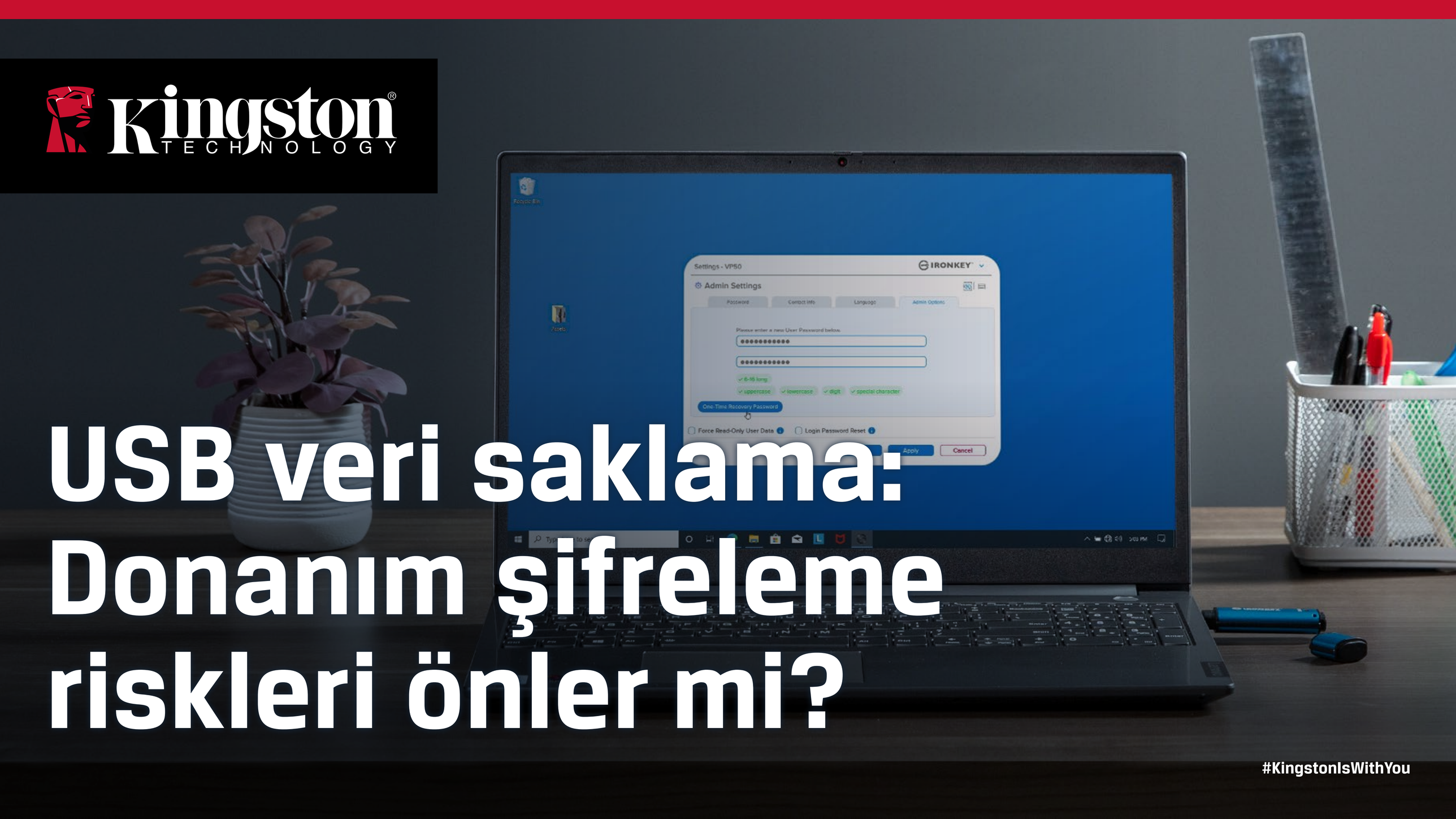
Kingston
TECHNOLOGY
Settings - VP50
IRONKEY
Admin Settings
Password
Contact Info
Language
Admin Options
Please enter a new User Password below.
6-16 long
uppercase
lowercase
digit
special character
One-Time Recovery Password
Force Read-Only User Data
Login Password Reset
Apply
Cancel
USB veri saklama:
Donanım şifreleme
riskleri önler mi?
#KingstonIsWithYou

USB veri saklama: Donanım şifreleme riskleri önler mi?

