IOT GÜVENLİĞİ:

Daha güvenli bağlanmış bir ofis için 4 adım

Canon

İçindekiler

> Benim için, Nesnelerin İnterneti ile ilgili en büyük risk, güvenliktir. Bu cihazları alan insanlardan, benim bilgilerimi almalarından ya da cihazların fiilen yanlış bir şey yapmalarına neden olmalarından, endişeleniyorum.
>
> Dan Kaufman, Gelişmiş Teknoloji ve Ürünler Şefi, Google

Nesnelerin İnterneti (IoT), büyük veri ve siber suç, son zamanlarda birçok haberin odak noktası olmuş olsa da, bilgi ve veri güvenliği konuları artık çok daha çeşitli ve karmaşık hale geldi. Bu karmaşıklığa, yeni ve çok daha sıkı yönetmelik ortamı da katkıda bulunuyor.

Bu haberlerin bir çoğu tüketici IoT'nin tehlikelerine odaklandı. Gerçekten de, hemen hemen her gün, yanlış yapılandırılmış bir tüketici donanımının yol açtığı bir veri ihlali veya veri ifşası haberi çıkıyor. Kurumsal kullanıcıların birçoğu, aynı sorunların ofislerde de yaşandığının farkında değil. İnsanlar bebek izleyici cihazlarının veya kablosuz kapı zillerinin, üçüncü kişiler tarafından internet üzerinden korsan saldırısına uğrayabileceğinin farkındalar; ancak ofis yazıcıları da aynı tehlikede. Cihazları güncelleştirmenin ve güvenli tutmanın önemi anlaşılıyorsa da, ofis donanımının güvenli tutulması ile ilgili mesajın daha dikkatle dinlenilmesi gerekiyor.

Bu sorun niçin var? Yanıt kısmen, ofis cihazlarının, büyük miktarda kurumsal veri içerme ve ağa bağlı olma nedenleriyle birer "IoT" olduklarının iyi anlaşılmamasıdır. Bir bebek monitörü veya internete bağlı bir buzdolabı, yabancıların yaşamınıza göz atmalarına yol açabiliyorlarsa, yanlış yapılandırılmış ofis IoT'leri de kurumsal verilerinizi açığa çıkartabilir ve saldırganların şirket güvenliğinizi ihlal etmelerine neden olabilir.

Ortalama ofislerdeki güvenlik sistemlerini ihlal etmeye niyetli kişiler, artık daha gelişmiş yöntemler kullanıyorlar, fakat aynı zamanda, bazı temel taktiklerin de etkili olduğunu gözlemliyorlar. Dış tehditler dikkate alınmalı fakat içteki aksiliklerin ve bilinçli sabotajların da yaratabileceği riskler unutulmamalıdır.

Dijital dönüşümün, işletmelerde ve yönetim kurullarında en çok konuşulan eğilim olmasının süregelmesine rağmen, organizasyonların çoğu hala kağıtlara basmaya bel bağlamaktalar. Böyle bir ortamda, maliyeti, karmaşıklığı ve korumayı dengelemek zor, ve bu zorluk sürmekte.

Genelde benimsenen standartlar olan yangın duvarları, anti virüs yazılımları ve spam filtreleri düzenlemek tek başlarına çoğunlukla yetersizdir. Etkin bir ofis güvenliği sağlam politikalar, çok katmanlı ve entegre güvenlik çözümleri gerektirir. Ayrıca çalışanlar da, verileri güvende tutmak için gereken en basit yöntemleri de sürekli uygulamalıdırlar.

Şimdi, IoT olarak bağlı ofislerin karşı karşıya oldukları güvenlik zorluklarının nasıl aşılabileceğini görmenin zamanıdır.

Bu ısmarlanmış rapor, günümüzün güvenlik ortamını inceler ve organizasyonların ofis güvenliğini artırmak ve yarınlarını korumak için atmaları gereken dört adımı özetler.

Belgelerin %42'sinin hassas bilgiler içermesine rağmen, katılımcıların yaklaşık yarısı belgelerini şirket sistemleri dışında da paylaşıyorlar.

