GDPR sonrası ortamda veri koruması ve siber güvenlik

#KingstonIsWithYou

GDPR sonrası ortamda veri koruması ve siber güvenlik

Önsöz

Sayısız şirket ve kuruluş GDPR'ye hazırlanmak için çok sıkı çalıştı ve personel sayısını artırdı. Belki siz de onlardan birisiniz. Yine de siber tehditlerin sürekli değişen yapısı nedeniyle bu çabalara ara veremezsiniz. GDPR ile uyum tek seferlik gerçekleştirilecek bir uygulama değildir. Aslında sizin devam etmekte olan veri koruması ve siber güvenlik çabalarınızı değerlendiren bir çerçeve çalışmasıdır. Rehavete kapılmamak gerekir.

Bu kısa e-Kitap'ta Birleşik Krallık'ın siber güvenlik konusunda en deneyimli yorumculardan bazılarını, GDPR'nin uygulanmaya başlamasından bu yana veri korumasının nasıl değiştiğini konuşmak üzere bir araya getirdik. Aynı zamanda şirketlerin çalışanlarını uyum gereksinimi hakkında nasıl eğittikleri ve IT departmanlarının ve teknoloji sağlayıcılarının, IT altyapısını yaklaşmakta olan güvenlik zorluklarına karşı nasıl daha iyi güçlendirebileceklerini ve son kullanıcıları nasıl eğitebileceklerini de ele alacağız.

GDPR sonrası ortamda veri koruması ve siber güvenlik

Katılımcılar

Bu kısa e-Kitap, veri koruması ve siber güvenlik konusunda uzman 5 kişi tarafından derlendi.

Rob Allen
@Rob_A_kingston

Rob, Kingston Technology'de Pazarlama ve Teknik Hizmetler Müdürüdür ve 1996 yılından bu yana şirkette çalışmaktadır. Rob, tüm Kingston markaları ve ürünleri için Halkla İlişkiler, Sosyal Medya ve Kanal Pazarlamanın yanı sıra Dijital Pazarlama Medyası ve Yaratıcılık'tan sorumludur.

Tara Taubman-Bassirian
@clarinette02

Tara birçok unvana sahiptir: hukukçu, avukat, arabulucu, araştırmacı, danışman, konuşmacı ve yazar. Gizlilik, fikri mülkiyet ve ver koruması gibi alanlarda müthiş deneyimi ile özellikle Birleşik Krallık, Fransa ve ABD olmak üzere dünyanın birçok yerinde şöhrete sahiptir.

Rafael Bloom
@rafibloom73

Salvatore ltd.'nin müdürüdür. Görevinde şirketlerin teknolojik ve yasal değişiklikler nedeniyle ortaya çıkan stratejik, ticari ve yöntemsel zorlukları ve fırsatları yönetmelerine yardımcı olmaktadır.

Miriam Brown
@Kingston_MBrown

Kingston Technology'de B2B Stratejik Pazarlama Müdürüdür ve 1997 yılından bu yana şirkette çalışmaktadır. Miriam, şirketteki görevinde tüm Kingston B2B ürünleri için pazarlama stratejisi, içerik ve kampanyalardan sorumludur.

Sally Eaves
@sallyeaves

Prof. Sally Eaves, ‘etik teknolojinin lideri' olarak tanımlanmaktadır. Yönetim Kurulu Başkanlığı ve Teknoloji Başkanlığı, Yaklaşan Teknolojiler Profesörlüğü ve Global Strateji Danışmanlığı alanlarındaki engin deneyimlere sahiptir. Sally, ödüllü bir uluslararası konuşmacı, araştırmacı ve kamuoyu oluşturucu ve alanında gerçekten kabul gören bir liderdir.

GDPR sonrası ortamda veri koruması ve siber güvenlik

İçindekiler

Bölüm 1 – GDPR'den bu yana veri koruması nasıl değişti?

Şirketler önemli yol kat etti. Geçtiğimiz iki yılda hukuk ekipleri genişletildi. İşe alınan Veri Koruma Görevlileri sayısında önemli artışlar oldu[1] ve dışarıdan veri gizliliği danışmanlarıyla yapılan konsültasyonlar arttı. Veri koruması etki değerlendirmelerinin (Data protection Impact Assessments - DPIA'lar) yapılması artık binlerce kuruluş açısından olağan hale geldi.

