YAZILIM ŞIFRELEME VE YASAL UYUM: ÖNEMLI GÜVENLIK RISKLERINE SAHIP DAHA UCUZ ÇÖZÜM

DÜZENLEYICI VE UYUM GEREKSINIMLERI

Eskiden Veri Güvenliği yalnızca IT bölümlerinin görevleri arasındaydı. Ancak sürekli tüketici veri ihlallerinin ortaya çıkmasıyla dünya genelinde devletler, kişisel olarak tanımlanmayı sağlayabilecek tüm verilerin şifrelenmesi ve korunması için kurumlara her geçen gün daha fazla gereksinim uygulamaya başladı.

Sağlık sektöründeki HIPAA'dan EMEA'da GDPR ve Kaliforniya'da CCPA'ya kadar koruma altındaki veri sınıflarının şifrelenmesi düzenlemelerle zorunlu hale getiriliyor. Uyum kuruluşlarının sayısı yaklaşık son 3 yılda, bu düzenlemeler ve bunlara bağlı cezalar ve yasal ödül risklerinin çok artmasıyla müthiş oranlarda yükseldi.

Bu değişikliklerle IT bölümleri, güvenlik ve giderek artan maliyetlerle baş etmekte zorlandılar. COVID pandemisi boyunca, bütçeler veri şifrelemeye odaklanılarak ek donanım ve güvenlik duvarı yatırımlarına harcanıyor.

Aslında, Microsoft BitLocker® kullanan yazılımsal şifreleme veya Symantec, McAfee gibi şirketlerin uç nokta yönetim yazılımlarının popülerliği artıyor. Bazı işletmeler ve tüketiciler, bazı sağlayıcıların yazılımsal "kasa" sürücülerine sahip standart USB belleklerini de kullanıyorlar.

ŞIFRELEME VE TAŞINMAKTA OLAN VERI

Çalışanlar ve tüketicilerin verileri yanında taşıması gerekmektedir. Bunun için aşağıdaki seçeneklerden yararlanabilirler:

1. Bulut hizmetleri: Bunlar harika olanaklardır ve internete bağlı herhangi bir cihazdan erişilebilir. Ancak bu esneklik belirli bir fiyat karşılığında elde edilmektedir. Bulutta veri saklama, verilerinin kontrolünün kullanıcının ya da şirketin elinden çıkmasına neden olur ve kilitlenmeyen ya da erişilen Bulut sunucular gördüğümüzden risk potansiyeline sahiptir.
2. Standart USB bellekler: Bir USB bellek taşımak daha güvenli görünse de belleğin kaybedilmesi durumunda verilerin ifşa olması riski yüksek olabilir. Örneğin, içinde gizli bilgilerin bulunduğu kayıp bellekler ya da içi kaybolmuş USB belleklerle dolu çamaşırhane çekmeceleri ile ilgili birçok hikaye bulunmaktadır.
3. Donanım şifrelemeli USB bellekler: Bu USB bellekler, yerleşik bir şifreleme denetleyicisi ve erişim denetimi içeren özel mimarilere sahiptir. Veriler, genellikle XTS modunda en güçlü AES-256 bit şifreleme ile şifrelenir ve fiziksel ve ürün yazılımı tabanlı saldırıları azaltmak için diğer olası güvenlik önlemleri ile korunur. Bu bellekler, güvenlik cihazlarında uzmanlaşmış şirketler tarafından üretilir ve standart USB belleklerden daha pahalı olsa da daha iyi veri güvenliği sunar. FIPS 197 veya FIPS 140-2 Seviye 3 bellekler, daha yüksek düzeyde koruma ve iç rahatlığı sağlayabilir.
4. Yazılım şifrelemeli standart USB bellekler: Yönetmeliklerin gerektirdiği güvenlik adına, BitLocker veya diğer araçlarla yazılım şifrelemesi kullanılabilir. Bunlar göreceli ucuz oldukları ve aynı AES-256 XTS şifrelemesini sundukları için iyi seçeneklerdir.

Çoğu durumda, işletmelerin ve endüstrilerin yazılım şifrelemeli Standart USB bellekleri kullanarak seçenek 4'ü seçme eğiliminde olması şaşırtıcı değildir. Bunun ana nedeni BitLocker veya diğer veri kasası yardımcı programları gibi yazılım şifrelemesi "ücretsizdir".

YAZILIM ŞIFRELEMESI YÖNETMELIKLERE UYGUN DEĞILDIR

Bir iş güvenliği uzmanı için yazılım şifrelemesi, daha pahalı donanım şifrelemeli USB belleklerle tam olarak aynı şifreleme özelliklerini sunabilir. Peki bu doğru bir tercih midir? İşletmeler, bütçeler kısıtlı olduğundan, yazılım tabanlı şifrelemenin karanlık tarafından haberdar olmadan uyumluluk amacıyla yazılım şifrelemesine geçiyor.