GÜNÜMÜZDE OFİS GÜVENLİĞİ

Son zamanlarda, tekil iş alanlarının hiçbirine güvenlik kadar odaklanılmıyor ve yatırım yapılmıyor. Hızla evrilen iş yerleri, iş güçleri ve dijital dönüşümün yarattığı risklerle karşı karşıya kalan sayısız işletme, bulut sistemlerinin akımı, mobilite, Herşeyin İnterneti (IoE) ve sosyal medyanın etkileriyle çalışma yöntemlerini dönüştürmek zorunda kaldı. Ancak, bütün bu yenilikler saldırı alanının da genişlemesine neden oldu.

2016'da şirketlerin %32'si siber suç kurbanı oldu

2016 Küresel Ekonomik Suç Araştırmasına göre[1], şirketlerin %32'si 2016'da siber suç kurbanı oldular. Bu pek şaşırtıcı değil zira, en son yapılan Harvey Nash/KPMG CIO Araştırmasının[2] ortaya çıkardığına göre, beş Bilgi Teknolojileri Müdüründen (CIO) sadece biri, bir siber güvenlik saldırısını "çok iyi" savuşturduklarına inanmaktadır.

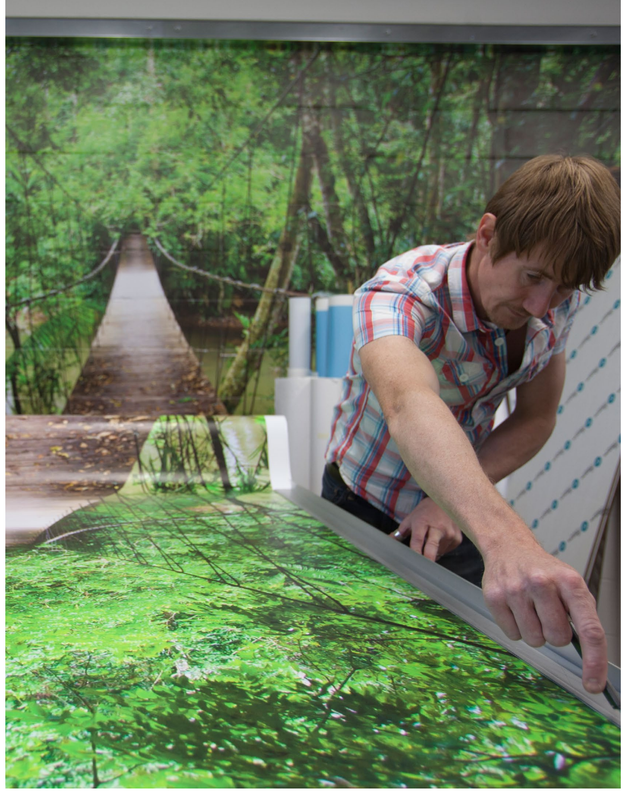
Veri kaybeden veya çaldıran işletmeleri ciddi sonuçlar bekliyor. Uğranılan zarar, yasal cezalar veya itibar kaybı da olsa, üst düzey yöneticilerin %80'inin belge güvenlik sistemlerini 1-2 yıl içinde yükseltmeyi düşünmeleri şaşırtıcı değil.

İşletmeler, güvenlik tehditleri hacminin büyümesi ve çeşitlenmesiyle başa çıkmaya çalışıyorlar. Korsanların neden olduğu tehditler ve kötücül ve gelişmiş virüsler ile ilgili abartılı haber bombardımanları, ateşe körükle gidiyor. Bu tehlikeli bir bileşim ve tehditlerin farkedilmediği ve kontrol edilmediği korkuları ile işletmenin güvenlik ekiplerinin dikkatleri dağılıyor. Sonuç, bir çok örnek olayda, güvenlik açıklarının günlerce, haftalarca veya aylarca kapanamamaları oluyor.

Bilgi güvenliği yönetimi bilgisayarlara ve çevrimiçi süreçlere odaklanma eğilimi gösterse de, değerli bilgilerin ofisin her yerinde bulunduğunu unutmamak önemlidir. Çalışanların belgeler ve sistemlerle iletişim kurdukları yer, kurumsal güvenliğin en geçirgen yeridir.