Ancak daha yapılması gereken çok şey var.

GDPR ile ilgili en büyük zorluklardan biri, gözünüzü toptan ayırmamanız gerekmesidir. Çoğu kuruluşta neredeyse personelin herhangi bir üyesi, herhangi bir zamanda kuralları ihlal edebilir. Sorun, sağlık, eğitim ve hukuk gibi iş gücünün geniş olduğu ya da yüksek düzeyde otonominin yer aldığı sektörlerde daha da büyüktür. Örneğin hukukta birçok avukat, hassas dava detaylarını basit bir e-posta eki ile göndermekten hiçbir şey olmayacağını düşünecektir. Sağlık uzmanları, hasta verilerini ya da bir MRI taramasının sonuçlarını, güvenli olmayan e-posta adreslerinden gönderip alacaktır. Stresin yüksek olduğu kuruluşlarda, uyum gereksinimlerinin göz ardı edilmesi için yapılacaklar listesinde biraz fazla baskı olması yeterli olacaktır. Üretkenlik, protokollerden daha önemli gibi görünecektir.

Bunun değişmesi gerekir.

Ayrıca hayır kurumları sektöründe farkındalıkla ilgili bir sorun vardır. Çoğu durumda hayır kurumları, GDPR'den muaf olduklarını düşünme eğilimindedir. GDPR'nin her türlü özel, kamu ya da üçüncü taraf sektör kuruluşları için geçerli olduğunu anlıyor olmalarına karşın, maddi kaynaklarını asıl amaçları yerine veri korumasına yatırmak konusunda, belki de anlaşılır şekilde çekinceli davranmaktadırlar.

Bu soylu bir davranış olmasına karşın aslında safça bir yaklaşımdır. GDPR'nin ihlal edilmesinden kaynaklanan olası cezalar, IT'ye yapılacak harcamalardan çok daha büyüktür.

Tara Taubman-Bassirian
@clarinette02

GDPR, Veri Koruması ve Fikri Mülkiyet Danışmanı

"Birçok üçüncü sektör kuruluşu: 'GDPR bizim için geçerli değil, biz sadece bir hayır kurumuyuz' diye düşünmektedir. Web siteleriyle ilgili uyumda bile onlara konunun toplanan veriler değil, ziyaretçilerinizin verilerine erişime izin verdiğiniz üçüncü şahıslar olduğunu anlatmaya çalışıyorum."

2016 yılından bu yana

Veri Koruma Görevlilerine (DPO - Data Protection Officer) olan talep fırladı ve %700'den fazla arttı.

1. Varonis: A Year in the Life of the GDPR: Must-Know Stats and Takeaways www.varonis.com/blog/gdpr-effect-review/ [accessed 11/26/2019]

GDPR'den bu yana veri koruması nasıl değişti?

Verilerin en aza indirilmesi cesaretlendirici bir trend

Verip toplamasının muazzam düzeyde olduğu bir çağda yaşıyoruz. "Büyük Dörtlü" (Google, Apple, Facebook ve Amazon), müşterileriyle ilgili çok miktarda veriyi ellerinde bulundurmaktadır. Diğer kuruluşların da Büyük Dörtlü'yü taklit edeceği ve mümkün olduğunca çok veri toplayacağını varsayabiliriz. Buna karşın ne kadar çok veriniz varsa o kadar çok riske maruz kalırsınız. GDPR'nin devreye girmesinden bu yana görülen en olumlu trendlerden biri de aşırı veri toplamasına karşı başkaldırıdır. Akıllı şirketler verilerin en aza indirilmesi için bir görüşe sahipler: ihtiyacınız yoksa veriyi almayın.

Tara Taubman-Bassirian
@clarinette02

GDPR, Veri Koruması ve Fikri Mülkiyet Danışmanı

"Verilerin en aza indirilmesi, GDPR'nin belki de en iyi ilkelerinden biridir. Her türlü veri tabanı oluşturma, risk oluşturma anlamına gelmektedir."

Rob Allen
@Rob_A_kingston

Pazarlama ve Teknik Hizmetler Müdür, Kingston Technology

"Verilerin silinmesiyle ilgili çok katı kurallarımız var. Evet, iş açısından kritik verilerin doğru biçimde saklanması gereklidir. Peki geri kalan veriler? Bir yıl sonra, işe yaramazlar. Saklamanın amacı nedir?"