Önsöz ve içindekiler

Siber güvenlik işletmeler için her zamankinden daha büyük bir endişe kaynağı olmasına karşın çok sayıda kuruluş siber güvenlik tehditleri konusunda bilgisiz ve hazırlıksızdır. UpCity'ye göre, Amerika Birleşik Devletleri'nde işletmelerin yalnızca %50'sinin bir siber güvenlik planı var; bunların %32'si, birçok kuruluşun uzaktan veya hibrit çalışma modellerine geçtiği COVID-19 salgınının başlangıcından bu yana siber güvenlik planlarını güncellemedi. Ve siber saldırıların sıklığı giderek artıyor: dünya çapında fidye yazılımı saldırılarına maruz kalan işletmelerin sayısı 2020'de %37 iken 2021'de %66'ya yükseldi[1].

Siber güvenliğin tehlikeye atılmasının bir işletme üzerinde yıkıcı etkileri olabilir. Siber saldırıların parasal maliyetinin yanı sıra veri, güvenlik ve itibar kaybı, kuruluşları hem kısa hem de uzun vadede birçok yönden olumsuz etkileyebilir.

Siber güvenlik tehditlerinde yaygın biçimde kullanılan bir araç USB sürücülerdir. Bunlar basitlikleri nedeniyle birçok kuruluşta çokça kullanılmaktadır. Bir makineye takılmalarıyla birlikte kullanıma hazırdırlar. Ancak, USB sürücüleri saldırılara karşı bu kadar savunmasız bırakan da tam olarak bu basitliktir: Kötü niyetli bir kişinin potansiyel olarak hassas verilere erişmesi için tek gereken yanlış yere konmuş veya çalınmış bir sürücüdür. İşte bu noktada şifreleme, USB sürücüleri kullanım için güvenli hale getirmede ve birey ve kuruluş için ilgili riskleri azaltmada önemli bir rol oynayabilir. Bu e-Kitapta aşağıdaki önemli soruları yanıtlıyoruz:

- Şifrelenmiş USB'ler siber saldırılara karşı korunmada neden bu kadar önemli?
- Kuruluşlar kendilerini nerede savunmasız hale getiriyor?
- Kendilerini korumak için neler yapabilirler?

USB veri saklama:
Donanım şifreleme riskleri önler mi?

Katılımcılar

Bu e-Kitap, kendi teknik uzmanımızın yanı sıra BT ve gelişmekte olan teknolojiler alanında sektörün önde gelen isimleriyle birlikte hazırlanmıştır.

David Clarke

David, Thompson Reuter'ın "Birleşik Krallık'ta, risk yönetimi, uyum ve yasal teknolojiler alanında sosyal medyanın en etkili 30 kanaat önderi ve düşünürü" listesinde en etkili 10 kişi arasında ve Kingston Technology'nin En Etkili 50 Global Uzman listesinde yer almaktadır.

Pasi Siukonen

Pasi, Kingston'ın Halkla İlişkiler, Kingston ürünleri ile ilgili Pazarlama, Saha Satışları, Teknik Destek ve Müşteri desteği gibi Kingston departmanlarını destekleyen uzmanlardan oluşan bir ekipten sorumludur. Odaklandığı ana ürün grubu Flash ve SSD ürün serileridir.