Örneğin, yazıcılar gibi ofis cihazları, doğru bir şekilde yönetilmiyorlarsa, modern ofislerin en kolay hedefleri olurlar. Bu cihazların işletme güvenliği için kritik bir zayıf nokta oldukları giderek anlaşılıyor.

1. http://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html
2. http://www.telegraph.co.uk/business/open-economy/it-security-vs-innovation-debate/



IOT - ya yazıcınız bir güvenlik zayıf notası ise?

1

Belge hırsızlığı ve gözetlenmesi:
Herhangi birinin, yazıcıdan başkasına ait bir belgeyi almasını önlemek için, baskı ve tarama yönetimi yazılımının, gizli belgelerin yayınlanmasını etkin bir şekilde kontrol ettiğinden emin olun.

2

Ayarların yetkisiz olarak değiştirilmeleri:
Yazıcı ayarlarınız ve kumandalarınız güvenli değilse, herhangi biri, yanlışlıkla veya kasıtlı olarak, baskı işlerini değiştirebilir ve tekrar yönlendirebilir, kaydedilmiş belgelerin kopyalarını açabilir, yazıcıyı fabrika ayarlarına döndürebilir veya ayarlarınızın tümünü silebilir. Bu da güvenlik açığını büyütmenin yanında, size zaman kaybettirebilir.

3

Dahili depolama:
Yazıcınızın bir dahili disk sürücüsü varsa, baskı işlerini, taramaları, belge kopyalarını ve faksları depolayabilir. Yazıcının, satılma gibi yasal iş nedenleriyle veya çalınma durumunda eski haline getirilmesi gerekiyorsa, kaydedilmiş belgeler kurtarılabilir.

4

Ağ yazıcı trafiğini gizli izleme:
Korsanlar ağ trafiğini gizlece izleyebilirler ve doğru bir şekilde şifrelenmemiş belgeleri yakalayabilirler.

5

Yazıcıya saldırı:
Parola korumalı olmayan veya güvenlik özellikleri bulunmayan eski yazıcı modellerinde, cihaza korsan giriş yapmak çok kolaydır. Modern çok işlevli cihazlar, basit yazıcılar veya fotokopi cihazlarından daha gelişmiştir. Aynı zamanda birer tarayıcı ve gelişmiş iletişim merkezleri olduklarından, yetkisiz kullanıcılara gizli belgeleri taratıp bir başka kişiye fakslama fırsatı tanımaktadırlar.

GÜVENLİĞİN KÖR NOKTASI

Yürürlüğe girecek olan Genel Veri Koruma Yönetmeliği (GDPR), yürürlüğe girerek, evrilmekte olan güvenlik ortamını etkileyen son yasa. GPDR nedeniyle, işletmelerin tümünün çalışma yöntemlerinde iyileştirmeler düşünmeleri gerekecektir. Bu, veri güvenlik sistemlerinin ve yöntemlerinin sağlamlığını tekrar incelemelerini de kapsayacaktır. İncelenecekler arasında, daha iyi kullanıcı kimlik doğrulamaları, veriler ve belgelerin ağlarda ve ağların dışında olan hareketlerinin kaydedilmeleri ve izlenmeleri bulunmaktadır. Ayrıca, veri dönüştürme, kataloglama, raporlama vb. gibi GDPR'ın özel gerekliliklerini karşılamak için yeni teknolojiler gerekecektir.

2017'de veri ihlallerinin ortalama maliyeti 3,07 milyon Avro oldu

Veri koruma gerekliliklerine bakıldığında, uyumluluk için artık yangın duvarları, anti virüs yazılımları gibi iyi bilinen güvenlik çözümlerine odaklanmanın yeterli olmayacağı açıktır. Dizüstü bilgisayarlar, akıllı telefonlar, ve diğer uç nokta cihazların da güvenlik gerektirdiği anlaşılmışken, çok işlevli yazıcılar (MFP'ler) gibi çevre birimlerinin güvenlik tehditleri için potansiyel giriş noktası olabilmeleri yeteri kadar ele alınmıyor.