Bu yaklaşımın avantajları, riskin sınırlandırılmasının ötesine geçmektedir. Örneğin pazarlamayı ele alın. Pazarlama veri tabanınız hijyenik değilse, işe yaramayan verileri saklıyor olabilirsiniz. Veri tabanınız on binlerce kişiye ulaştıysa ve sık sık e-posta kampanyaları yapıyorsanız, maliyetler artacaktır. Kampanyanızın performans istatistiklerini de bozacaktır.

Verilerin en aza indirilmesi fiziksel veriler için de geçerlidir. Bastıklarınıza (müşterilerinizin pasaport taramaları gibi) ve yazdıklarınıza (hesap parolaları gibi) dikkat edin. Ve eğer bir belgenin fiziksel kopyasını elinizde tutmanız gerekiyorsa, bunu güvenli biçimde saklayın. Masanızdaki kağıt yığını etkileyici gibi görünüyor olabilir. Ama hiç güvenli değil.

Rafael Bloom
@rafibloom73

Müdür, Salvatore Ltd

"Teknoloji ile işletmelerin aslında yaptıkları arasındaki arayüzde tamamen farklı bir düşünce şekline tanıklık ediyoruz. İşletme liderliğindeki bu dijital olgunluk seviyesinin hemen gerçekleşmesi gerekiyor."

İfşanın etkisi: Üst yöneticilerden tüketiciye

Bir düzenleyici konsept olarak veri koruması, onlarca yıldır uygulanıyor. Google[1], British Airways ve Marriott otel zinciri[2] dahil olmak üzere şirketlere şu zamana kadar kesilen büyük cezalar ve onların oluşturduğu medya kapsamı, üst yönetimlerin dikkatinin GDPR'ye toplanmasını sağladı. Bu durum, aşağıya doğru ilerleyen bir etki yarattı.

1. Varonis: A Year in the Life of the GDPR: Must-Know Stats and Takeaways www.varonis.com/blog/gdpr-effect-review/ [accessed 11/26/2019]
2. The Guardian: GDPR fines: where will BA and Marriott's £300m go? www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [accessed 11/26/2019]

GDPR'den bu yana veri koruması nasıl değişti?

Devam...

Güçlü veri korumasının benimsenmesinin arkasındaki bir diğer destekleyici güç de işbirlikçi çalışma sistemidir. Büyük işletmeler olası tedarikçilerin veri güvenliğinin sağlamlığına kapsamlı biçimde dikkat ediyorlar. Bunun nedeni, onlarla birlikte iş yapıyor olmaktan dolayı veri ihlallerinden sorumlu olmak istememeleridir.

GDPR'nin ticari olarak farkındalığının artmasının başka bir yönü daha var: tüketiciler kendi veri hakları konusunda daha da fazla farkındalığa sahipler. Aynı zamanda bir şirketin verilerinin kontrolünü kaybetmesi durumunda (not olarak bunun mutlaka bir ihlal olması gerekmiyor) tazminat alma hakkına sahip olduklarını biliyorlar. İşletmelerin konsantrasyonlarını korumaları gerekiyor.

Sally Eaves
@sallyeaves

CEO ve Müdür,
Sally Eaves Consultancy

"Veri koruması, işletmeler açısından güvenin kazanılabileceği ya da kaybedilebileceği bir zorunluluk haline geldi."

Bölüm 2 – Kuruluşlar çalışanlarını nasıl eğitiyor?

Personel eğitimi: iş gücünüzün gözlerini devirmesine neden olabilecek iki sözcük.

Eğitiminizin daha etkileyici olmasını sağlamanız için daha fazla neden. Eğitimli iş gücünün, veri koruması iyi uygulamalarını ihlal etme olasılığı daha azdır. Ayrıca bir veri ihlali varsa Bilgi Yetkilisinin Ofisi (ICO - Information Commissioner's Office) personelinizi veri güvenliği konusunda eğitmek için yeterli çabayı gösterdiğinizi kanıtlayabilirseniz sizin için daha olumlu karar verecektir.