Standart ve şifrelenmiş sürücüler arasındaki fark

Standart (şifrelenmemiş) sürücülere erişmek ve kullanmak son derece kolay olsa da donanım şifrelemesi USB veri saklama cihazlarını çok daha güvenli hale getiren hem fiziksel hem de dijital çeşitli güvenlik katmanları eklemektedir. Standart şifrelenmemiş sürücülerin kolay bulunabilirliği, düşük maliyeti ve taşınabilirliği, kullanıcı açısından çok kullanışlı olmasına karşın hassas verileri çalmak, şirket ağına kötü amaçlı yazılım veya fidye yazılımı sokmak gibi hedeflere sahip kötü niyetli kişiler için de kullanışlı olmalarına neden olmaktadır. USB'ler çok sık kullanıldığından, siber saldırılar için birçok fırsat bulunmaktadır. Standart sürücülerle ilişkili iki ana risk vardır:

- **Fidye yazılımı saldırıları:** USB tabanlı bu saldırılar, şirket ağlarına kötü amaçlı yazılımların sokulmasını, şirket bilgilerinin ve/veya sistemlerinin şifrelenerek fidye talep edilmesini içermektedir. Bunlara BadUSB adı verilmektedir ve şu anda en hakim kötü amaçlı yazılım haline gelmiştir.
- **Verilerin çalınması:** İster müşteri bilgileri, ister kaynak kodu, isterse de hassas finansal ve performans verileri olsun, kötü niyetli bir kişinin sürücüde saklanan verilere kolayca erişebilmesi için uygun güvenlik önlemlerinin alınmadığı kayıp, çalıntı veya ortada bırakılmış bir sürücü yeterlidir.

BadUSB – korumalı olmayan cihaz yazılımına sahip USB sürücülerin güvenlik açığından yararlanabilen ve daha sonra kötü amaçlı yazılımlarla programlanabilen bir saldırı türüdür. Bu kötü niyetli araçlar son derece yaygındır ve siber suçlular tarafından kolayca ulaşılabilir. Ancak bu araçlarla ilgili farkındalık düşük kalmaya devam etmektedir. Bu da USB sürücünün standart bir sürücünün yazılımını, bir klavye gibi davranabilen ve temel olarak güvenlik duvarına saldırmak için komut dosyaları çalıştırabilen bir yazılım ile değiştirerek bu saldırıları gerçekleştirmeyi çok kolay hale getirir. Pek çok siber saldırı, kötü niyetli olsun ya da olmasın, tehditlerin farkında olmayan şirket içinden kişiler aracılığıyla gerçekleştirildiğinden, siber suçluların başarı şansını azaltabilecek bu saldırıları önlemek için işletmelerin korumalı, dijital olarak imzalanmış ürün yazılımına sahip şifreli sürücüler kullanması son derece önemlidir.

> **Altyapıyı yeniden inşa etmenin ve belki de fidye ve diğer haraçları ödemenin maliyeti, yönetimli USB'lerin maliyetine kıyasla çok büyüktür. - David Clarke**

Neden şifrelenmiş USB'ler kullanılmalı?

Şifrelenmiş sürücüler, içinde bulunan verilerin yanı sıra sürücünün bağlanabileceği tüm cihazları korumak için özel olarak tasarlandığından herhangi bir kuruluşun BT cephaneliğinde değerli araçlardır. Siber güvenlik tehditleri daha gelişmiş hale geldikçe, şifreli sürücülerin özellikleri de gelişerek bu cihazlardan faydalanmak isteyen siber suçluların önüne geçmelerini sağladı. Kingston IronKey™ donanım şifrelemeli ürün serisinde görüldüğü gibi, en güçlü XTS modunda AES 256 bit şifreleme, sağlam ve kurcalamaya dayanıklı muhafaza, dijital olarak imzalanmış yazılım, sanal klavyeler, karmaşık parola ya da parola ifadesi modları gibi özellikler, kullanıcıların her türlü saldırıya karşı gerçekten korunmasını sağlamak için yıllar içinde geliştirilmiş ve eklenmiştir.

Siber riskler genellikle yeterince anlaşılmadığından, birçok işletme beraberinde getirdiği çeşitli güvenlik açıklarına karşın standart sürücüleri kullanmayı tercih etmektedir. Bunların kolay bulunabilirlikleri, düşük maliyetleri ve yazılım şifrelemesinin kullanımı, flash bellekler için kurumsal bir onay sürecinin olmaması gibi etkenler burada rol oynamaktadır. Çoğu zaman ISO27001, GDPR, SOC2 ve WISP devlet en iyi uygulamaları gibi çeşitli BT ve siber güvenlik standartlarına uymak için kurumsal en iyi uygulama politikaları veya süreçleri yoktur. Bu da risklerin genellikle kanıtlardan çok görüşlere dayalı olarak değerlendirildiğini göstermekte ve birçok kuruluşu saldırılara karşı savunmasız halde bırakmaktadır.