Yazılım şifrelemeli USB belleklerle ilgili sorun nedir? Saklanan veri ve taşınmakta olan veriler, AES-256 XTS ile şifrelenmiyor mu? Genellikle şifreleniyor. Asıl sorun şudur: Yazılım şifrelemesi, "kaldırılabilir şifreleme" olarak kabul edilmektedir.

Bir dakika... Kaldırılabilir mi? Yani yazılım şifrelemeli bir USB belleğin şifrelemesi, bir kullanıcı tarafından devre dışı bırakılabilir mi?

Yanıt: Evet. Kullanıcılar, yazılım şifreleme özelliğini USB belleklerinden kaldırabilir. Neden bunu yapsınlar ki diye sorabilirsiniz. Çünkü bunu yapabilirler ve çünkü dosyalara parola kullanmadan erişmek isterler ya da parolayı unutmuş ama USB belleği kullanmaya devam etmeleri gerekli olabilir.

ŞIFRELENMIŞ BIR USB BELLEKTEN YAZILIM ŞIFRELEMESI NASIL KALDIRILIR

Verilerine erişmek için karmaşık veya başka parolalar girmekle uğraşmak istemeyen bir kullanıcı için işlem basittir:

1. Yazılım şifrelemeli belleği bir bilgisayara takın
2. Belleği biçimlendirin
3. Bellek biçimlendirildikten sonra tüm şifreleme kaldırılmış olur
4. Kolay erişim için gizli veya özel bilgiler içeren dosyaları belleğe kopyalayın

Bu işlemi, kullanıcıların kısıtlanmamış bir bilgisayar kullanarak yapması kolaydır. IT departmanları, şirket bilgisayarlarında biçimlendirme komutlarının kullanımını kısıtlamıştır, ancak bu işlem, şirket dışı herhangi bir bilgisayarda yapılabilir.

Uyumluluk amacıyla: veri şifrelemesini kaldırma kolaylığı, bellekte yer alan şifrelenmiş veriler, şifreleme yukarıdaki yöntemle kaldırıldıktan sonra sonsuza kadar kaybolmuş olarak kabul edilse bile (şifreleme anahtarları verilere bağlanır) şirket tarafından sağlanan bellek artık şifrelenmemiş durumdadır. Şifreleme kaldırıldıktan sonra cihaza kopyalanan herhangi bir verinin güvenli olmadığı ve HIPAA, GDPR, CCPA ve diğer pek çok düzenlemeyi ihlal etme riski yaratabilecek düzenlemelere uyumsuz olabileceği kabul edilir.

ŞIFRELENMEMIŞ BELLEKLERIN KAYBEDILMESININ SONUÇLARI

Şirket tarafından verilen bir USB bellek kaybolur ve başka biri tarafından bulunursa, şirket ilk başta farkında olmasa da daha sonra sosyal medya aracılığıyla bunu öğrense bile, şirket için aşağıdakileri yapmasını gerektirebilecek özel uyumluluk gereksinimleri devreye girer:

1. Hangi verilerin kaybolduğunu belirlemek için adli soruşturma yürütmek
2. Hukuk bölümüne danışarak yasal bir ihlal olup olmadığını belirlemek
3. Müşterilerin bilgilendirilmesi gerekip gerekmediğini belirlemek

Sadece bir USB belleğin kaybedilmesinin çok masraflı olabileceği yer bu noktadır. Saatte yüzlerce doları aşan hukuki hizmet ücretleriyle, bu uyum süreci, olası para cezalarına, müşteri ve diğer davalara ve veri ifşasından kaynaklanan itibar kaybına ek olarak binlerce dolarlık masrafa neden olabilir.

Yazılım şifrelemesi, düşük maliyetli uygulaması nedeniyle tercih edildiğinde, bu riskler ve bunların büyük mali sonuçları dikkate alınmamaktadır.

Bir şirket ağında şifrelenmemiş USB belleklerin kullanımına izin vermenin başka bir tehlikesi daha vardır. Buna genel olarak "BadUSB" (Kötü USB) adı verilmektedir. BadUSB, kötü niyetli kişiler tarafından bir şirketin güvenlik duvarını ihlal etmek ve USB depolama cihazları aracılığıyla bir şirketin siber savunma sistemlerine kötü amaçlı yazılım sokmak için kullanılan bir kötü amaçlı yazılım sınıfıdır.

BadUSB

Bir bilgisayara bir USB bellek takıldığında, bilgisayarın yonga seti denetleyicisi, cihaz yazılımı aracılığıyla USB belleğin denetleyicisi ile iletişim başlatır. Bu veri alışverişi, Microsoft/macOS/Linux gibi İşletim Sistemi bir USB belleğin bağlandığının farkında bile olmadan gerçekleşir. Her USB bellekte, bellek bir USB bağlantı noktasına takıldığında çalışan cihaz yazılımı bulunur.