Rafael Bloom
@rafibloom73

Müdür,
Salvatore

"Verileri, kaynağı ve tüm yaşam döngüsünün düzgün biçimde yönetilmesi gereken bir tedarik zinciri öğesi olarak görüyorum. Ekibinizi yarım saatliğine bir odaya alıp, lütfen malzemeleri parçalamayın, lütfen güvenli bir parola belirleyin gibi neler yapmaları gerektiğini anlatmak iyidir ve yararlı olacaktır. Tabi ki kuruluşunuzun riskini azalttınız. Ama sonra, çalışanları zorunlu tuttuğunuz ilk küçük etki dışında somut bir fark görülüyor mu? Hayır."

Ancak Nisan 2019'da, Dijital İşler Bakanı Margot James, Birleşik Krallık'ta personelini eğiten on kuruluştan üç tanesinin siber tehditlerle uğraşmak zorunda kaldığını belirtti[1]. Artık eğitimin ciddiye alınması gereken bir zamandayız.

Bu bir kültürün geliştirilmesidir, sadece onay kutularının işaretlenmesi eğitimi değildir

Eğitim, gerçek davranışları ve kültürel değişimi etkilemek üzerinedir. Sadece onay kutularının işaretlenmesini öğretmek değildir. Veri koruması hakkında herkesin doğru yanıtlayabileceği kolay soruların yer aldığı bir online eğitim paketi satın almak kolaydır. Ancak bu gerçekten kuruluşunuzun korunmasına yardımcı olacak mı?

İyi veri koruması davranışlarının iki temel malzemesi vardır. Birincisi, akıllı, etkileyici ve kuruluşunuzun kendine özgü zorluklarına yönelik tasarlanmış bir eğitim. İkincisi, GDPR'nin tüm çalışanları her gün etkileyen güçlü bir iş yeri kültürü sorusu olduğunu fark etmektir. Kuruluş içinde verilerle doğru işleri, doğru şekilde yapmaktır. Örneğin İK'yı ele alalım. E-posta sunucularında duran tüm kişisel çalışan adayı bilgilerini düşünün.
Veri koruması herkesin sorumluluğundadır.

1. Intelligent CISO: One year on, what has been the impact of GDPR on data security? www.intelligentciso.com/2019/04/16/one-year-on-what-has-been-the-impact-of-gdpr-on-data-security/ [accessed 11/26/2019]

Kuruluşlar çalışanlarını nasıl eğitiyor?

Verilerin arkasında bir kişi vardır

İlk bölümde tüketicilerin veri hakları hakkında daha fazla farkındalık geliştirdiklerini belirttik. Veri koruması eğitimini konumlandırmanın iyi bir yolu, personelinize verilerin arkasında her zaman bir kişi olduğu bağlantısını yapmalarına yardımcı olmaktır. Çalışanlarınızdan, verilerini verdikleri tüm kuruluşları düşünmelerini isteyin. Veri korumasının kişisel gizlilik ile ilgili olduğunu fark edeceklerdir.

Bir acil durum planına sahip olun

Sally Eaves
@sallyeaves

"Çalışanların veri güvenliği ve gizliliği konusunda sürekli eğitmek, işletmeler açısından bir zorunluluktur. Bunun tek seferlik, yılda bir kez yapılan bir eğitim oturumu değil, günlük iş deneyimlerinin bir parçası haline gelecek, proaktif, etkileşimli ve etkileyici bir deneyim olması gerekmektedir. Çalışanların, neleri önlemek, yönetmek ve savunmak istediğimizle ilgili bir iletişime katılması gerekmektedir."

Miriam Brown
@Kingston_MBrown

"Eğitim sırasında insanlara 'Bu sizin verileriniz olsaydı ne düşünürdünüz?' diye sormanın ilgi çekici olduğunu düşünüyorum. Bankamın yöneticisi, evde dizüstü bilgisayarından çalışıyor olsaydı ve o dizüstü bilgisayarda hassas bilgiler bulunuyor olsaydı, bunun şifrelenmiş bir sürücüde olmasını isterdim."

Rob Allen
@Rob_A_kingston

"Verilere, sanki sizinmiş gibi davranın."

Bölüm 3 – IT departmanları cihazların güvenliğini artırabilir mi?

Uzaktan çalışma artık yeni normal olarak kabul edilen bir olgu haline geldi

Personeliniz, büyük olasılıkla çalışma dünyalarına kolayca trende ya da takside unutulacak kişisel cihazlar dahil olmak üzere birçok farklı cihazdan erişiyordur. Sizin yapmanız gereken, personelinizin, sizi güvenlik riskleri ve veri ihlallerine açık duruma getirmeden verimli biçimde çalışmalarına yardımcı olmanın bir yolunu bulmaktır. Veri koruması ile ilgili çabalarınızın çökmesi için bir kişi yeterlidir.