Yeni yönetmelikle altında, veri ihlali olasılığı dörtte bir[3] kadar yüksektir. Bu da, organizasyonların risklerini ve bu risklerin etkilerini anlamalarını gerektiriyor. Daha da önemlisi, hangi öğelerin etkiyi azaltıp artırabileceğini ve veri ihlalinin maliyetlerini de anlamalıdırlar. Ponemon Enstitüsünün "2017 Veri İhlali Maliyet Çalışması", 2017'de veri ihlallerinin ortama maliyetinin 3,62 milyon Dolar / 3.07 milyon Avro olduğunu saptamıştır[4]. Bu da organizasyonları çoğu için hatırı sayılır bir meblağdır.

İhlallerin neden olduğu potansiyel kayıplar bu kadar ciddi olunca, Canon'un Ofis İçgörüleri 2017 araştırmasına katılanların %50'sinin, çalışanlarının gizli belgeleri yazıcıda veya fotokopi cihazında bırakmalarından endişe duymaları pek de şaşırtmıyor. İşletmeler, akıllı telefonları, dizüstü bilgisayarları ve kurumsal ağlarını korumak için birçok önlem alıyor olsalar da, yazıcılar güvenlik zincirindeki eksik halka olmayı sürdürüyorlar. Ancak, yasa düzenleyicileri ve müşteriler, güvenlik açıklarını gelişmişliklerine göre farklılaştırmıyorlar.

Fakat tehdit gerçek. EMEA genelindeki yönetim düzeyindeki çalışanların hemen hemen yarısı (%47), organizasyonlarında belge kayıplarının farkında. Ayrıca, bu yöneticilerin %46'sı da, çalışanların şirket dışındayken belge kaybettiklerini belirtti. Belgelerin %42'sinin hassas bilgiler içermesi, bu kayıpların ciddi sonuçlar doğurabileceği anlamına geliyor.

MFP'lerin çoğu, baskı verilerini bir önbellekte elektronik olarak depolarlar. Sıkı güvenlik önlemleri alınmamışsa, korsanlar cihaz içindeki hassas kişisel veya kurumsal verilere erişme fırsatını yakalarlar. Güvenlik önlemleri alınmamış bir MFP, aynı zamanda, kararlı bir korsanın, görünmez bir "arka kapı" yoluyla, cihazların tümünün bağlı olduğu kurumsal ağa erişebilmesini sağlar.

3. https://www.ibm.com/security/data-breach
4. https://www.ibm.com/security/data-breach

MOBİL GÜVENLİK

Çalışanların belge ve verilere erişmek ve paylaşmak için kullandıkları cihazlar sadece yazıcılar ve bilgisayarlar değildir. Şirket dışında, akıllı telefonlar ve dizüstü bilgisayarlarla hareket halindeyken, yani mobil çalışma, uygulamaların ve verilerin, güvenli veya güvensiz, birçok ağa ulaşabilmelerini sağlıyor ve bu cihazları ciddi risklere sokuyor.

Mobil cihazlarla donatılmış esnek bir iş gücü verimlilik ve üretkenliğin gelişmesini de getirir, ancak aynı zamanda, bilginin "geleneksel" ofis ortamının dışına yayılmasına neden olur. Bu, işletmelerin, yöneticilerin ve BT departmanlarının karşılaştığı zorluktur.

Bu cihazlar, nihayetinde, sayısız üretkenlik aracı, kaynak ve sosyal etkileşim fırsatlarına açılan kapılardır. Kurumsal ağ faaliyetlerinin %50'sinden fazlası mobil cihazlardan gelmektedir ve bu sayının azalması değil artması beklenmektedir[5]. Mobil cihazlar çalışanların rüyasıdır fakat aynı nedenlerle, bir BT güvenliği ve yönetim karabasanına dönüşebilirler.

> Skycure'a göre, organizasyonların %21'i veri ihlali olayının 'Kendi Cihazını Getir' (BYOD) programından kaynaklandığını keşfetti[6].