Bazıları mevcut yazılım şifreleme araçlarına sahip standart sürücüler kullansa da bu genellikle kötü bir yatırım olabilir. Bunun nedeni birçok yazılım şifrelemeli sürücünün internette herkesin kullanabileceği ücretsiz veya ücretli araçlarla kırılabiliyor olmasıdır. Yazılım şifrelemesi, kullanım kolaylığı sağlamak veya sürücüleri desteklenmeyen işletim sistemli platformlarda kullanmak için bir kullanıcı tarafından sürücünün basit bir şekilde yeniden formatlanmasıyla da kaldırılabilir. Donanım şifrelemeli USB'ler kapatılamayan her zaman açık şifrelemeye sahip olsalar da amaca uygundurlar. Kurcalanmaya karşı dayanıklı, kurcalanmaları gösterecek şekilde üretilmişlerdir ve sürücünün güvenilirliğinden ve sağlamlığından emin olmak için dijital olarak imzalanmış yazılım kullanırlar. IronKey VP50 gibi şifrelemeli sürücülerin diğer iki özelliği olan parola denemelerini sınırlama (Brute Force saldırı koruması) ve sanal klavyeler (tuş kaydetme ve ekran kaydetmeye karşı koruma), tehditlerin farkında olmayan kullanıcılardan parola almayı amaçlayan kötü niyetli kişilere karşı sektördeki en iyi uygulamalarla uyumluluğu sağlamaktadır.

> IronKey sürücüsü cihaz yazılımının değiştirildiğini tespit ederse, sürücüyü kullanılmaz hale getirerek ve açılmayarak siber güvenliği artırır.
> - Pasi Siukonen

Kimler risk altında?

Gerçekten de USB erişimlerini kontrol edemeyen tüm şirketler risk altındadır ve genellikle bu risklerin tam olarak ne olduğunun farkında değildirler. Bununla birlikte, bazı şirketleri siber saldırılar için daha çekici ve savunmasız hedefler haline getirebilecek etkenler vardır.

Sağlık ve finans sektörlerindeki şirketler açısından bakıldığında bu şirketlerin verileri hem siber suçlular için çok daha cazip hem de kuruluşları ve müşterilerini daha ciddi şekillerde etkiliyor. Birleşik Krallık'ta, 2017 yılında NHS'yi hedef alan bir siber saldırı 19.000'den fazla randevunun iptal edilmesine neden oldu ve NHS'ye 92 milyon sterlinlik üretim kaybının yanı sıra veri ve sistemleri geri yükleme maliyetine mal oldu. Bu durum yalnızca etkilenen hastaların sağlık hizmeti almasını engellemekle kalmadı, aynı zamanda NHS, daha önceki siber tehdit uyarılarına yeterince çabuk veya ciddi bir şekilde yanıt vermediği için ağır bir şekilde eleştirildi. Tüm kuruluşların siber güvenlik konusunda güncel ve bilgili olması gerekirken, özellikle özel kategorideki veriler olmak üzere hassas bilgilerle ilgilenen kuruluşlar siber riskler konusunda çok daha dikkatli olmalıdır.

Şirketin ciro ile ölçülen değeri ne kadar yüksekse, kötü niyetli aktörler için ödül ve dolayısıyla siber tehditlerden kaynaklanan risk de o kadar büyüktür. Ancak bu, daha küçük kuruluşların siber güvenlik konusunda endişe duymaması gerektiği anlamına gelmemelidir. Büyük kuruluşlar saldırılar için daha cazip hedefler olsalar da genellikle siber tehditleri ele alacak kaynaklara ve özel çalışanlara da sahiptirler. Öte yandan, pek çok KOBİ'nin özel siber güvenlik ekipleri yoktur ve üst düzey yöneticiler için USB yönetiminden kaçınma istisnaları yaparlar. Bu da onları yıkıcı sonuçlara karşı önemli ölçüde savunmasız hale getirir. Bazı araştırmalar, aslında küçük ve orta büyüklükteki işletmelerin siber saldırılar için daha fazla hedef alındığını göstermektedir.

