sağlamak için, farklı teknolojiler kullanılmaktadır. Örneğin, Kendiliğinden Şifrelenen Diskler, disk sahibinin kontrolünden çıktığında fakat verileri veri merkezi içindeki belirli tehditlere karşı koruyamadığında, verilerin tehditlere karşı korunmasını sağlar. Örneğin bir saldırgan, kilitlenmemiş bir diske erişim sağlayabilen bir sunucuya eriştiğinde,diskten gelen düz metni okuyabilir. Bu sebeple, SED şifreleme teknolojisinin veri merkezinin erişim kontrollerinin yerini almaktan çok, bu kontrolleri tamamlayıcı bir rol oynadığını unutmamak gerekir.

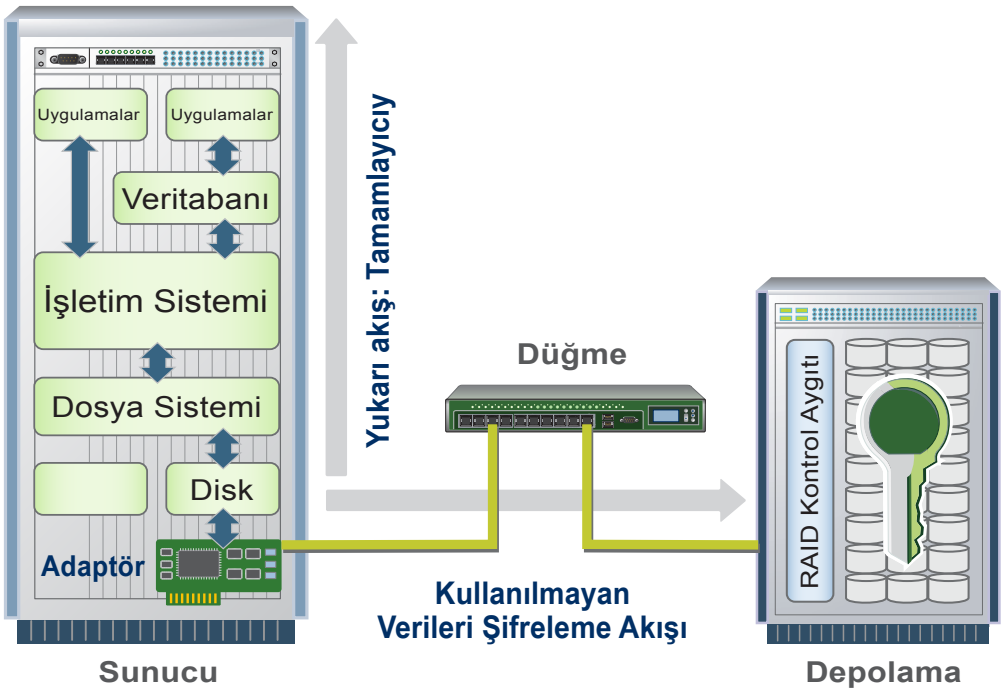
Kullanılmayan verilerin korunması da, diğer kontrollerin yerini almaktansa, hareketli verilerin korunmasını tamamlayan bir unsur görevi görmelidir. İster NAS üzerinde Ethernet yoluyla, ister bir SAN üzerinde blok seviyesinde olsun, dosya sisteminin kablo akışı boyunca hareket eden verilerin büyük çoğunluğu, fiziksel olarak BT depolama yöneticisinin kontrolündedir ve dolayısıyla bir güvenlik riski olarak görülmez. Fiziksel olarak yöneticinin kontrolünde olmayan hareketli verilerdeyse, yaygın olarak kabul gören ve yerleşmiş şifreleme uygulaması, IPSec veya IP üzerinden FC kullanmaktır; bu uygulama, küçük veri miktarlarını şifrelemek için, geçici oturum şifreleme anahtarlarından faydalanır. Bu oturum güvenliği tekniğini kullanmak yerine, sabit diskteki verileri tüm örgü üzerinde şifrelemek daha iyi bir çözümmüş gibi görünebilir: böylece veriler sadece sabit disk üzerinde şifrelenmekle kalmaz, örgü içinde hareket ederken de şifreli halini korur. Ancak bu yaklaşımda temel bir aksaklık söz konusudur: Bu yaklaşım, güvenliği arttırmaz, aksine azaltır ve uzun ömürlü anahtarlar olan şifreleme anahtarları dayatarak karmaşıklığı arttırırken, sadece tek bir şifreleme anahtarıyla şifrelenmiş yüksek miktarda rakam metni ortaya koyar. Hareketli veriler için şifreleme gerektiğinde, IPSec veya IP üzerinden FC ile sağlanmalıdır. Disk üzerindeki verilerin şifrelenmesi işlemi, aşağıdaki sebeplerden ötürü, en iyi şekilde diskin kendisi tarafından yapılır.

Uygulama, veritabanı, OS ve dosya sistemi şifreleme (bakınız Şekil 1), disk verilerine karşı (veritabanı, dosya veya sistem yöneticileri veya hacker'lardan kaynaklanan) veri merkezinde doğan tehditleri kapsayan tekniklerdir . Fakat önemli ölçüde performans kaybı ve bu şifreleme işleminin beraberinde getirdiği uygulama, veritabanı, OS veya dosya sistemine ilişkin ölçeklendirilemeyen değişiklikler yüzünden, verilerin sadece sınırlı bir kısmından fazlasının şifrelenmesi mümkün değildir. Yöneticiler, bu sınırlamalarla sadece en duyarlı verileri şifreleyerek başa çıkmaya çalışırlar.

Bu durum, yöneticileri, duyarlı verileri tanımlamak ve yerlerini belirlemek için veri sınıflandırmalarına güvenmeye zorlar; ne yazık ki, bu işlemin tüm duyarlı verileri tanımlamakta başarılı olamadığı yaygın olarak bilinmektedir. Veri sınıflandırması, özellikle de duyarlı bilgilerin korumalı bir kaynaktan korumasız bir varış noktasına kopyalanabilmesi halinde, zor, yoğun çalışma gerektiren ve korunması güç bir iştir. Bu tür sorunlar, diske çok fazla miktarda şifresi çözülmüş duyarlı verinin yazılmasıyla sonuçlanır ve bu veriler diskin kullanım ömrü sona erdikten uzun süre sonra bile sabit disk üzerinde kalır.

Bu nedenle, tüm diskin şifrelenmesini sağlama ve veri sınıflandırmasının duyarlı verileri yakalayamaması halinde oluşan boşluğu kapama görevi, dosya sisteminin şifreleme teknolojileri akışına düşer. Bu teknolojiler, veri koruyucularını, yönetim açısından sevimsiz ve ekstra maliyetli bir iş olan veri merkezinden ayrılan verilerin duyarlılığını sınıflandırma sorumluluğundan kurtarır. Örgü, RAID disk kontrol aygıtı (bir sunucuda veya depolama alt sistemi kontrol aygıtında) veya sabit disk üzerinde şifreleme, mevcut olasılıklardır. Peki bu şifreleme nerede yapılmalı?

