

Veri Sızmasını Engellemek...

SafeGuard LeakProof ile,
Sessiz Tehdidi Önlemek...

utimaco[®]
s a f e w a r e

Veri Sızmasını Engellemek SafeGuard LeakProof ile Sessiz Tehdidi Önlemek...

Yıllar süren çalışma ve yatırımlardan sonra, birçok işletme, çevresini güvenceye alma ve içeri sızmayı engelleme yeteneği konusunda kendine güvenir. Her şey bir yana, güçlü güvenlik duvarları, veri şifreleme ve anti-virüs yazılımı erişim elde etmeye çalışan dış güçlere karşı şirketi ve en değerli varlığı olan verilerini korumaktadır. Ancak, tüm bu çözümler yaşamsal değerinde bir bilginin kaybını önlemek için gerekli önlemler olsa da, *iç kaynakların* ele geçirdiği ya da çaldığı bilgiler için koruma sağlamazlar.

Güvenlik ihlallerinin raporlanan % 50sine (raporlanmayanlarla birlikte % 80ine) kuruluşun içinde ve güvenlik duvarının arkasında olanlar neden olmaktadır. Bu belki tüm tehditlerin en büyüğüdür. Ancak, sorun hakkında artan bilince yasal baskılar, markanın zarar görme potansiyeli ve basında çıkacak olumsuz yayınların eklenmesi, hızla büyüyen Veri Sızmasını Önleme (Data Leakage Prevention-DLP) pazarını iyice ateşlemiştir.

Veri Sızmasını Önlemenin (DLP) Tanımı

Analistler mali kayıpla sonuçlanan tüm şirket güvenliği olaylarının % 70inin, farkında olmadan yapılan eylemlerle ya da kimi zaman otoritelerini uygunsuzca suistimal ederek, kurum içindeki kişilerden kaynaklandığını tahmin etmektedir. DLP tanımı, şirket verilerinin kurumun dışında herhangi bir kişiye yetkisiz olarak aktarımını bulma ve önleme çalışmalarını açıklar. Bu, çoğunlukla duyarlı bilgilerin kaza sonucunda yanlış kullanımını önleyen koruma ve uyarı sistemleri kurmak anlamına gelse de, kasıtlı eylemleri tanımlama ve engelleme yeteneğini de kapsar.

Duyarlı bilgilerin kullanıcıların elinde olması riskini azaltmaya yardım eden ve uygunsuz veri taşıma olaylarını asgariye indiren DLP, herhangi bir kuruluşun Bilgi Risk Yönetimi (Information Risk Management-IRM) stratejisinin gerekli bir parçasıdır.

Ayrıca, başarılı bir DLP'nin önceliği, bilgiyi, yaşam döngüsünün tüm aşamalarında tanımlama ve izlemedir. Bu işlem ağda aktarılan "hareket halindeki verileri", dosya paylaşımları, veritabanları ve uç noktalarda saklanan "duran verileri" ve kullanıcı bilgisayarları ya da gezici cihazlarda olan "kullanımdaki verileri" kapsar.

Veri sızmasını önlemek on (hatta 5) yıl öncesine göre çok daha zorlu bir işe dönüşmüştür. Gezici personel sayısındaki keskin artış şirketleri fiziksel duvarların ötesinden veri erişimine izin vermeye zorladı. Bunun yanı sıra, mesajlaşma sistemleri, kablosuz ağlar ve USB bellek cihazları şirket ve müşteri bilgilerinin güvenlik duvarının dışına doğru gizlice yol bulmasını her zamankinden kolay hale getirmiştir.

Bütün bu durumları daha da kötüleştirmek istemesine, bu girişimlerin ödülleri de daha önce hiç olmadığı kadar yüksektir. Payment Card Industry (PCI) Data Security Standard (Ödeme Kartı Sektöründe Veri Güvenliği Standard), ABD'deki Sağlık Sigortası Taşınabilirliği ve Sorumluluğu Yasası (Health Insurance Portability and Accountability Act-HIPAA), Gramm-Leach-Bliley Yasası (GLBA), Avrupa Birliği Veri Koruma Yönergesi, 1386 Sayılı Senato Yasası ve Sarbanes-Oxley gibi çok çeşitli veri güvenliği ve mahremiyet düzenlemelerinin çıkışı kuruluşları bilgiyi gizli tutmak ve müşteri mahremiyetini korumak üzere politikalar uygulamaya ve ölçütlerini belgelemeye zorlamıştır. Ve burası veri sızmasının en fazla zarara neden olabileceği yerdir. Uyumsuzluk ve ihlaller tazminatlar ve pahalı hukuksal işlemlerle sonuçlanabilir; afişe olan olaylardan kaynaklanan olumsuz yayınlardan söz bile etmiyoruz.