Üst düzey yönetici pozisyonundaki çalışanlar için risk daha da büyüktür. Bu kişiler kolayca izlenebilir ve genellikle kuruluşlarında yönetici ayrıcalığına sahiptir. Yani USB yönetim prosedürleri gibi siber kontroller onlar için uygulanmaz. Dolayısıyla siber suçlular için kazançlı hedefler haline gelirler. İşte bu noktada, siber güvenlik konusunda bilgili olmanın ve en iyi uygulamaları ve süreçleri takip etmenin yanı sıra sürekli açık donanım şifrelemeli sürücüler, riski azaltmada ve saldırılara karşı korunmaya büyük katkı sağlayabilir.

> Yakın zamanda yaşanan ihlallerin çoğu, isteyerek ya da bilmeyerek içeriden yardım alma konusunda uzmanlaşmış kötü niyetli kişiler tarafından gerçekleştirilmiştir.- David Clarke

Kimler risk altında?

> Kuruluşlar siber güvenlik tehditlerine karşı koymak için yeterince çaba göstermiyor. - David Clarke

Tedarik zinciri, kuruluşlar için bir başka olası güvenlik açığı noktasıdır ve tedarik zinciri saldırıları çok yaygındır. 2013 yılında ABD'li perakendeci Target, 40 milyondan fazla müşterinin banka ve kredi kartı bilgilerini ifşa olduğu, perakende tarihinin en büyük veri ihlallerinden birine maruz kalmıştır. Saldırıdan 6 ay önce kapsamlı bir siber güvenlik sistemi kurmuş olan Target'ın kendisi siber güvenlik konusunda oldukça ilgili olmasına rağmen, saldırganlar Target'ın üçüncü taraf tedarikçilerinden birine sızmış ve onlar aracılığıyla Target'ın ana veri ağına erişim sağlamışlardır. Sonuç olarak, Target aleyhine 90 dava açıldı ve şirket ihlal nedeniyle 61 milyon dolar kaybetti. Saldırıdan doğrudan sorumlu olmasalar da tedarik zincirlerinin siber güvenliğindeki bu zayıflık hem finansal hem de itibar açısından zarara neden olmak için yeterliydi.

Çalışanların güvenlik önlemlerini atlatma çözümleri de bir güvenlik açığı kaynağı olabilir. Bu atlatma çözümleri çalışanların günlük işlerinde daha verimli olmalarını sağlayabilirken, çoğu zaman parola yönetimi gibi temel güvenlik süreçleri ve en iyi uygulamalar göz ardı edilmektedir. NCSC ve CISA'nın verdiği yol gösterici bilgiler oldukça anlaşılır olsa da özellikle BT ve siber güvenlik konusunda az bilgi sahibi ekip üyeleri tarafından pratikte uygulanması genellikle daha zordur. Özel bir siber güvenlik ekibine sahip olmak kesinlikle yardımcı olabilirken, çalışanlara donanım şifrelemeli sürücüler gibi doğru araçları vermek, çalışanların geçici çözümlerinden kaynaklanan riskleri azaltmaya büyük katkı sağlayabilir.

> Günümüzde çeşitli arayüzlere (grafik, tuş takımı, dokunmatik ekran), geniş işletim sistemi desteğine ve her kuruluşun ihtiyaçlarını karşılayan kapasitelere sahip donanım şifrelemeli USB sürücülerin kullanıma alınması ve mevcut siber güvenlik politikalarına entegre edilmesi kolaydır. - Pasi Siukonen

Kuruluşlar siber saldırı riskini nasıl azaltabilir?