Sally Eaves
@sallyeaves

CEO ve Müdür,
Sally Eaves Consultancy

"Verilerin taşınırken, sabitken ve kullanımdayken korunması gerekir. Tüm bu süreçler boyunca tam kapsamlı bir güvenlik, kurtarma ve veri silme planına sahip olmak kritik öneme sahiptir. Genellikle önemsiz gibi görülen, örneğin şifrelenmemiş USB'ler, şifrelenmemiş ekler gönderirken e-postaların kullanılması ve hassas kullanıcı verilerinin ifşa olmasına neden olacak web tarayıcı özellikleri gibi risk alanlarına dikkati çekmek çok önemlidir. Bu kadar çok cihazın bağlı olması ve çalışma düzenlerinin değişmesiyle bir cep telefonunda bulunan verilerin, şirketin sunucusunda saklanan veriler kadar güvenli olmasını sağlamak kritiktir."

İki faktörlü doğrulama

Ortalama bir kuruluş için yapabileceğiniz en iyi ve en kolay şey ağınızın etrafını korumaktır. Bu, parola yöneticileri ve iki faktörlü doğrulamaların kullanımı kadar basittir. İki faktörlü doğrulamaya iyi bir örnek olarak, kullanıcının dizüstü bilgisayarına parola girmesinin istenmesinin yanı sıra parola doğru biçimde girildikten sonra cep telefonlarına bir onay kodunun gönderilmesi gösterilebilir.

VPN'ler ve şifrelenmiş SSD'ler/USB'ler

VPN'ler, KOBİ'ler arasında giderek daha popüler hale geliyor. Bunlar özellikle iş verilerine halka açık WIFI ağlarından erişen personel için dikkat çekicidir. Ancak işletmelerin VPN'lerin yeteneklerini abartmamak için dikkatli olmaları gerekmektedir. Bunlar tam bir çözüm değil, çözümün bir parçasıdır. İşletmeler genellikle VPN'leri yalnızca donanım şifrelemesi olmayan dizüstü bilgisayarlar ya da laptop'lar kullanan uzaktan çalışanlar için uygulamaktadır. Neredeyse herkes dizüstü bilgisayarlarında dosyalar saklamaktadır. Cihaz bilgisayar korsanlarının saldırısına uğrarsa, kaybolursa ya da çalınırsa ne olacak? Şifrelenmiş USB'ler ve SSD'ler standart modellerde sadece çok daha az pahalıdır. Şifrelenmiş USB'ler kullanmak ve dizüstü bilgisayarınıza donanım şifrelemeli SSD'ler takmak, uzaktan çalışmanın zorluklarının üstesinden gelmede büyük bir etkiye sahiptir. Bir cihaz kaybolur ya da çalınırsa, kimsenin şifrelenmiş dosyalarınıza erişemeyeceğinden emin olabilirsiniz. Hatta kaybolan USB'leri uzaktan kullanılmaz hale getirebilirsiniz.

"Bir şirketin CEO'sunu iki faktörlü doğrulamanın uygulanması için ikna etmeye çalışan bir siber güvenlik uzmanı ile tanışmıştım. CEO bu öneriyi şiddetle reddetmiş: 'Hayır, bunu yapmayacağız, bu zorluk çıkaran bir uygulama, ekstra bir adım. İstemiyorum.' Kısa bir süre sonra 40.000£'luk bir sahtekarlığın kurbanı oldular."

Rafael Bloom
@rafibloom73

Müdür, Salvatore Ltd

"Sonuçta güvenlik farkındalığını geliştirmenin en iyi yöntemi, hem güvenli hem de üretken stratejiler bulmak için çalışanlarla görüşmektir."

Rob Allen
@Rob_A_kingston

Pazarlama ve Teknik Hizmetler Müdür,
Kingston Technology

IT departmanları cihazların güvenliğini artırabilir mi?