Sunucular için Kendiliğinden Şifrelenen Diskler, NAS ve SAN Dizileri



Şekil 1

Birkaç yıl önce, Seagate henüz disk şifreleme üzerinde çalışmaya başlamamışken, Ulusal Güvenlik Ajansı (NSA), veri güvenliği sorununu analiz etti ve şifrelemenin yapılacak en uygun yerin sabit disk olduğunu belirledi. Bu, muhafızların mücevherlere mümkün olduğunca yakın durmalarını öngören, herkesçe bilinen bir güvenlik kuralıdır. Benzer şekilde, sabit disk içindeki şifreleme, verinin bulunduğu yer burası olduğu için, yapılacak optimum uygulamadır. SED'ler, tam disk şifreleme sağlayarak, sunucuların direkt bağlı depolarının, SAN'ların ve NAS depolarının sahipliğine ilişkin toplam maliyeti düşürmek için üstün bir teknoloji kullanırken, çok önemli bazı avantajlar sunarlar:

- **Basitleştirilmiş Anahtar Yönetimi:** SED, bir veri şifreleme anahtarını izleme veya yönetme ihtiyacını ortadan kaldırır; sadece güvenli silme için kullanıldığında, doğrulama anahtarının da izlenmesine veya yönetilmesine gerek yoktur;
- **Standartlaştırılmış Teknoloji Sayesinde Düşük Maliyetler:** Endüstriye göre standartlaştırılmış bir teknoloji kullanmak, maliyetlerden kısar ve SAN, NAS, sunucu, masaüstü, dizüstü bilgisayar ve taşınabilir depolama platformlarında ortak bir teknoloji sağlar;
- **Optimum Depolama Verimliliği:** Bazı şifreleme teknolojilerinin aksine, SED, veri sıkıştırmayı ve kopyalama önlemeyi mümkün kılarak, disk depolama kapasitesini en yüksek seviyeye çıkarır;
- **Yüksek Veri Bütünlüğü:** SED, Koruma Bilgileri sağlayarak, veri bütünlüğünün geleceğini garanti eder ve sabit diskin güvenilirliğini veya garantisini etkilemez;
- **Maksimum Performans ve Ölçeklendirilebilirlik:** SED, tam disk hızında çalışırken, lineer ve otomatik olarak ölçeklendirilebilir;
- **Veri Sınıflandırması Yok:** En yüksek performansın korunması için, yüksek maliyetli ve vakit kaybettirici veri sınıflandırma işlemine gerek yoktur;
- **Azaltılmış Yeniden Şifreleme:** SED, veri şifreleme anahtarının asla açığa çıkmaması sayesinde, yeniden anahtarlandırma ve yeniden şifreleme işlemlerine çok düşük bir oranda ihtiyaç duyulmasını sağlar;
- **Üstün Güvenlik:** NSA, ilk SED modelini uygun bulmuştur. SED, depolama örgüsünü gereksiz yere şifreleyerek güvenliği zayıflatmaz ve uzun ömürlü rakam metinlerinin ve anahtarların açığa çıkmasına sebep olmaz. SED, hatta şifreleme işini, hareketli verilerin korunması için tasarlanan teknolojilere bırakır.

Sunucular için Kendiliğinden Şifrelenen Diskler, NAS ve SAN Dizileri

Kendiliğinden Şifrelenen Disklerin standardizasyon işlemi de, daha düşük edinim maliyetleri vaat etmektedir. Dünyanın en büyük altı sabit disk satıcısı, Trusted Computing Group (TCG) tarafından yayınlanan son işletme şartnamesini oluşturmak için bir araya geldi. Kendiliğinden Şifrelenen Disklerin geliştirilmesi ve yönetimi için bir standart olarak oluşturulan bu şartname, farklı satıcılar tarafından piyasaya sunulan SED'lerin, birlikte çalışabilirlik özelliği taşımasını sağlamaktadır. Bu birlikte çalışabilirlik özelliği, daha büyük bir piyasa rekabetini ve çözüm üreticileriyle nihai kullanıcılar için daha düşük fiyatları mümkün kılar. Geçmişte, sabit disk sektörü, sektör genelindeki standartların hacmi arttırarak, maliyetleri azalttığını göstermiştir. Bu ölçek ekonomileri, ASIC'lerde artan mantığın disk malzemesi maliyetlerinin küçük bir kısmı olarak kalmasını sağlar. (Ek B'de sabit disk şifreleme teknolojileri ile SED'lerin avantajları arasında yapılan daha ayrıntılı bir karşılaştırma verilmektedir.)

Sonuç

Sunucu, SAN ve NAS dizinleri yöneticilerinin verilerini şifrelemek için gayet iyi sebepleri vardır. Kendiliğinden Şifrelenen Diskler, hem bu sebeplere hem de bazı BT profesyonellerinin bugüne kadar veri şifreleme yöntemlerini kullanmasına engel olan endişelere hitap eder.

Kendiliğinden Şifrelenen Disklerin yararları oldukça açıktır. Anlık güvenli silme, anahtar yönetimine gerek kalmaksızın, BT departmanlarının disklerin kullanımdan kaldırılması sırasında ortaya çıkan operasyonel masraflardan tasarruf etmesini sağlar. Ayrıca, kullanımdan çıkarılan diskin güvenli bir şekilde yeni bir amaca göre ayarlanmasını veya hizmet, garanti ya da süresi dolan kira anlaşmaları sebebiyle geri döndürülmesini sağlayarak, diskin değerini korur. Oto-kilitlemeli SED'ler, disklerin sistemden çıkarılması sırasında, verilerin disk hırsızlığına veya yanlış yerleştirmelere karşı otomatik olarak korunmasını sağlar. Böylelikle bir disk tehlikeye girse bile, verilerini asla açığa çıkarmaz.

Kendiliğinden Şifrelenen Diskler, bunun yanı sıra çok büyük avantajlar da sunar. Verilerin kurtarılması için şifreleme anahtarının izlenmesine veya yönetilmesine gerek yoktur; çünkü şifreleme anahtarı diskten asla çıkmaz, böylelikle disk sahibi kendi verilerindeki şifreyi kaldıramamak gibi bir endişeye kapılmaz. Yalnızca doğrulama anahtarının izlenmesi veya yönetilmesi gerekir; bu anahtarsa, güvenli bir şekilde yedeklenebilir, çoğaltılabilir ve çöküş onarım merkezlerinde kopyası çıkarılabilir. Bir SED sadece anlık güvenli silme işlemi için kullanılıyorsa, bu anahtarın tanıtılmasına veya yönetilmesine de gerek yoktur.

SED şifreleme işlemi, otomatik ve saydam olması sebebiyle, normal depolama yönetimi, işletim sistemi, uygulamalar ve veritabanları üzerinde yapılacak maliyetli değişikliklere ihtiyaç bırakmaz. Depolama sistemindeki verilerin verimli bir şekilde sıkıştırılması ve çoğaltılmasının önlenmesi konusunda sağlanan önemli maliyet tasarrufları, tamamen korunur. Bunun yanı sıra, performans, lineer ve otomatik olarak ölçeklenir; ayrıca, tüm veriler performans kaybı olmaksızın şifrelenebildiği için, maliyetli ve vakit kaybettirici veri sınıflandırma işlemine gerek kalmaz.