Kuruluş açısından bakıldığında, uç noktaların güvenliğini sağlamak ve verileri korumak için yapılabilecek bir çeşitli önlemler vardır. GRC (Governance, Risk, Compliance- Yönetişim, Risk, Uyumluluk) olmadan siber güvenliğin başarısız olması kaçınılmazdır. Bu nedenle süreçleri bilmek ve uygulamak işletmelerin kendilerini korumaları için son derece önemlidir. Sağlam bir uç nokta güvenlik yazılımı kullanmak, herhangi bir güvenlik açığını kapatma konusunda mümkün olduğunca hızlı tepkili olmanın yanı sıra bir dizi siber tehdidi de etkisiz hale getirebilir.

> **Zorunlu şifreleme politikalarını uygulamaya alıp almamak, risk yönetimi açısından verilerinizi yedeklemeyi seçip seçmemeniz kadar önemli, hatta belki de daha önemli bir sorudur. - Pasi Siukonen**

Ancak bireysel düzeyde, şifrelenmiş donanımlar siber güvenlik tehditlerine karşı kırılganlıkları büyük ölçüde azaltabilir. Uzaktan ve hibrit çalışmanın artışı ve kalıcılığının yanı sıra özellikle geçtiğimiz yıl siber saldırılardaki artışla birlikte kuruluşun her seviyesindeki çalışanların şirket verilerini güvenli bir şekilde kullanmasını, aktarmasını ve okumasını sağlamak her zamankinden daha önemli hale geliyor. Donanım şifrelemeli USB'ler, kullanıcıların flash belleklerin taşınabilirliğinden ve basitliğinden faydalanmaya devam etmelerini sağlarken, aynı zamanda bu cihazlarla ilişkili riskleri de büyük ölçüde azaltır. Yanlış bir yere konmuş veya çalınmış bir standart sürücü veri, para, itibar kaybı ve çok daha fazlasına neden olurken, donanım şifrelemeli sürücüler hassas verileri çok çeşitli saldırılara karşı korumak için tasarlanmıştır. Siber suçlular yeni saldırı yöntemleri geliştirdikçe, şifrelenmiş sürücüler de bu yeni zorlukların gereklerini karşılamak için gelişmeye devam edecektir.

Sonuç olarak, bir siber saldırıyla başa çıkmanın maliyeti çok yüksek olabilir. Gerçekten de, şifrelenmiş sürücülerin kurumsal düzeyde uygulamaya alınması ve kullanılması daha kapsamlı bir onay ve kurulum gerektirse de uzun vadede şirkete hem haraç maliyetleri hem de zedelenen itibar nedeniyle kaybedilen gelir açısından daha fazla para tasarrufu sağlayabilir. Bir ihlalin sadece yasal maliyetleri bile donanım şifrelemeli USB sürücülerin ek maliyetini kolayca karşılayabilir.

> **Mükemmel şifrelenmiş USB çözümleri sunma konusundaki uzun vadeli kararlılığı sayesinde Kingston'ın ürün portföyü, her kuruluşun siber güvenlik yapılandırmalarını karşılamasına olanak sağlamaktadır: endüstri standardı zorunlu donanım şifrelemesi, uç nokta politikasına uyumlu tasarımlar, cihaz yönetimi özellikleri. - Pasi Siukonen**

Özet

Kingston olarak her zaman siber güvenlik alanındaki gelişmeleri takip ediyor, IronKey şifrelemeli sürücülerimizin en son gereksinimlere uygun olmasını ve hem büyük hem de küçük kuruluşların siber güvenlik ihtiyaçlarını karşıladığından emin oluyoruz. Siber güvenlik tüm dünyada giderek artan bir sorun kaynağı olmaya devam ederken, kuruluşların kullanabilecekleri doğru araçlar ve bilgilerle kendilerini, çalışanlarını ve müşterilerini korurken bu zorlukların gereklerini yerine getirebilecek donanıma sahip olacaklarından eminiz.

Kingston hakkında

Kingston 35 yıllı aşkın deneyimi ile mobil veriyle ilgili zorluklarınızı belirlemek ve çözmek, bu sayede iş gücünüzün kuruluşunuzu tehlikeye atmadan güvenli biçimde çalışmasını kolaylaştıracak bilgiye sahiptir.

#KingstonIsWithYou

1. https://www.techtarget.com/searchsecurity/news/252516423/Sophos-66-of-organizations-hit-by-ransomware-in-2021