Özel sunucular ve MSP'ler

Her geçen gün daha fazla sayıda büyük kuruluş, sunucularını kendi tesislerine yerleştirmeye geçiyorlar. Bu şekilde sunucuları üzerinde tam kontrole sahip olmayı ve hiçbir bilginin buluttan erişilebilir durumda olmamasını sağlamak istiyorlar. Daha sonra hassas olmayan verilerin bulutta ancak kişisel verilerin tesiste bulunduğu hibrit sunucu çözümleri de var. KOBİ'ler ve üçüncü sektördeki kuruluşların kendi sunucularına sahip olmaları yüksek maliyetli olabilir. İşte bu noktada yönetimli hizmet sağlayıcıları ve sanal özel sunucular devreye giriyor. Bunlar işletme giderlerinizi önemli ölçüde artırmadan güvenliğe daha fazla odaklanılmasını sağlıyor.

Süresi dolan verilerin otomatik belirtilmesi

GDPR'nin ilkelerinden biri, eski verilerin silinmesidir. Örneğin belirli türlerdeki kişisel verilerin yedi yıldan daha uzun süre saklanmaması gerekiyor. Verinin 'süresinin dolması' yaklaştığında size otomatik olarak bildirilse nasıl olur? Doğru veri tabanı ile IT ekibinin verilerin saklanma süresinin sonuna yaklaştığında DPO'ya otomatik olarak oluşturulan bir posta gönderecek bir eylem oluşturması kolay olacaktır.

Doğru sağlayıcılarla çalışın

Konu IT güvenliği olduğunda sayısız üretici ve sağlayıcı bulunuyor. Araştırmanızı yapın. Sizin endüstrinizde ya da sektörünüzdeki kuruluşlara benzer hizmeti sunmada belirli bir deneyime sahip güvenilir bir sağlayıcıdan gelen bir sisteme sahip olmak önemlidir. Seçtiğiniz sağlayıcı ya da sağlayıcıların sadece teknolojiye sahip olmadığından, aynı zamanda veri güvenliğinin uygulanmaya alınmasındaki zorlukları anladığından emin olun.

Bölüm 4 – Teknoloji sağlayıcıları süreçleri ve anlayışları nasıl iyileştirebilir?

DPO için TLC

2016 yılından bu yana Veri Koruma Görevlilerine (DPO - Data Protection Officer) olan talep fırladı ve %700'den fazla arttı.[1] Şu anda Avrupa'da 500.000'den fazla DPO çalışıyor. Bu değer 2017'de öngörülenden altı kat daha fazla.[2] Yine de DPO'nun görevinin önemi genellikle göz ardı ediliyor ve değersizleştiriliyor.

Bir DPO şirketinizin güvenlik ve veri gizliliği alanında tam görünürlüğe ihtiyaç duyar. Bu, tam zamanlı bir iştir. Buna karşın bazı kuruluşlarda 'DPO', teknolojiden en iyi anlayan bir personele verilen basit bir etiketten oluşuyor. DPO'lar normal günlük işlerindeki standart görevlerini gerçekleştirirken aynı zamanda şirketin tümünün veri gizliliğinden sorumludur.

Gerçekte bu yeni nesil DPO'ları desteklemek için çeşitli profesyonel hizmetlerin ve araçların var olması gerekiyor. Tam zamanlı bir DPO'nuz olmasa bile veri güvenliği çok hızlı hareket ediyor ve her zaman ikinci bir görüş gerektiren zorluklar olacaktır. Dışarıdan bir veri güvenliği danışmanı ile birlikte çalışmak etkili olabilir ancak kuruluşunuz içinde bu tür tüm işleri düzgün duruma getirmeniz gerekiyor.

Açıklık, acil durum ve uyum

IT alt yapınız yalnızca en zayıf halkası kadar güçlüdür. İşte bu nedenle IT ekosisteminize eklenecek her türlü öğe için teknoloji ağlayıcınızın, olası güvenlik tehditleri hakkında tam açıklık ve yeni ürününüzün güvenli biçimde nasıl kullanılacağıyla ilgili açık öneriler sağlaması gerekiyor.

Tara Taubman-Bassirian
@clarinette02

GDPR, Veri Koruması ve Fikri Mülkiyet Danışmanı

"Her yere CCTV kameraları takan insanlara, genellikle parolasız olarak kurulduklarından bunun mutlaka güvenlik olmadığını anlatmaya çalışıyorum. Dolayısıyla sadece bir web sitesine giriş yapabilir, arkanıza yaslanıp izleyebilirsiniz. Aslında hırsızlara şunu söylüyorsunuz: 'gel ve benim olmadığım zamanlara bak!"