Kendiliğinden Şifrelenen Diskler, optimum yönetilebilirlik, birlikte çalışabilirlik ve maliyet verimliliği için, standartlara dayandırılmıştır; tüm sabit disk üreticileri, standartların oluşturulma sürecinde yer almıştır. Anahtar yönetimi de, büyük depolama sistemi satıcılarının OASIS'in Anahtar Yönetimi Birlikte Çalışabilirlik Protokolü'nü desteklemesi sayesinde, birlikte çalışabilirlik özelliği kazanmaktadır. SED'ler, tipik depolama sistemi güncelleme çizelgesine göre uygulanan standart ürünlere entegre edilebilecek şekilde tasarlanmıştır.

Basitçe ifade etmek gerekirse, diskteki şifreleme, diğer şifreleme teknolojilerine göre üstün bir maliyet verimliliği, performans, yönetilebilirlik ve güvenlik sağlar. Bu yüzden ileri gelen birçok analist, sistem üreticisi ve NSA gibi devlet kurumları, şifreleme işleminin diskte yapılması gerektiği sonucuna varmıştır. Özet: SED'ler, güvenliği arttıracak ve dünya sunucularındaki, SAN ve NAS dizinlerindeki toplam mülkiyet maliyetini düşürecek önemli bir atılımdır.

SED'lerin diskin kullanımdan çıkarılma masraflarını düşürmesi ve BT sorunlarını azaltması göz önünde bulundurulduğunda, birçok kurum SED'leri güvenlik politikalarına dahil etmenin faydaları üzerinde durmaya başlamıştır. Güvenlik politikalarını oluşturan kişiler, politikalarını gelecekteki tüm sabit disk alımlarının, mümkün olduğunca SED'lerden yana yapılmasını gerektirecek şekilde güncellemeyi düşünmelilerdir. IBM ve LSI, Kendiliğinden Şifrelenen Disklerin çözümlere dahil edilmesine öncülük etmekte, Seagate ise SED'leri genel sabit disk portföyüne hızla katmaktadır. Diğer sabit disk satıcıları da piyasaya yeni SED'ler sürmeye başlamıştır; böylelikle, kısa bir süre içinde, tüm sabit diskler Kendiliğinden Şifrelenen Diskler haline gelecektir.

Sunucular için Kendiliğinden Şifrelenen Diskler, NAS ve SAN Dizileri

Ek A: Kendiliğinden Şifrelenen Disk Teknolojisi

Yeni Edinilen Kendiliğinden Şifrelenen Diskler

Her Kendiliğinden Şifrelenen Disk (SED), fabrikadayken diske katıştırılmış olan rasgele bir şifreleme anahtarı üretir. SED otomatik olarak tam disk şifrelemesi yapar; bir yazma işlemi gerçekleştirildiğinde, diske temiz metin girer ve diske yazılmadan önce (diske gömülü bir şifreleme anahtarı kullanılarak) şifrelenir. Bir okuma işlemi gerçekleştirildiğinde, diskteki şifrelenmiş veriler diskten ayrılmadan önce bunların şifresi çözülür. Normal çalışma sırasında, bir SED sisteme karşı tamamen saydam olarak, şifreleme yapmayan bir disk gibi çalışır. Kendiliğinden Şifrelenen Disk, sürekli olarak şifreleme yapar—şifreleme özelliği, yanlışlıkla kapatılamaz.

Disk sahibi, diski aldığında, bu katıştırılmış şifreleme anahtarı, net metin formundadır ve disk oto-kilitleme moduna geçirilene kadar da açık kalır; bu moda geçildiğinde, bir doğrulama anahtarı verilir. Disk, diske yazdığı veya diskten okuduğu tüm verileri her zaman şifreleyecek veya şifrelerini çözecektir; ancak bir doğrulama anahtarı oluşturulmadıkça, hiç kimse diskteki net metin verilerini yazamaz veya okuyamaz.

Sistemin ayarlanması oldukça kolaydır. Disk sahibi, SED'yi oto-kilitleme modunda mı, yoksa sadece anlık güvenli silme için mi kullanacağına karar vermelidir. Her iki kullanım biçimi de aşağıda ele alınmaktadır.

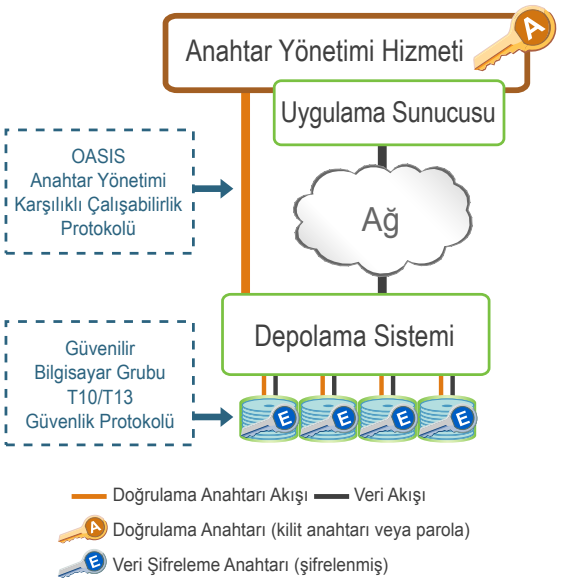
Anlık Güvenli Silme Teknolojisi

Bir disk sahibi, diskini sadece anlık güvenli silme için kullanmak istiyorsa, diskini kullanmaya normal çalışma halinde başlaması yeterlidir. Sadece güvenli silme modu, disk sahibinin verilerin şifresini kaldırmak ve verileri okumak için herhangi bir doğrulama anahtarına veya parolaya ihtiyacı olmadığı anlamına gelir. Bu durum, doğrulama anahtarının yanlış yönetimi ihtimalini ve buna bağlı veri kayıplarını önler.

SED teknolojisi, diskin yeni bir amaca göre ayarlanmasını veya atılmasını büyük ölçüde kolaylaştırır. Bir diski yeni bir amaca göre ayarlamak isteyen bir disk sahibinin, şifreleme anahtarını değiştirmek için bir anahtar silme işlemi yapması yeterlidir. Disk, şifreleme anahtarını siler ve disk içinde rasgele oluşturulan yeni bir şifreleme anahtarıyla değiştirir. Anahtar silme işleminden sonra, diske yazılmış olan tüm veriler okunmaz hale gelir—önceki anahtarla şifrelenen verilerin şifresi, yeni şifreleme anahtarıyla kaldırıldığında, bu veriler okunmaz bir hal alır (bakınız Şekil 2). Disk, fabrikadan çıktığı günkü konumuna gelerek, yeni bir kullanıcının diski sadece güvenli silme modunda kullanması veya oto-kilitleme moduna geçirmesi için hazır bir hal alır.

Şekil 2

Sunucular için Kendiliğinden Şifrelenen Diskler, NAS ve SAN Dizileri



Şekil 3

Anahtar Yönetimi ve Oto-Kilitlemeli Kendiliğinden Şifrelenen Disklerin Yönetimi

SED oto-kilitleme modunda kullanılırken, disk kilidinin okuma/yazma işlemlerine açılması için, dış bir kaynak tarafından oluşturulacak bir doğrulama anahtarı gerektirir. Oto-kilitlemeli Kendiliğinden Şifrelenen Diskler içeren bir veri merkezi, doğrulama anahtarlarını saklayan, yöneten ve veren bir anahtar yönetimi hizmetiyle, doğrulama anahtarlarını doğru diske aktaran bir depolama sisteminden faydalanır (bakınız Şekil 3). Seagate, IBM ve LSI kendi kurumlarındaki teknolojileri bir araya getirerek, IBM System Storage DS8000 ve IBM System Storage DS5000'de olduğu gibi, tam Kendiliğinden Şifrelenen çözümler sunmak için işbirliği içinde çalıştılar.