Korsanlar tarafından mobil cihazların hedeflendiği kötü niyetli programların sayısı katlanarak artmaktadır, ve mobilleri hedef alan kötü amaçlı yazılımlar gittikçe daha da gelişiyorlar.

5. https://www.forbes.com/sites/danwoods/2016/11/18/does-your-company-need-a-mobile-security-solution/#735e431e38bb
6. https://www.skycure.com/blog/1-in-5-organizations-experience-data-breach-via-byod-2016-spotlight-report/

> Teknolojik yenilikler arttıkça risklerimiz daha da büyüyor. Özellikle iş gücümüzün performansını yükseltmek için mobil teknolojilere aktif olarak yatırım yapıyoruz. Ancak, bu cihazların ve onlara depoladığımız verilerin organizasyonun genel güvenliğini nasıl etkileyeceğinin bilincine giderek daha çok varıyoruz.
>
> Kıdemli müdür, işletme danışmanlık şirketi, Fransa

Taşınabilirlik, mobil cihazların kaybedilmesini ve çalınmasını kolaylaştırıyor; kapasiteleri işletme bilgilerini riske atıyor ve bağlanabilirlik, BT sistemlerini ve verileri yetkisiz izleme ve erişime açıyor.

BYOD'nin bu risklere rağmen benimsenmesi, çalışanların ana bilgisayar ve uygulama tabanlı mobil erişim stratejileri kullanarak birlikte çalışmalarını ve memnuniyetlerini iyileştiriyor, fakat bu gelişme kurumsal güvenlik konusunun daha da karmaşık olmasına neden oluyor.

Canon'un Ofis İçgörüleri araştırması kapsamında, Avrupa'daki organizasyonların karar vericileri ile yüz yüze konuştuk ve onların şimdiki güvenlik ortamı hakkındaki düşüncelerini dinledik. Ayrıca, bu yeni güvenlik ortamına ve değişen zorluklarına nasıl uyum gösterdiklerini sorduk.

> İşletmemizdeki belgeler gizli bilgiler içeriyor ve her gün kullanılıyorlar. Bu bilgileri korumak için yapılacak yatırım bir öncelik. Ancak, acil güvenlik endişelerimiz, belge yönetimine yapmayı planladığımız yatırımın sadece bir kısmının nedeni. Gelecek olan GDPR'ı da inceliyoruz ve hem fiziksel hem de dijital bilgilerimizin mümkün olduğu kadar güvenli olmasına çalışıyoruz. Bu yasa belgelerimizi nasıl depolayacağımızı etkileyecek ve biz hazır olmak zorundayız."
>
> IT Müdürü, eğitim enstitüsü, İspanya

OFİS ORTAMINDA BİLGİ GÜVENLİĞİ YÖNETİMİ

Bilgi hiç bir zaman bu kadar değerli veya bu kadar yaygın olmamıştı. Bilginin hacmi ve değeri arttıkça çevreleyen riskler de artıyor.

İşletmenin hem iç ve hem dış zorlukları için geliştirilen yenilikçi teknoloji çözümleri, dijitalleştirilmiş bilginin hemen hemen canlı bir yayın olmasını gerektirdiğinden, Ofis İçgörüleri 2017 araştırmasına katılanların %77'sinin kağıt belgeleri dijital ve düzenlenebilir belgelere dönüştüren sistemlerin kritik veya önemli olduğunu ifade etmeleri pek şaşırtıcı değil.

İşletmede şimdiye kadarkinden çok daha fazla gizli bilgi hareket ediyor. Bu hareket, internete bağlı bir altyapı, kişiler, süreçler ve cihazlardan oluşan ve genişleyen bir ekosistem genelinde oluyor. Buna ek olarak, dizüstü bilgisayarlar, tabletler, mobil telefonlar ve diğer kablosuz cihazların kurumsal ağa bağlanmaları, olası korsanlara ek saldırı patikaları yaratıyor.