SafeGuard LeakProof'a Bir Giriş

Utimaco'nun SafeGuard LeakProof ürünü verinin iki uç nokta arasında saptanmasına, sınıflandırılmasına, korunmasına ve izlenmesine yardımcı olmaktadır. Özellikle, şirketlerin uç noktalardan (yani genellikle verinin en çok sızdırıldığı yerlerden) doğrudan doğruya veri sızmasını önlemelelerinde yardımcıdır. Gezici, şube ve şirket ofisleri için ideal olan SafeGuard LeakProof şirketlerin uç noktalarında dosya içeriklerini araştırmak, hareket halindeki duyarlı dosyaları saptamak ve gizli belgelerin aktarımını engellemek, işlemi kaydetmek, belgeyi şifrelemek ya da işlem için bir gerekçe ya da neden girilmesini zorlamak suretiyle, veri kullanım ihlali risklerini büyük ölçüde azaltır. Öte yandan, zorlanabilen politikalar kurmak, önceden ayarlanan uyumluluk şablonları sunmak, şirketlerin sürekli olarak risk değerlendirmesi yapmasına, ihlalleri izlemesine, kaydetmesine ve onları engellemesine yardımcı olmak ve elemanları çeşitli durumlarda kurumsal bilgilerin en iyi nasıl ele alınacağı konusunda eğitmek suretiyle de, kurallara uyumu olanaklı hale getirir.

SafeGuard LeakProof bir yönetim konsolunun yanı sıra, istemci yazılımı da içermektedir. Bileşenleri, duyarlı bilgileri korumak ve hem kasıt, hem de kaza sonucu veri sızmalarını önlemek için birlikte çalışırlar.

İstemci Yazılımı

SafeGuard LeakProof uç noktalarda yüksek kesinlikte, yüksek performanslı filtrelemeden yararlanır ve tüm veri işlemlerini gerçek zamanlı olarak ve "sır" ya da "gizli" gibi duyarlı anahtar sözcükle dayanarak tarar. USB cihazlarına, Bluetooth'a, Webmail'e, FTP'ye, HTTP'ye ve anında mesajlaşmaya yönelik dosya hareketleri olduğunda SafeGuard LeakProof arka planda sessizce çalışıp, belge parmak izlerinde içerik bulma zekasını kullanarak, bildiği duyarlı dosya özelliklerini arar. Ayrıca, kredi kartı numaraları ya da diğer müşteri bilgileri gibi veri yapılarını tanır. Duyarlı bilgiler bulunduğu, SafeGuard LeakProof bu bilgilerin güvenliğini sağlamak için gereken ölçütleri proaktif olarak uygular. Yazılım:

- * Kullanıcıyı uyarıp mesajlar göndererek kaza sonucu veri sızması olaylarını azaltır
- * İşlemi kaydedip engelleyerek kasıtlı veri sızması olaylarını asgariye indirir
- * Hareket halindeki veriyi şifreleyerek korur

IDC analiz firmasına göre, gizli bilgilerin % 70 ten fazlası uç noktada tutulmaktadır.

Yönetim Konsolu

Her kuruluş gizli bilgileri değişik biçimde tanımlar. Dolayısıyla, SafeGuard LeakProof özgün bir duyarlı anahtar sözcükler kümesi, parmak izli belgeler ve kurallı ifadelerle, yöneticilerin bir içerik politikasını tanımlamalarına olanak sağlar. Yöneticiler konsol sayesinde, her bir uç noktayı tarayarak tüm duyarlı bilgilerin yerini bulabilir, olayları izleyebilir ve kuşku işlemler üzerine adli kovuşturmalar başlatabilir. Dahası, konsol olayların kuruluş içinde değişik roller tarafından ele alınmasına olanak veren bir iş akışını kurmaktadır. Konsol aynı zamanda, güvenlik ihlallerinin uç noktalara, kullanıcılara ve veri türlerine göre izlenebildiği bir gösterge panelini de sunmak suretiyle, şablonların kurulmasına ve kuşku işlemlerin işaretlenmesine yardımcı olur.

Özgün Parmak İzi Teknolojisi

SafeGuard LeakProof her duyarlı belgenin bir "parmak izini" oluşturmak için, patentli bir teknolojiden yararlanmaktadır. Bu işlem her içerik parçası üzerindeki işaretleri tanıyan özgün bir şablonu hesaplamak suretiyle yapılır. Sonra "parmak izi" dağıtılır ve her uç noktadaki küçük bir dosyada saklanır. Belgeler değişik ortamlara taşındığı zaman algoritma onları hızla tarar ve saklanan bir "parmak izi" ile eşleşme varsa, belge gizli olarak işaretlenir. Algoritma hemen tüm dosya türleri ve Çince ile Japonca dahil olmak üzere her dildeki belgeler üzerinde çalışmaktadır.