Depolama sistemi, geleneksel işlevlerinin yanında güvenli hacim gruplarını tanımlar, anahtar yönetimi hizmetinden doğrulama anahtarlarını alır ve anahtarı doğru diske aktarır. 3. şekildeki turuncu çizgi, bu işlemi gösterir. Bu şekilde, depolama sistemi, şifreleme fonksiyonunu ana bilgisayar, işletim sistemi, veritabanları ve uygulamalar için saydam hale getirir.

Disk açılırken doğrulama tamamlandıktan sonra, şifreleme depolama sistemine tamamen saydam olur ve sistem, klasik fonksiyonlarını normal olarak yerine getirebilir. Şekil 3'teki koyu gri çizgi, veri akışını, yani net metin verilerini göstermektedir. Depolama sistemleri, veri sıkıştırma ve kopyalama önleme işlemleri için şifrelenmemiş verileri optimize eder.

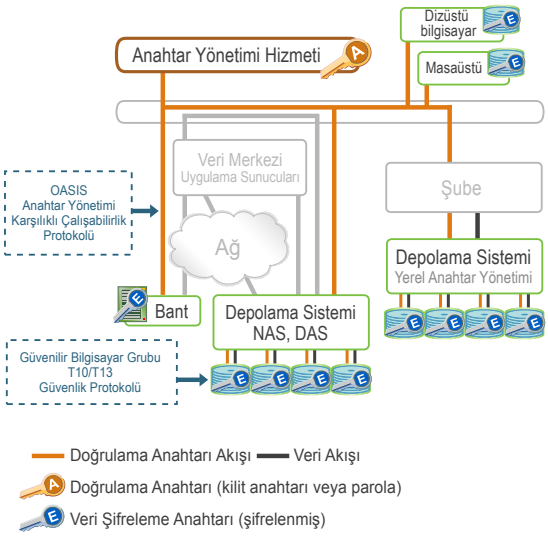
Bir anahtar yönetimi hizmeti, işletme genelinde ilgili doğrulama ve şifreleme anahtarlarının oluşturulması, atanması ve yönetilmesi için, yazılım veya donanım bazlı anahtar depolarından faydalanabilir. Etkili bir anahtar yönetimi, hem hizmetin hem de anahtarların yetkisiz erişimlere karşı yeterli bir şekilde korunmasını sağlamak için, kuruluşun mevcut güvenlik politikalarına uyum sağlamalıdır.

Ayrıca, etkili bir anahtar yönetim sistemi, yedekleme, senkronizasyon, ömür yönetimi, denetim ve uzun süreli tutma kapasitelerine sahip olmalıdır. Bir kuruluşun mevcut yüksek kullanılabilirlik ve çöküş onarım çözümlerinden faydalanmak mümkün olduğunda, bir anahtar yönetimi hizmetinin kurulması büyük ölçüde kolaylaşır.

IBM Tivoli Anahtar Yaşam Çevrimi Yöneticisi (eski Şifreleme Anahtarı Yöneticisi), IBM Kendiliğinden Şifrelenen bant sürücüler ve tam disk şifreleme diskli IBM System DS8000 ile kullanılan doğrulama anahtarlarını oluşturabilen, koruyabilen, saklayabilen ve tutabilen Java tabanlı bir yazılım programıdır. IBM Tivoli Anahtar Yaşam Çevrimi Yöneticisi, bir Java uygulaması olarak, z/OS, i5/OS, AIX, Linux, HP-UX, Sun Solaris ve Windows işletim sistemlerinde çalışır ve bir işletme içindeki çeşitli noktalara kurularak, uygulamanın yüksek oranda kullanılabilir olmasını sağlayan, ortak bir kaynak olarak tasarlanmıştır.

Platform tarafsızlığı ve mevcut güvenlik politikalarıyla bir kuruluşun en güvenli sunucu platformundaki yüksek kullanılabilirlikli ortamdan faydalanabilmesi sayesinde, IBM Tivoli Anahtar Yaşam Çevrimi Yöneticisi, işletme içinde sayıları gittikçe artan şifreleme anahtarlarının yönetimi için basit ve etkili bir yöntem sağlar.

Sunucular için Kendiliğinden Şifrelenen Diskler, NAS ve SAN Dizileri



Şekil 4

IBM Tivoli Anahtar Yaşam Çevrimi Yöneticisi, kullanım sırasında, anahtar malzemesinin güvenli bir konumda merkezi bir şekilde saklanmasını sağlayan anahtarlar verir; bu, anahtar sağlama için birçok protokolü destekleyen ve simetrik ve asimetrik anahtarların yanı sıra, sertifikaları da yöneten benzersiz bir yaklaşımdır. Kullanıcılar, ayrıca, özelleştirilebilir bir grafik kullanıcı arabirimi (GUI) kullanarak, bu anahtarları ve sertifikaları merkezi olarak oluşturabilir, içe aktarabilir, dağıtabilir, yedekleyebilir, arşivleyebilir ve yaşam çevrimlerini yönetebilir. Bunun yanında, IBM Tivoli Anahtar Yaşam Çevrimi Yöneticisinin saydam şifreleme uygulaması, anahtarların merkezileştirilmiş bir konumda oluşturularak, buradan verildiğini ve kesinlikle "açıkta" gönderilmediğini veya saklanmadığını ifade eder.

Sonuç olarak, bu teknoloji, Şekil 4'te de gösterildiği gibi, tüm veri merkezine uygulanabilir. Kendiliğinden Şifrelenen diskler, depolama dizilerinde, SAN, NAS ve sunucular üzerinde ve veri merkezleri, şubeler ve küçük şirketlerde bulunabilir. Birleştirilmiş bir anahtar yönetimi hizmeti, tüm depolama biçimlerinin (ve diğer güvenlik uygulamalarının) anahtar yönetimi koşullarını destekler.

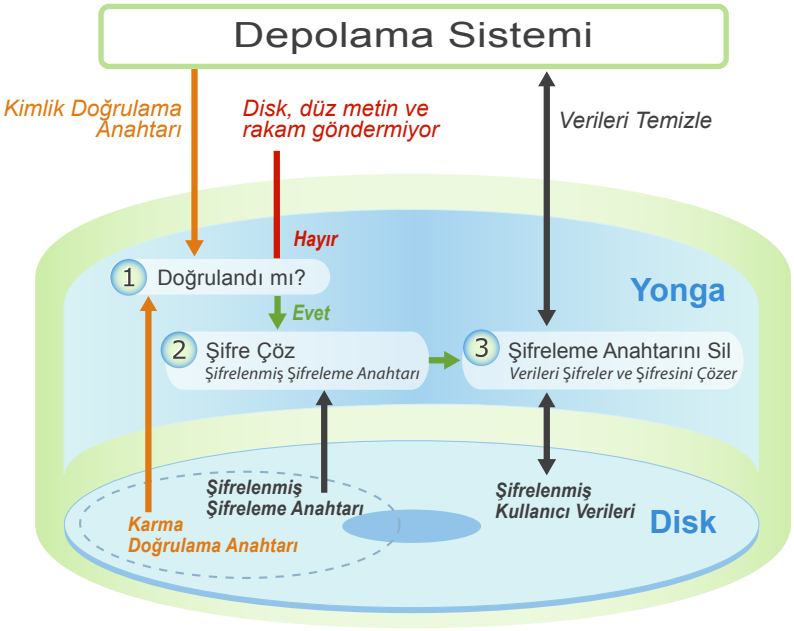
Oto-Kilitlemeli Kendiliğinden Şifrelenen Disk Teknolojisi