Organizasyonlar, kötücül yazılımları yenmek için daha etkin stratejiler benimseseler de, bu kez saldırganlar yaklaşımlarını değiştireceklerdir. Yasal kimlikler ve yazılımlar kullanarak 'fiziksel olarak içerde' gibi davranacaklardır. Yazıcılar gibi cihazların güvenlik zayıflıkları, kötü amaçlı kişilere bu açıklardan faydalanma fırsatı veriyor. Bu da, eski yazıcı kütükleri gibi hassas bilgiler içerebilen birçok alana yetkisiz erişim anlamına gelir. Buna ek olarak, bu açıklar, korsanların ağdaki bir cihazı yerleşme noktası olarak kullanıp organizasyonun içinde yanal hareket ederek bilgi toplamalarında kullanılabilir.

Katılımcıların %77'si kağıt belgeleri dijitale dönüştüren sistemlerin kritik veya önemli olduğunu söyledi

MFP'lerin bir çoğu, baskı, fotokopi, tarama, gönderme ve faks işlevleri sağlar ve böylece dijital ve fiziksel bilgi sınırları arasında köprü kurar.

MFP'ler, PC ve sunucular gibi bir ağ üzerinde çalışırlar, internete bağlanabilirler ve sabit disklere veri kaydedebilirler. Organizasyonlar bu cihazları altyapılarına ekledikleri zaman, bazı alanların işletmenin genel güvenlik stratejisinin bir parçası olarak ele alınmaları gerekir. Burada dikkat edilmesi gerekenler gizlilik ile işletmenin ağ sistemlerinin bütünlüğü ve işlerliğidir.

Sağlam ofis güvenlik politikaları ve önlemlerini uygulamaya koymuş olmak, kişisel ve mali veriler ile işletmenin fikri mülkiyetlerini korumanın sadece bir parçasını oluşturur. Etkin bir bilgi güvenliği yönetimi için, potansiyel riskler ve sakınılması gereken yöntemler organizasyonun bütünü tarafından anlaşılmalıdır.

DAHA GÜVENLİ BAĞLANMIŞ BİR OFİS İÇİN 4 ADIM - NELER YAPABİLİRSİNİZ?

Ofislerin çehresi değişmeye devam ediyor ve buna ayak uydurmak en ilerici organizasyonlar için bile zor olabilir. Bağlanmış ofis ortamınızın risklerini ve sorunları nasıl ele alıp nasıl çözebileceğinizi değerlendirmek için dört adımlı bir yaklaşım öneriyoruz:

Adım bir: Denetleyin ve değerlendirin

Belgelerin hepsi hassas bilgi içermez; yapacağınız tüm değişikliklerde, harcama veya aksamaları en aza indirgemek için, hassas olanlarına odaklanmalısınız. Değerlendirmeyi planlayarak, belge güvenliğinizdeki fiziksel ve dijital açıkları tanımlayabilir ve en büyük riski taşıyanlara öncelik verebilirsiniz.

Bunları sorun: Şu anda hangi kontrolleri uyguluyorsunuz? Kimler, hangi belge tiplerine ve nasıl erişiyorlar? Ne tür belgeler kullanıyorsunuz ve hangilerinden sorumlusunuz? Belge hassasiyetinin değişik düzeyleri nelerdir?

Adım iki: Ortamı koruyun

Baskı cihazlarınızın bağlı olduğu ağın güvenli olduğundan emin olun; bu cihazları kapsayan bir ağ sağlık kontrolü, kapanmaları gerekecek açıkları tanımlayabilir. Yazıcılarınızın ağın neresine yerleştirilmiş olduklarına bakın. Fiziksel olarak mı, kablosuz mu bağlılar? Kablosuz Yerel Alan Ağları (WLAN'lar), yetkisiz erişimlere genelde en açık bağlantılardır ve kablosuz bağlanmış cihazları ve onlara gönderilen verilerin korumasız olmalarına neden olur. Üçüncü taraf bir tedarikçi kullanıyorsanız, bunu incelemelerini isteyin.

Bunları sorun: Organizasyonunuz cihazları geniş ağınızla nasıl entegre ediyor ve baskı ortamındaki verileri kimlik denetimi yoluyla nasıl koruyorsunuz?