1. Varonis: A Year in the Life of the GDPR: Must-Know Stats and Takeaways www.varonis.com/blog/gdpr-effect-review/ [accessed 11/26/2019]
2. The Guardian: GDPR fines: where will BA and Marriott's £300m go? www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [accessed 11/26/2019]

Teknoloji sağlayıcıları süreçleri ve anlayışları nasıl iyileştirebilir?

Acil durumda önemli hususlardan biri. Bir ürün kullanım ömrünün sonuna geldiğinde ya da güncelleme gerektirdiğinde ne olur? Teknoloji sağlayıcıları, yanlışlıkla içindeki verileri tehlikeye atmadan ya da daha geniş IT ekosisteminizi ifşa etmeden ürünleriyle ilgili acil durum önerileri sağlamalıdır. Örneğin bir MRI tarayıcıyı düşünün. Hasta görüntülerinin saklanması için dört terabayt şifrelenmiş bir SSD'ye sahip olabilir. Peki veri saklama alanı dolduğunda ne olur?

Teknoloji sağlayıcıları ve kuruluşların kendisi, hem kuruluş içinde hem de dışarıdan tedarikçiler ve iş ortaklarıyla çalışırken dijital uyum ve veri uyumunun yer aldığı bir ortam sağlamalıdır. Bu durum özellikle NHS gibi çok yönlü, çok bölümlü ve çok konumlu kuruluşlar açısından hayatidir.

Miriam Brown
@Kingston_MBrown

Kingston Technology'de B2B Stratejik Pazarlama Müdürü

"NHS'e çok sayıda ürün sattık. Ancak hangi veri koruması politikaları ve protokollerini uyguladıklarını sorduğumuzda her biri arasında güven açısından bariz farklar var."

Ufuk taraması

Teknoloji, bazen güvenlikten daha hızlı hareket ediyor. Çin'de yüz tanıma ile ödeme gibi yeni teknolojilerde kuruluşlar bazen, olası güvenlik ve veri koruma etkilerini düşünmeden çıkan teknolojiyi almak için yarışa girebiliyor. Bir ya da iki yıl içinde 5G ağların yaygınlaşmasıyla, Sınır Bilişim (Edge Computing) ve dağıtık veri siloları gerçeğe dönüşecek. Teknoloji sağlayıcılarının kuruluşlara kendi veri bütünlüklerini ya da IT güvenliğini tehlikeye atmadan yaklaşmakta olan teknolojilerden güvenli biçimde yararlanmalarına yardımcı olabilmelidir.

Sally Eaves
@sallyeaves

CEO ve Müdür,
Sally Eaves Consultancy

"GDPR'de, uygulama sancılarının azaltılmasından gelişmiş IT süreçleri, yedekleme ve kurtarma ve gelişmiş güvenlik gibi kazançların artırılmasına odaklanmaya ve bunları endüstrideki benzerlerine göre fark yaratma noktası olarak kullanmaya doğru bir değişim görmeye başlayacağımıza inanıyorum."

Özet

GDPR, üst yönetimlerin ve tüketicilerin has veri gizliliği ve ağ güvenliğine dikkat etmesini sağlayarak işletmeleri daha iyi bir duruma getirdi. Ancak uyum, tüm iş gücünüzde her gün veri güvenliğine sürekli dikkat edilmesini gerektiriyor. Teknolojinin ve siber tehditlerin sürekli değişen yapısı, iyi güvenlik alt yapısı, iyi eğitim ve bunun arkasında teknoloji ve veri gizliliği ile ilgili iyi danışmanlık desteğinin, iş açısından çok önemli olduğunu gösteriyor. Personele verilerin arkasında her zaman bir insan olduğunu hatırlatmak, iş gücünüzde bir veri koruma kültürünün yerleştirilmesinde önemli bir adımdır. Ayrıca kültürel değişim, sadece onay kutularının işaretlenmesine yönelik eğitim egzersizlerinden çok daha etkilidir.

Kingston hakkında

Kingston 32 yıllık deneyimi ile uzaktan çalışmadaki zorluklarınızı belirlemek ve çözmek, bu sayede iş gücünüzün kuruluşunuzu tehlikeye atmadan istediği yerden güvenli biçimde çalışmasını kolaylaştıracak bilgiye sahiptir.

#KingstonIsWithYou