Kendiliğinden Şifrelenen Diski oto-kilitlenme moduna geçirmek için, disk sahibi, ilk olarak, yeni bir SED üzerinde güvenli silme işlemini kullanmak suretiyle, ekstra güvenlik için şifreleme anahtarını değiştirmek isteyebilir. Bu işlem, diski aynı zamanda bir depo saldırısına karşı da korur. Disk sahibi, ardından diskin dış etiketinde yer alan SID'sini (Güvenlik Kimliği, sahiplik göstergesi) girip bir doğrulama anahtarı oluşturmalı, sonrasında da disk tarafından şifreleme anahtarını şifrelemek için kullanılan doğrulama anahtarını ayarlamalıdır. SED artık oto-kilitlenme modundadır. Disk, güvenli bir duruma geçmiştir; disk durdurulduğunda kilitlenir ve çalıştırıldığında kilidinin açılması için doğrulama gerektirir. Oto-kilitlenmeli bir SED'de, şifreleme anahtarı ve doğrulama anahtarı, diskte saklanan verilere erişim sağlamak için bir arada çalışırlar.

Doğrulama anahtarı kullanmak üzere yapılandırılmış, oto-kilitlenmeli bir SED, bulunduğunda şifreli verileri açığa çıkarabilecek gizli bilgiler içermez. Kilidi açma işleminin basit bir açıklaması, bunun neden doğru olduğunu gösterir. Kilidi açma işlemi, diskin çalıştırma faaliyetinin, şifrelenmiş verilere erişim olanağı sağlayan kısmıdır. Disk, kendisine bir kimlik bilgisinin (doğrulama anahtarının) ulaştırılmasını bekler ve geldiğinde bunu, diske yetkili kullanıcı tarafından erişildiğini kanıtlamak için doğrular.

Sunucular için Kendiliğinden Şifrelenen Diskler, NAS ve SAN Dizileri

Aşağıdakiler, önceden korumaya alınmış bir diskin doğrulama işlemi sırasında görülen adımları açıklamaktadır (bakınız Şekil 5):



Şekil 5

1. Doğrulama

- Depolama sistemi, doğrulama anahtarını anahtar yönetim hizmetinden alır ve doğru kilitli diske gönderir;
- Disk, doğrulama anahtarını karma hale getirir ve sonucu diskin güvenli alanında depolanmış olan karma doğrulama anahtarıyla karşılaştırır;
- İki karma doğrulama anahtarı eşleşmiyorsa, doğrulama işlemi sona erer ve disk, diskten veri okunmasına izin vermez. Disk kilitli kalır. Diskin hiçbir zaman diskten rakam metni göndermediğini unutmayınız.

2. Şifrelenmiş şifreleme anahtarının şifresini çözün

- İki karma değer eşleştiğinde, diskin kilidi açılır ve disk, depolama sisteminden aldığı doğrulama anahtarını, diskin güvenli bir alanında saklanan (doğrulama anahtarıyla daha önce şifrelenmiş olan) şifreleme anahtarının bir kopyasının şifresini çözmek için kullanır. Doğrulama işlemi başarıyla tamamlandıktan sonra, kapatılacağı bir sonraki sefere kadar diskin kilidi açılır. Bu doğrulama işleminin, sadece disk ilk açıldığında yapıldığı unutulmamalıdır; işlem, her okuma ve yazma işlemi sırasında tekrarlanmaz.

3. Net şifreleme anahtarı, verileri şifreler ve şifrelerini çözer

- Net metinli şifreleme anahtarı daha sonra, diske yazılacak olan verileri şifrelemek ve diskten okunan verilerin şifresini çözmek için kullanılır;
- Disk artık veri transferleri sırasında standart bir şekilde çalışmaktadır; şifreleme ve şifre çözme saydam bir şekilde arka planda gerçekleşir.

Disk oto-kilitleme moduna geçirildiğinde, bir güvenli silme işleminin yapılmasının ardından, tekrar sadece güvenli silme moduna döndürülebilir. Disk sahibinin, diskini yeni bir amaca göre ayarlamak veya kullanımdan kaldırmak istemesi halinde (sözgelimi, diski başka kimsenin kullanamaması için oto-kilitlenme modundan sadece güvenli silme moduna geçirmek gibi), şifreleme anahtarını değiştirmek için bir güvenli silme işlemi yapması yeterlidir.

Sunucular için Kendiliğinden Şifrelenen Diskler, NAS ve SAN Dizileri

Ek B: Sabit Disklerdeki Verileri Koruma Teknolojilerinin Karşılaştırılması

Kullanılmayan verilere yönelik tüm tehditleri içeren kapsamlı bir şifreleme yaklaşımı yoktur. Her bir yaklaşımda, göz önünde bulundurulması gereken maliyet, birlikte çalışabilirlik, performans ve gecikme süresi konuları söz konusudur; bu yüzden verilerin nerede şifreleneceği seçilirken dikkatli olunmalıdır. Veri şifreleme seçenekleri, birçok biçimde bulunmaktadır:

- Ana bilgisayar bazlı yazılım;
- Şifreleme donanım aygıtları;
- Adaptör, düğme, RAID kontrol aygıtı veya sabit diskte bulunan şifreleme ASIC'leri.

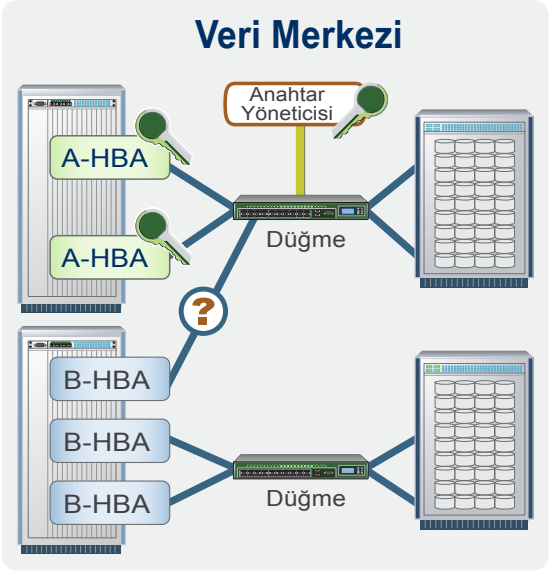
SAN, NAS veya sunucunun doğrudan bağlı deposundaki kullanılmayan verilerin nasıl korunacağı ve nerede şifreleneceği değerlendirilirken, en iyi çözüm, depoya mümkün olduğunca yakın bir konumda—ideal olarak sabit diskte şifrelemeyi seçmek olacaktır.

