Ricoh Güvenlik Çözümleri

İşletmenizi korumanıza yardımcı

RICOH
imagine. change.

Siber güvenlik, modern işletmelerin varlığını sürdürmesi ve başarısı karşısındaki en büyük tehdittir. Tüm ölçekteki şirketler, sürekli olarak kimlik avı, DDoS veya fidye yazılımı gibi yıkıcı saldırılardan mağdur olma riskiyle karşı karşıyadır. Bu saldırıların gerçek maliyeti milyonlara ulaşır. 2017 yılında, Ponemon Enstitüsü veri ihlallerinin global ölçekteki ortalama maliyetinin 3,62 milyon dolar olduğunu saptamıştır. Sistemlerini ve verilerini uygun şekilde koruyamayan işletmelere, GDPR gibi resmi düzenlemelerle büyük cezalar verilmesi beklendiğinden önümüzdeki yıllarda bu maliyet daha da artacaktır. Bu sarsıcı cezalardan kaçınmak için, bir işletmenin verilerini koruyabiliyor olduğunu göstermesi gerekir. Bu, bir kurumdaki tüm güvenlik açıklarına bütünsel bir bakış gerektirir.

Günümüzde iş yerlerinin büyümesi ve dijitalleşmesinin yanı sıra veri hacimlerindeki patlama, işletmeler için siber güvenlik zorluğunu daha da fazla artırmaktadır. İş akışları genellikle aygıtlara, ağlara ve coğrafyalara yayılmaktadır. Bilgi, bir işletmede dolaşım halindeyken en yüksek riskle karşı karşıyadır. Yolculuğunun her aşamasında sürekli koruma altında olması gerekir. Bu durumun ortaya çıkardığı güvenlik riski ortamında, modern işletmeler öncelikli olarak güvenli belge ve veri yönetimi sistemleri olmadan artık faaliyette bulunamamaktadır. Aynı zamanda, ofis yazıcılarının ve çok işlevli aygıtların yetenekleri son yıllarda on kat artmıştır. Artık işletme veri girişi, çıkışı, aktarımı ve depolama işlemlerinin büyük bir kısmı bu cihazların sorumluluğundadır. Bu durum, günümüzde bu cihazları iş yerindeki en tehlikeli, yine de sıklıkla gözden kaçan, tehdit taşıyıcılarından biri haline getirmektedir.

Birçok şirket güvenlik yeteneklerini sunma iddiasında bulunsa da, Ricoh on yıllardır güvenli iş yeri çözümleri ve hizmetleri geliştirmektedir. Örneğin yazıcılarımız 20 yıldan fazla bir süredir güvenli sabit disk üzerine yazma yeteneklerini sunmaktadır.

Güvenlik, tüm dijital iş yeri portföyümüzün temel yapı taşlarından biridir. Günümüzde sahada 4 milyondan fazla ofis ürünümüz bulunmaktadır. Bu ürünlerin her biri ve bunun yanında dağıttığımız her hizmet, yerleşik güvenlik özellikleriyle donatılmıştır. Ayrıca birçok ürünümüzde yalnızca Ricoh'a özgü bir işletim sistemi kullanılmaktadır. Güvenlik savunma sistemlerimizin önemli bir unsuru olan bu özellik sayesinde, daha yaygın işletim sistemlerini hedefleyen işletim sistemlerine özgü tehditler kontrolü ve bunlardan korunma sağlanmaktadır.

Ricoh, müşterileri için tehdit bilgisinin etkin şekilde paylaşılmasını ve buna göre davranılmasını sağlayan, dünya çapında tutarlı bir hizmet ve destek yapısı sunmaktadır. Baskı-çıktı cihazlarımızda standart olarak uygulanan IEEE 2600 sertifikasyonunun yanı sıra Ricoh, IEEE Standartları Birliği'nin önde gelen bir üyesi ve ana yazarıdır. Ricoh aynı zamanda ISO 27001 sertifikalıdır ve bu bilgi güvenliği yönetim sistemine uyumu devam ettirmeyi taahhüt etmektedir. Müşteri merkezli bir dizi global inovasyon programıyla, ürün geliştirme sürecimizi müşterilerin iş ihtiyaçlarına ve güvenlik endişelerine odaklanmış bir halde tutmaktayız.

Etkin, gösterilebilir siber güvenliğin en iyi uygulamalarının talepkâr gereksinimlerini karşılamak amacıyla, güvenlik Ricoh portföyünün her ürününde ve hizmetinde, kesinlikle sonradan akla gelen bir özellik değildir, bilinçli olarak yer alır. Bizler, tüm güvenlik açıklarına bu bütünsel bakışın, modern işletmelerin varlığını sürdürmesi için esas olduğuna inanmaktayız.

MÜŞTERİ GÜVENLİĞİ ZORLUĞU

TRENDLER: Veri hacimleri arttıkça, güvenlik açıkları, saldırılar ve cezalar da artmaktadır.