Kötü niyetli kişiler, USB bellekte çalışan cihaz yazılımını, USB bellekle iletişim kurarken kötü amaçlı yazılım yerleştiren kötü amaçlı başka bir yazılım ile değiştirerek hedef bilgisayar sistemine, bu iletişim mekanizması aracılığıyla kötü amaçlı yazılım sokabileceklerini öğrendiler. Standart bir USB belleğin, denetleyicisi tarafından yürütülen dahili yazılımı üzerinde hiçbir güvenliği yoktur. Yani BadUSB, güvenlik duvarlarını aşmak ve siber savunmaları geçmek için iyi USB belleklerin silahlandırılmasıyla doğdu.

Birçok şirket, sistemlerinde USB belleklerin kullanımını yasaklamaya çalışıyor, hatta önlemleri, USB bağlantı noktalarını epoksi ile doldurmaya kadar varıyor. Ancak, bazı çalışanların yanlarında USB belleklerle veri taşıması gerektiğini anladılar. Örneğin, yöneticiler verileri üzerinde çalışmak için yanında götürmek veya bir şirket Bulutu üzerinde olmayan dışarıdan Hukuki veya Mali danışmanlara; üzerinde çalışmak için verilere ihtiyaç duyan ancak şirket veritabanlarına sınırlı erişimi olan şirket yüklenicilerine; aylık raporları kapatmak için acelesi olan ve evde elektronik tablolar üzerinde çalışması gereken finansal analistlere vermek isteyebilirler.

Önceki analizlerin gösterdiği gibi, bu standart USB bellek + yazılım şifreleme çözümünü kullanmanın önemli bir riski vardır. İlk bakışta, daha ucuz görünen çözüm, sonunda çok zararlı ve çok daha pahalı hale gelebiliyor. Potansiyel bir veri ihlali hakkında bir avukatla 2-3 saatlik görüşme maliyeti, daha ucuz çözümü kullanmanın sağladığı tüm tasarrufları ortadan kaldırır.

DONANIM ŞIFRELEMELI USB BELLEKLER, YÖNETMELIKLERE UYUM IÇIN EN IYI SEÇENEKTIR

Donanım şifrelemeli USB belleklerin, bu yönetlikler kapsamındaki uygulamalar için en iyi tercih olmasının nedenleri:

1. Donanım şifrelemeli USB bellekler, her zaman AÇIK olan şifrelemeye sahiptir: Kullanıcıların şifrelemeyi kapatmasının, parola kurallarını (minimum uzunluk, karmaşıklık) sıfırlamasının ve otomatik parola yeniden deneme sayısını devre dışı bırakmasının bir yolu yoktur. Yazılım sözlük saldırıları yoluyla tekrarlanan parola tahminini engellemeyen yazılımla şifrelemenin aksine, donanım şifrelemeli modeller parola yeniden deneme sayısını sınırlar ve 10 kez veya bazen daha da az kez yanlış parola girildiğinde verileri kilitler. Bu, süper bilgisayarlar çağında çok güvenli bir seçenektir.
2. Donanım şifrelemeli bellekler, birinci sınıf şifreleme denetleyicileri kullanır ve birçok güvenlik özelliği içerir: Tüm güvenlik önlemlerini her zaman açıklamasak da BadUSB'ye karşı korunmak için bir önlem vardır. Fabrikada yazılım, yalnızca donanım şifrelemeli belleklere yüklenirken dijital olarak imzalanır ve yüklenir. Yani bu şifrelenmiş USB bellekler takıldığında, şifreleme denetleyici ilk olarak dijital imza aracılığıyla yazılım bütünlüğünü kontrol eder ve bellek, yalnızca doğrulamayı geçerse yüklenir. Yazılımı değiştirmeye yönelik herhangi bir girişim, belleği kullanılmaz hale getirecek ve tehdit oluşturmasının önüne geçecektir.
3. Donanım şifrelemeli USB bellekler, belirli bir şirket için ayarlanmış özel Ürün Kimliklerine (PID'ler) sahip olabilir: Bu üst düzey bellekler, içlerinde programlanmış bir dijital tanımlayıcıya sahip olabilir. Böylece bir bellek şirketin iç veya dış güvenlik duvarına takıldığında, bellek şirket tarafından verilmiş bir bellek olarak tanımlanabilir. Örneğin, bir çalışan şirket tarafından verilen belleği kaybederse ve aynı modeli mağazalardan satın alırsa, yeni satın alınan bellek şirket ağında doğrulanmaz. Bu özelleştirme, USB belleklerin kullanımına başka bir güvenlik katmanı ekler.
4. Donanım şifrelemeli bellekler çok hızlı bir şekilde tasarruf sağlar: Sadece risklerin azaltılması ve ortadan kaldırılması, parasını çıkarma süresini kısaltır.

Kingston, dünyanın en büyük Şifrelenmiş USB bellek üreticisidir ve çeşitli özelliklere ve fiyat düzeylerine sahip bellek ürün serileri sunmaktadır. Yöneticiler, çalışanlar, yükleniciler ve daha fazlası için Şifrelenmiş USB çözümleriyle yönetmeliklere uyumlu kalmanıza nasıl yardımcı olabileceğimizi görüşmek üzere doğrudan Kingston ile iletişime geçin.