Kolaylaştırılmış Anahtar Yönetimi ve Birlikte Çalışabilirlik

SED'ler, şifreleme anahtarı diskten hiç çıkmadığı için, anahtar yönetimini büyük ölçüde kolaylaştırırlar; böylelikle, şifreleme anahtarının izlenmesine veya yönetilmesine gerek kalmaz. Veri merkezi yöneticisinin, verilerin kurtarılabilirliğini korumak için şifreleme anahtarını emanet etmesi gerekmez; çünkü disk, şifreleme anahtarının şifrelenmiş kopyalarını disk üzerinde birden fazla konumda saklar.

Sadece SED'ler şifreleme anahtarının emanet edilme gerekliliğini ortadan kaldırır; çünkü, diskin şifreleme anahtarının tüm kopyalarını kaybetmesi halinde, diskin bozulma olasılığı yüksektir, bu da verilerin hiçbir durumda okunamamasına yol açar. Veri artıklığıyla otomatik olarak daha çok şifreleme anahtarı eklenir—veriler bir başka Kendiliğinden Şifrelenen Diske her yansıtıldığında, bu diskin kendine ait bir şifrelenmiş şifreleme anahtarları takımı olacaktır. Buna karşın, örgü ve kontrol aygıtı şifreleme, verilerin okunması ve yazılması için uç noktalarını etkinleştirmek amacıyla, şifreleme anahtarlarının izlenmesi, yönetimi ve emanet edilmesi konularında güçlükler arz edebilir.

Donanım şifreleme işleminde, düğme veya adaptörde oluşan büyük zorluklarla karşılaşılabilir. Şifrelemeyi verinin saklandığı yerden ayırmak, çözüm karmaşıklığını arttırırken, hata olasılığını da yükseltir. Örneğin, bir sanallaştırma ortamında veri şifresinin çözülmesi



Şekil 6

için gerektiğinde, doğru anahtar hemen bulunamayabilir. Ortak ekipman sayısının çokluğu, belirli bir anahtarı paylaşması gereken kişilerin sayısını arttırır ve örgü içinde hareket eden daha fazla anahtarın izlenmesi, açığa çıkma, karmaşıklık ve performans sorunlarını beraberinde getirir.

Yerleşik şifreleme ASIC'leri bulunduran adaptörler, yerleşik şifrelemeyi desteklemeyen çok satıcılı adaptörlerle, birlikte çalışabilirlik sorunları doğurur. Adaptöre monte edilen donanım ile şifrelenen veriler, sadece aynı şifreleme algoritmasını kullanan ve aynı anahtar yönetimi altyapısına erişebilen uyumlu donanımlar tarafından okunabilir. Örneğin, Şekil 6'da, en alt sunucudaki bir mavi HBA (Ana Bilgisayar Veri Yolu Adaptörü) hedefte şifrelenmiş olan verileri okuyamamakta veya anahtar yöneticisi veya şifreleme düğmesiyle doğrulayamamaktadır, çünkü ya anahtar yöneticisine erişememektedir, ya da uyumsuz bir şifreleme donanımı bulundurmaktadır.

Kendiliğinden Şifrelenen Diskler, şifreleme anahtarı asla diskten çıkmadığı için, kendiliğinden yönetilebilirlik sağlarlar. Bunun yanı sıra, mevcut bir diziye farklı katıştırılmış şifreleme algoritmalarına sahip motorlar eklemek kolaydır. Böylelikle, veri merkezinde çok çeşitli şifreleme motorları bulunabilir, çünkü şifreleme algoritması sistem için saydamdır. Disk modelleri değiştikçe ve sabit disklerde daha yeni şifreleme teknolojileri kullanılmaya başlandıkça, bunlar, yeni diskin daha yüksek koruma düzeyine

Sunucular için Kendiliğinden Şifrelenen Diskler, NAS ve SAN Dizileri

özel hiçbir değişiklik yapmadan şifrelemeyi destekleyen depolama sistemlerindeki daha eski disklerle karıştırılabilir.

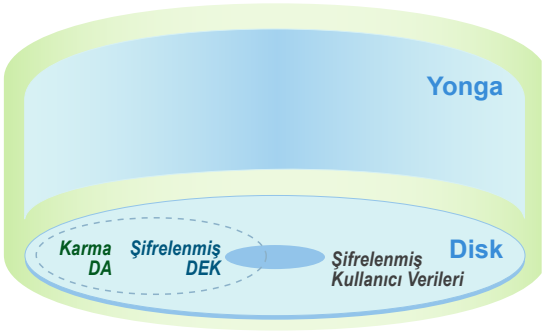
Anahtar yönetimi de birlikte çalışabilir hale gelmektedir. IBM, LSI ve Seagate, OASIS'e açık standartlar işleminde ilerleme için beyan edilen Anahtar Yönetimi Ortak Çalışabilirlik Protokolü'nü destekleyecektir.

Devlet Seviyesinde Güvenlik

Kendiliğinden Şifrelenen Diskler, üstün güvenlik sağlayarak, veri güvenliği çözümünün daha sıkı düzenlemelere bağlı olarak gelecekte çıkarılarak değişmesi gerekliliğini azaltır. Daha önce de sözü edildiği gibi, SED, depolama yapısını gereksiz yere şifreleyerek güvenliği zayıflatmaz ve uzun ömürlü rakam metinlerinin ve anahtarların açığa çıkmasına sebep olmaz. SED'ler aynı zamanda güvenlik özelliklerini diğer tam disk şifreleme teknolojilerinden daha güçlü kılan birçok avantaj sunmaktadır.

Amerika Birleşik Devletleri Ulusal Güvenlik Dairesi (NSA), ABD devlet kurumları ve ulusal güvenlik amaçlarıyla çalışan yükleniciler tarafından kullanılan bilgisayarlardaki bilgilerin korunması için, ilk Kendiliğinden Şifrelenen Disk olan Momentus® 5400 FDE sabit diski onaylamıştır. Ayrıca, bu ilk modeldeki şifreleme algoritması uygulaması, NIST AES FIPS-197 uyumludur. Seagate, gelecekte üreteceği SED'ler için benzer bir kabul sağlama sürecindedir.

Şekil 7'de, potansiyel saldırganların, kapandığı zaman kilitlenen güvenli bir SED'yi ele geçirdikleri takdirde neyle karşılaşacağı gösterilmektedir. Şifreleme anahtarı, diskten asla çıkmaz; anahtar sadece o diske özgüdür ve o disk tarafından üretilmiştir. Dahası, net bir şifreleme anahtarı hiçbir yerde bulunamaz—diskte şifreleme anahtarının sadece şifrelenmiş bir versiyonu saklanır. Diskin hiçbir yerinde, net metin gizlemeleri yoktur; sadece doğrulama anahtarının bir parmak izi (karması) vardır. Buna ek olarak, sabit diskler, bir "soğuk-açma" saldırısına karşı savunmasız olan bellek tipleri kullanmazlar.



Şekil 7

Hem veriler, hem de şifreleme anahtarı, ABD devletinin sır düzeyindeki gizli bilgileri korumak için kullanılması onaylanmış olan aynı şifreleme algoritması, yani AES 128 algoritması kullanılarak şifrelenmiştir. Seagate, diski tasarlarken bir saldırganın diskin tasarımının ve diskte bulunabilecek tüm sırların konumlarının tamamını bilebileceği varsayımına dayanır. Diskte, verilerin şifresinin çözülmesine neden olabilecek hiçbir ipucu bulunmadığından, disk tasarım ve yapısının ince ayrıntılarını bilmeleri, hacker'lar için hiçbir avantaj teşkil etmez. Aynı şekilde bir diski kırmak, saldırganın diğer diskleri daha kolay kırmasını sağlayacak hiçbir bilgiyi açığa çıkarmaz.