Adım üç: Cihazlar ve baskı sistemlerine akıllıca yaklaşın

Hangi baskı cihazlarını ve hangi yönetilen baskı hizmetlerini kullanacağınıza karar verirken, güvenlik politikalarınızla ve kimlik denetimi yaklaşımlarınızla uyumlu teknolojiler seçin. Ayrıca, ne türlü bir kimlik denetimi uygulaması kullandığınızı ve hangi ek denetimleri eklemek isteyebileceğinizi düşünmek de faydalıdır. Örneğin, mali belge baskıları yapılan bir yazıcı için ek güvenlik tavsiye edilir mi? Bu cihazlar veya sistemler o tür bir kimlik denetimini destekliyorlar mı? Baskı süreci boyunca alınan ve gönderilen verileri korumaya yönelik sektör standartlarını karşılayan cihazlar arayın. Ayrıca, çok işlevli cihazların, bağımsız yazıcıların ve tarayıcıların 'tarama kilidi' ve 'beni izle' özelliklerini de düşünün. Bunlar taranmakta olan veya yazıcıda unutulan hassas bilgilerin riskini azaltacaktır.

Bunları sorun: İşletme, cihazları kimin kullandığını ve hangi belgelere eriştiklerini ve hangi belgeleri ürettiklerini saptayabiliyor mu?

Adım dört: Korunma için bir politika benimseyin

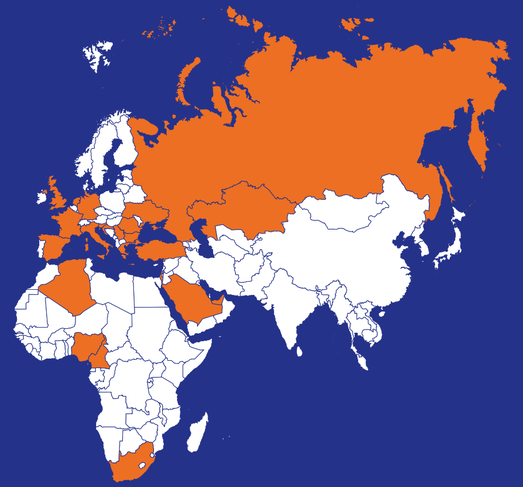
Elinizdeki belge ve veri yönetimi politikalarını gözden geçirin, güncelleyin ve çalışanların bu politikaların farkında ve bilgi sahibi olduklarından emin olun. Bu politikaların, mümkün olduğunda otomatik olarak uygulanmalarını sağlayarak çalışanlar üzerindeki baskıyı azaltın ve benimsenmelerini kolaylaştırın.

Sabit disk içeren belge cihazlarının disklerinin, yer değiştirmelerinden veye elden çıkarılmalarından önce silindiklerinden emin olun. İşten ayrılan çalışanların ellerindeki, belgelere ve yönetilen sistemlere erişim sağlayan dizüstü bilgisayarların ve mobil cihazların, hemen geri verilmelerini sağlayın. Birçok ofis hâlâ parolalara güvenmekte; kimlik denetimi için kullanılan parolaların kolay tahmin edilemeyecek olmalarını sağlayın ve düzenli olarak değiştirin (en az yılda üç kez). Ayrıca, fiziksel güvenliği de ihmal etmeyin. Çalışanların hassas belgeleri ortada bırakmalarını engelleyecek temiz masa politikaları uygulayın. Kağıt imhası işlemi her gün yapılmalıdır.

Bunları sorun: Korsanlar belirli bir cihazla NE YAPABİLİRLER? Bir yazıcının içine Telnet bağlantısı yapılabilir mi? Baskı işleri izlenebilir mi? Baskı işleri tekrar yürütülebilir mi? Yönetici ayarları değiştirilebilir mi? Kötü niyetli çalışanların veya misafirlerin cihazlara fiziksel olarak erişip, doğru bir şekilde korunmamış bir cihazı veya içindeki sabit diski fiziksel olarak çalmaları riski var mı?

SONUÇ

Ofis BT sistem ve cihazları, düzenli olarak kontrol edilmiyorlarsa, hassas kişisel ve kurumsal veriler için tehlikeli yerler olabilirler. BT tarafından yönetilen yapısal veriler için kullanılan sıkı güvenlik önlemleri, belgelere ve onları basmak, yakalamak ve paylaşmak için kullanılan cihazlara, çoğunlukla uygulanmamaktadır.