Yararları

- × Mahremiyeti korumak – Müşteri ve personel bilgilerinin uygunsuz kullanımını izlemek ve engellemek
- × Entellektüel mülkiyeti korumak – Kritik şirket varlıklarını bulmak, sınıflandırmak ve izlemek
- × Gizlilik düzenlemelerine uymak – Kullanımı izlemek, uç noktaları taramak ve riski azaltmak üzere personeli eğitmek
- × Personeli eğitmek – Personel eğitimi ve iş akışları için etkileşimli diyaloglar uyarlamak
- × Duyarlı bilgileri bulmak – Dizüstü, masaüstü ve sunuculardaki duyarlı verileri bulmak

Veri Sızmalarını Önlemek

- × Gezici, şube, şirket merkezi
- × Çevrim içi, çevrim dışı uç noktalar
- × Şirket ağları
- × Halka açık ağlar
- × USB, Bluetooth, WiFi, e-posta
- × Hareket halindeki, duran ve kullanılan veriler

Sonuç

Utimaco SafeGuard LeakProof'u işletmelerin güvenlik çalışmalarını veri sızmasını önlemeyi kapsayacak biçimde genişletmesine yardım etmek için bir yöntem olarak portföyüne eklemiştir.

SafeGuard LeakProof işletmelerin dizüstleri, masaüstleri ve sunuculardaki tüm gizli bilgileri tanımasına ve bu bilgilerin yetkisiz hedeflere yönelmesini izlemesine ve engellemesine yardımcıdır. SafeGuard LeakProof bunu yaparken, uyumsuzluk riskinin azalmasını destekler, mahremiyeti sağlar ve şirket bilgilerini korur.

www.utimaco.com

MERKEZ
Utimaco Safeware AG
P.O. Box 20 26
61410 Oberursel
Almanya
Telefon +49 (61 71) 88 0
Faks +49 (61 71) 88 10 10
E-Posta: info@utimaco.com

Utimaco Safeware AG
Hohemarkstraße 22
61440 Oberursel
Almanya
Telefon +49 (61 71) 88 14 44
Faks +49 (61 71) 88 14 90
E-Posta: info.de@utimaco.com

ABD
Utimaco Safeware Inc.
10 Lincoln Road
Foxboro, MA 02035
Telefon: +1 (508) 543 1008
Faks: +1 (508) 543 1009
E-Posta: sales.us@utimaco.com

BİRLEŞİK KRALLIK
Utimaco Safeware Ltd.
Ash House
Fairfield Avenue
Staines
Middlesex TW18 4AB
Telefon: +44 1784 22 42 25
Faks: +44 1784 22 42 29
E-Posta: sales.uk@utimaco.co.uk

JAPONYA
Utimaco Safeware K.K.
Nisso 16 Building, 3F
3-8-8 Shin Yokohama, Kohoku-ku
Yokohama 222-0033
Japonya
Tel.: +81(0)45 470 1430
Faks: +81(0)45 470 1431
E-Posta: info.jp@utimaco.jp

HONG KONG
Utimaco Safeware Asia Ltd.
Unit 602, Stanhope House
734 King's Road
Quarry Bay
Hong Kong
Telefon: +8 52 25 20 26 08
Faks: +8 52 25 29 26 18
E-Posta: info@utimaco-asia.com

FRANSA
Utimaco Safeware France
8, Place Boulois
75017 Paris
Telefon: +33 (1) 56 21 25 25
Faks: +33 (1) 42 67 30 00
E-Posta: info@utimaco.fr

İSVİÇRE
Utimaco Safeware (Schweiz) AG
Zürcherstrasse 20
8952 Schlieren
İsviçre
Telefon: +41 (44) 7 35 40 80
Faks: +41 (44) 7 35 40 85
E-Posta: info.ch@utimaco.ch

AVUSTURYA
Utimaco Safeware AG
im Regus TwinTower
Wienerbergstrasse 11/12
1100 Wien
Avusturya
Telefon +43 1 99 460 6517
Faks +43 1 99 460 5000
E-Posta: info@utimaco.at

BENELÜKS
Utimaco B.V.
Hoevestein 11B
4903 SE Oosterhout (NB)
Hollanda
Telefon: +31 (162) 480 240
Faks +31 (162) 430 330
E-Posta: sales@utimaco.nl

İSVEÇ
Utimaco Safeware AB
Box 16, Malaxgatan 1
16493 Kista
Telefon: +46 (8) 5 84 00 600
Faks: +46 (8) 5 84 00 610
E-Posta: info.se@utimaco.com

FİNLANDİYA
Utimaco Safeware Oy
Airport Plaza Presto
Äyritie 12 B
01510 VANTAA
Telefon: +358 9 855 3200
Faks: +358 9 855 32030
E-Posta: info.fi@utimaco.com