Genellikle rakam metninin açığa çıkması, bir saldırıya yardımcı olabilir. Örneğin diskteki dosya sistemi çok iyi bilinen bir yapı olduğunda, bir hacker, şifrelemeye yapacağı saldırıya, bazı sektörlerin her zaman bilinen değerleri içerdiği gerçeğinden yararlanarak başlayabilir. Benzer şekilde, veritabanı yapıları da iyi bilinmektedir. Kendiliğinden Şifrelenen Disklere özgü önemli bir avantaj da, SED'nin rakam metni göndermeyerek, bu tür saldırıları etkili bir şekilde püskürtmesidir.

SED'ler, önceden belirlenen sayıda doğrulama girişiminin başarısız olmasının ardından, kendilerini kesin olarak tuğlaya dönüştürme kabiliyetine sahiptir. Aksine, diğer bir yöntemle şifrelenmiş, SED olmayan bir diski ele geçiren bir saldırgan, sayısız doğrulama girişimi yapabilir ve disk herhangi bir şekilde korunmaz. Bunun yanında, SED, indirebileceği ürün yazılımlarını korumuş durumdadır; bir saldırgan, diske değiştirilmiş ürün yazılımı ekleyemez. Seagate, saldırılara karşı savunmasızlığı daha da azaltmak için, son olarak, SED'lerin içine hiçbir güvenlik gizli kapısı yerleştirmez.

Sunucular için Kendiliğinden Şifrelenen Diskler, NAS ve SAN Dizileri

Tam Disk Hızında Performans; Daha Az Veri Sınıflandırma Gereksinimi

Kendiliğinden Şifrelenen Diskler, tam arabirim hızıyla şifreleme için özel bir motora sahiptir. Donanım bazlı şifreleme kullanan SED şifreleme motoru, kontrol aygıtı ASIC'de bulunur. Her bir disk bağlantı noktası, bağlantı noktasının maksimum hızını karşılayan özel bir şifreleme motoru kullanır. Kısacası, şifreleme, sistemi yavaşlatmaz.

SED performansı da lineer ve otomatik olarak ölçeklenir. Daha fazla disk eklendikçe, şifreleme bant genişliği de orantılı bir şekilde artar. Veri merkezi yöneticisinin bir diziye daha fazla disk veya veri merkezine daha fazla dize eklerken, şifreleme iş yüklerini dengelemeyi düşünmesi gerekmez.

Veri merkezi yöneticileri istedikleri bütün verileri performans kaybı olmaksızın şifreleyebildiği için, veri sınıflandırmasına çok daha az gerek duyulur. Daha önce de belirtildiği gibi, tüm duyarlı bilgi örneklerini tanımlamak, yoğun çalışma gerektiren, zaman alıcı bir iştir. Bu verilerin korunması ve güncellenmesiyse, korumalı bir kaynaktan korumasız bir varış noktasına kolaylıkla kopyalanabilecekleri durumlarda, özellikle zordur. Veri sınıflandırması gerekliliğinin azaltılması, veri merkezindeki planlama sürecini ve şifre yönetimi işini büyük ölçüde kolaylaştırır.

Sıkıştırma ve Çoğaltmayı Önleme Verimlilikleri Tamamen Korunur

Depolama sistemi veri sıkıştırma ve çoğaltmayı önleme özellikleri, depolama masraflarını önemli ölçüde azaltma fırsatı sunar; ancak bu fırsat sadece veri şifrelenmemiş olduğu zamanlarda doğar; çünkü depolama sitemleri, veri sıkıştırma ve çoğaltma önleme işlemlerini yaparken, şifrelenmemiş veriler için optimize edilmiştir. SED'lerde, depolama sisteminin verileri verimli bir şekilde sıkıştırma ve çoğaltılmasını önleme özelliği tamamen korunmuştur.

Verileri Bütünlüğünün Koruma Bilgileri Standardı Tamamen Korunur

SED, veri bütünlüğünün geleceğini, yani T-10 SCSI bazlı uçtan uca veri koruma özelliği olan PI'yı (Koruma Bilgisi; Veri Bütünlüğü Özelliği olarak da bilinir) mümkün kılar. Bu SCSI protokolü standardının SAS ve Fiber Kanal sistemlerine uygulanması, veri yolundaki her bir unsurun verileri inceleyerek, herhangi bir bozulmanın olmadığını doğrulamasını sağlar. Bu işlem, verilere yapılan özel bir ekin kullanılmasıyla yapılır; fakat söz konusu unsurdan geçen veriler şifrelenmişse yapılamaz.

SED, şifreleme işlemini veri yolunun sonunda yaptığı için (örn., verinin saklandığı diskte), veri yolu boyunca Koruma Bilgisini destekleyen tek çözümdür. Bu üstün veri bütünlüğü sağlanırken, SED sabit diskin güvenilirliğini, kullanılabilirliğini veya hizmet verebilirliğini/garantisini kesinlikle etkilemez.

Standartlaştırılmış Teknoloji Maliyetleri Azaltır

Dünyanın en büyük altı sabit disk satıcısı (Fujitsu, Hitachi, Samsung, Seagate, Toshiba ve Western Digital), Trusted Computing Group (TCG) tarafından yayınlanan son işletme şartnamesini oluşturmak için bir araya geldi. Kendiliğinden Şifrelenen Disklerin geliştirilmesi ve yönetimi için bir standart olarak oluşturulan bu şartname, farklı satıcılar tarafından piyasaya sunulan SED'lerin, birlikte çalışabilirlik özelliği taşımasını sağlamaktadır. Bu birlikte çalışabilirlik özelliği, daha büyük bir piyasa rekabetini ve çözüm üreticileriyle nihai kullanıcılar için daha düşük fiyatları mümkün kılar.

En sonunda, tüm satıcılardan gönderilen diskler, Kendiliğinden Şifrelenen Diskler olacak (bu satıcıların yarısı, daha şimdiden SED gönderimine başladı bile). Bu durum, sabit disklerin sahiplerinin kontrolünden çıkması halinde, veri ihlali riskine bir son vermeyi vaat etmektedir.

Sunucular için Kendiliğinden Şifrelenen Diskler, NAS ve SAN Dizileri

Sonuç olarak, tüm uç noktalarda kendiliğinden şifrelenen bir depolama olması beklenmektedir; bunlara şu aygıtlar da dahildir:

- Sunucular, SAN'ler, NAS dizileri (sanallaştırılmış veya sanallaştırılmamış), RAID'ler, JBOD'ler veya bağımsız diskler;
- Teyp diskler;
- Sağlam durumdaki diskler;
- Masaüstü bilgisayar diskleri;
- Dizüstü bilgisayar diskleri;
- Taşınabilir diskler.