Çok işlevli cihazlar, ağ yazıcıları, fotokopi cihazları, faks ve tarama cihazları, ofis ağınızın uç noktaları olarak, doğru bir şekilde yapılandırılmamışlarsa ve güvenli bir ağa bağlanmamışlarsa, işletmenizin veri güvenliğinde bir zayıflığa neden olurlar.

Kağıt belgelerde olan bilgileri, yetkisiz birine, kasıtlı veya yanlışlıkla iletmek kolaydır. Aynı şekilde bu tür belgelerin, imha edilmek yerine çöp kutusunu boylamaları da olasıdır. Eğer o belge yasal bir işleme konu olursa, belgenin nereden geldiğini veya yetkisiz erişimin nereden kaynaklandığını bilemezsiniz.

Basılı belgeleri dijitalleştirme ve baskı işleri koleksiyonunu doğrulama yoluyla, veya bilginin işletme içinde sorunsuz iletilmesi ile olsun, verilerin güvenli tutulması her şeyden önemlidir. Bu bilgilerin güvenliğini sağlamak için, her yerde organizasyonlar, iş güçlerini iç ve dış tehditlere karşı koymak üzere harekete geçiriyorlar.

Dayanıklı mimariler ve iş süreçleri benimseyerek, tepki veriyor olmaktansa önleyen olmak ve güvenlik riskleriyle emin bir şekilde mücadele etmek mümkündür.

Canon Ofis İçgörüleri 2017 araştırması hakkında

Ofis İçgörüleri 2017 adlı bağımsız araştırma Canon tarafından uluslararası bir pazar ve sosyal araştırma şirketi olan Breaking Blue'ya sipariş edilmişti. İçgörüler, Batı, Orta ve Doğu Avrupa, Avrasya, Orta Doğu ve Afrika'daki teknoloji karar vericileri ve son kullanıcılardan toplanmışlardı.

Ana bilgiler:

- 24 ülke genelinde 2.550 söyleşi
- Söyleşi yapılan organizasyonların boyu: (Küçük: 1-49) %58, (Orta: 50-199) %25, (Büyük: 200+) %17
- Katılımcıların %53'ü Yönetici rolüne sahipti
- %58'i genel ofis ortamlarında çalışıyorlardı
- %56'sı satın alma karar süreciyle doğrudan ilgiliydiler

Ayrıca, üçüncü taraf istatistikleri, kısa öyküler ve düşüncelerin referansları dipnotlarda verilmiştir.

Canon Europe Hakkında

Canon, sektörün en büyük ofis cihazları portföyüne sahiptir ve kendi ağ yönetim yazılımları ile, tek ve çok işlevli, küçük ve geniş format cihaz teknolojilerinin tümünü desteklemektedir. Donanımlarımız ve yazılımlarımız arasındaki eşleşme, belgelerin bilgi yaşam döngüleri içindeki hareket ve geçişlerinde güvenliği sağlama kabiliyetimizi iyileştirmektedir.

Görüntüleme teknolojileri ve hizmetlerinin küresel tedarikçisi olan Canon Europe, Canon Inc.'in EMEA koludur ve dünyanın en iyi tanınan ve sevilen markalarından biridir. Canon Europe, bölge genelinde 120 ülkede faaliyet göstermektedir ve 19.000 çalışana sahiptir. Canon Europe yıllık olarak, Canon'un küresel gelirlerinin üçte birini sağlamaktadır.

Canon Europe hakkında daha fazla bilgi için: www.canon-europe.com

Canon Inc.
Canon.com

Canon Europe
canon-europe.com

English Edition 0147W156

Canon Europe Ltd
3 The Square,
Stockley Park,
Uxbridge,
Middlesex
UB11 1ET UK

/Canon

/Canon

/CanonBusinessUK

Canon Eurasia AS
Degirmen Sokak
Nida Kule Is
Merkezi No:18/10
K:1 Kozyatagi
34742 Kadiköy
Istanbul Türkiye
canon.com.tr