Daha Az Yeniden Şifreleme Gerekliliği

Doğrulama ile şifreleme anahtarlarının ayrılması, disk sahipleri için birden fazla yönetim avantajı sunar. Şifreleme anahtarının kendisi şifrelenmiş olduğundan ve diskten ayrılmadığından, veri merkezi yöneticisinin şifreleme anahtarını, normalde bir kullanıcının parolasını güvenlik nedenleriyle belli aralıklarda değiştirdiği gibi, periyodik olarak değiştirmesi gerekmez. Bu da verilerin şifresinin çözülmesi ve yeniden şifrelenmesi gerekliliğini ortadan kaldırarak, kaynakların yoğun bir şekilde kullanılmasına sebep olan bu işleme son verir.

Doğrulama anahtarı, sözgelimi bir yönetici şirketten ayrılırken, yeniden şifrelemeye gerek olmaksızın, istenen sıklıkla değiştirilebilir. Bir depolama yöneticisi işten ayrıldığında veya yeni bir operatör geldiğinde, depolama aygıtına erişim yetkileri, şifrelenmiş veriler etkilenmeden gerçekleştirilebilir.

Buna karşın, kontrol aygıtı ve örgü bazlı şifreleme, veri şifreleme anahtarlarını, güvenli depolama için anahtar yöneticisiyle şifreleme noktası arasında sürekli olarak hareket ettirir ve anahtar emaneti gerektirir. Bunların şifreleme anahtarları, artık doğrulama anahtarlarından daha güvenli değildir; bu nedenle, periyodik olarak yeniden anahtarlanmaları gerekir. Bu da, büyük bir performans ziyanı olan verilerin yeniden şifrelenmesi işlemini zorunlu kılar.

Hareketli Veriler Fiziksel Olarak veya Oturum Şifreleme ile Korunur

İster NAS üzerinde Ethernet yoluyla, ister bir SAN üzerinde blok seviyesinde olsun, dosya sisteminin kablo akışı boyunca hareket eden verilerin büyük çoğunluğu, fiziksel olarak BT depolama yöneticisinin kontrolündedir ve dolayısıyla bir güvenlik riski olarak görülmez.

Fiziksel olarak BT depolama yöneticisinin kontrolünde olmayan dosya sisteminin kablo veri akışında hareket eden veriler için, yaygın olarak kabul gören ve yerleşik kablo üzerinden aktarılan veri şifreleme uygulaması, geçici oturum şifreleme anahtarı kullanmaktır. Tek bir aktarım, aktarımın ardından derhal kullanımdan kaldırılacak olan bir oturum anahtarıyla şifrelenebilir—bunu takip edecek bütün aktarımlarsa, yeni ve farklı bir oturum anahtarıyla korunur. Bu çok kısa süreli anahtarlar, bir sabit diskte saklanan verilerin şifrelenmesinde kullanılan uzun süreli anahtarların aksine, veri savunmasızlığını en aza indirgerler.

Kullanılabilecek üç oturum şifreleme senaryosu mevcuttur:

Birinci Senaryo:

Veri merkezinden çıkarak, SAN'ı uzak ofislere, diğer kampüslere veya çöküş onarımı için uzak konumlara uzatan Fiber Kanal örgü bağlantıları, potansiyel riskler barındırır. Bu durumlarda, güvenlik, İnternet Protokolü (IP) üzerinden FC bağlantıları kullanılarak ve verinin IP güvenliği ile korunmasıyla sağlanır.

İkinci Senaryo:

Yönlendiriciler ve düğmeler, WAN'lar üzerindeki SAN'ları korumak ve bağlamak için IPSec gibi teknolojilerden faydalanırlar. Bu tür güvenlik tehditlerini özel olarak hedef almak için, düğme ve yönlendiriciler IPSec veri şifrelemesini desteklediği sürece, ana bilgisayar/adaptör bazlı şifrelemeye gerek olmaz. Fiber Kanal teknolojisi, sadece 10 kilometrelik bir mesafeye ulaşabilir; halbuki, BT yöneticilerinin verileri bundan çok daha uzun mesafeler boyunca, hatta bazen coğrafi sınırların ötesine kadar paylaşmaları, korumaları ve göndermeleri gerekir. QLogic, SAN'ları WAN'lar üzerinde bağlayarak, SAN trafiğinin IP üzerinde hareketini mümkün kılan yönlendiriciler ve düğmeler sağlar.

Sunucular için Kendiliğinden Şifrelenen Diskler, NAS ve SAN Dizileri

Üçüncü Senaryo:

IP SAN'ı Internet'e veya özel hatlara genişlettiğinde, bu uzak bağlantılar üzerinde değerli hareketli verileri uzun mesafeler boyunca korumak, veri çoğaltmayı, SAN veri cihaz paylaşımını desteklemek ve yedekleme ve iş sürekliliği sağlamak için, IPSec güvenliği kullanılır. WAN bağlantılarında (geçici anahtarlarla) bağlantının güvenli kalmasını ve anahtarların uzun süre boyunca açığa çıkmamasını sağlamak için, Güvenli Soketler Katmanı (SSL) oturumları kullanılır.

Örgüde fiziksel bir güvenlik koruması olup olmadığına bakılmaksızın, diskin sahibinin kontrolünden çıkmasının ardından, sabit diskteki verilerin korunması hala çok önemli bir gerekliliktir. Yukarıda açıklanan bu oturum güvenliği tekniğini kullanmak yerine, sabit diskteki verileri tüm örgü üzerinde şifrelemek daha iyi bir çözümmüş gibi görünebilir: böylece veriler sadece sabit disk üzerinde şifrelenmekle kalmaz, örgü içinde hareket ederken de şifreli halini korur. Ancak bu yaklaşımda temel bir aksaklık söz konusudur: Bu yaklaşım, güvenliği arttırmaz, aksine azaltır ve uzun ömürlü anahtarlar olan şifreleme anahtarları dayatarak karmaşıklığı arttırırken, sadece tek bir şifreleme anahtarıyla şifrelenmiş yüksek miktarda rakam metni ortaya koyar.

Hareketli veriler için şifreleme gerektiğinde, IPSec veya IP üzerinden FC ile sağlanmalıdır. Disk üzerindeki verilerin şifrelenmesi işlemi, yukarıdaki bölümlerde sözü edilen sebeplerden ötürü, en iyi şekilde diskin kendisi tarafından yapılır.

Ek Bilgiler

Depolama güvenliği hakkında ek bilgilere Trusted Computing Group'tan ulaşılabilir: www.trustedcomputinggroup.org

Bu bilgileri Depolama Ağı Sanayisi Derneği (SNIA) Depolama Güvenliği Sanayi Forumu'ndan (SSIF) da bulabilirsiniz: www.snia.org/forums/ssif/knowledge_center

Kendiliğinden Şifrelenen Disk beyaz bültenleri, web yayınları ve bir performans demosu videosu aşağıdaki adreste bulunabilir: www.SEDSecuritySolutions.com

KUZEY VE GÜNEY AMERİKA Seagate Technology LLC 920 Disc Drive, Scotts Valley, California 95066, ABD, +1 831-438-6550
ASYA / PASİFİK Seagate Technology International Ltd. 7000 Ang Mo Kio Avenue 5, Singapur 569877, +65 6485 3888
AVRUPA, ORTA DOĞU VE AFRİKA Seagate Technology SAS 130-136, rue de Silly, 92773 Boulogne-Billancourt Cedex, Fransa, +33 1 41 86 10 00