Dijital İş Yerlerinin Korunması ve Güçlendirilmesi

Ricoh, çalışanların eylem halinde olduğu her yerde dijitalleştirilmiş işi etkinleştirmek ve korumak için çabalamaktadır. Modern dijital ekonomide bu durum, geleneksel ofisin kısıtlamalarının ötesinde, birinci sınıf iş yerlerinde değer katmak anlamına gelir. Uzak ofisler ve çalışanlar günlük işlemlerde işletmelere olağanüstü esneklik ve üretkenlik artışları sağlamaktadır. Müşteri beklentilerini ve hizmet gereksinimlerini daha iyi karşılamaları için şirketlere yardımcı olmaktadır.

Ancak, ağın kenarında çalışmak işletme güvenliğinde en büyük risklerden bazılarını ortaya çıkarmaktadır. Çalışanların oluşturduğu bu verilerin ve bunları tutmak için kullandıkları uzak aygıtların uygun bir şekilde güvence altına alınması gerekmektedir. Çalışanların sık sık ağlar ve farklı bölgeler arasında çalışmak zorunda olması bu görevi daha da karmaşık hale getirmektedir. , GDPR gibi resmi düzenlemeler, işletmelerin verilerini kullanım ömürleri boyunca mutlaka gösterilebilir biçimde korumalarını gerektirmektedir aksi takdirde ciddi cezalarla yüz yüze kalmaları öngörülmektedir. İş yerleri geliştikçe ve dijital iş akışlarını kapsadıkça, işletme verilerinin yaşam döngüsü giderek daha karmaşık hale gelmektedir. Bu durumu şimdi aşama aşama inceleyelim.

İlk adım, Ricoh güvenlik savunmasının hayati bileşeni olan, veri girişi ve verilerin tutulduğu aygıtlardır. Burada, veriler ağlar arasında güvenli bir şekilde aktarılmalı ve depolanmalıdır. Bu aşamada, veri bütünlüğünün korunması çok önemlidir. Ricoh sistemleri, dolaşımda veya bekleme halindeyken verilerin üzerinde oynanamamasını sağlamak amacıyla, aygıt ve ağ işlevselliğine kullanıcı erişimini kısıtlar. Bu hizmetler erişim kontrolü, şifreleme ve kopya korumasını içerir. Biz bu işleme Kontrol diyoruz.

Ancak, belgelerin depolandıktan sonra ayrıca işletme içerisinde bunlara ihtiyaç duyanlara rahatlıkla erişilebilir olması gerekir. Bilgileri gerektiğinde kullanılabilme ve etkili bir şekilde görselleştirilme becerisi bu kullanılabilirliğe bağlıdır. Veri analizi, güçlendirilmiş dijital iş yerinin çok önemli bir bileşenidir. Satıştan İK'ya kadar işletmenin her öğesi için etkin şekilde bilgi sağlar. Yetkilendirme altyapı araçları, kullanıcı konumuna veya aygıt seçimine bakılmaksızın hızlı güvenli erişim sağlar.

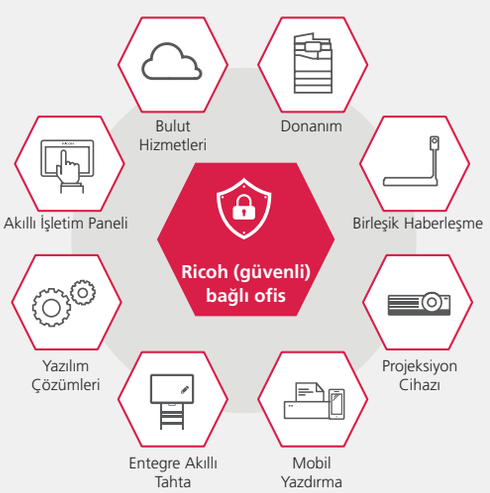
Güvenlik protokollerinin inovasyonu veya işlevselliği engellememesi veya çalışanlardan direnç görme riski taşımaması önemlidir. Bu aşamaya Koruma adı verilmektedir.

Son olarak, bu veriler güvenli, denetlenebilir bir biçimde ortadan kaldırılmalıdır. Bu adım düzenleyici gerekliliklere uyum için önemlidir ve ileride olabilecek hırsızlık veya kayıp olasılığını minimize eder. Bu işlem fiilen bir belgenin kullanım ömrü boyunca ve nihai silinme işleminde gerçekleşir. Bir dosya yazdırıldığındaı Çok İşlevli Yazıcıların (MFP'ler) sabit diskinde yetkisiz erişimi engellemek için üzerine yazılması gereken gizli bir görüntü bırakır. Ricoh veri ortadan kaldırma hizmetleri, korsanların bir belgenin arkasında bıraktığı ayak izlerinden hassas bilgileri derlemesini önlemek için sabit disk temizleme, bellek boşaltma, yazdırılmamış dosya silme ve oturum kapatırken silme işlemlerini kapsar. Bu işleme İmha adı verilir.

Ricoh'ta, bu kullanım ömrü süresince iş yeri verilerini etkin şekilde korumak amacıyla, gizlilik ve güvenlik için 'CIA' prensiplerii kullanılır: Gizlilik, Kullanılabilirlik ve Bütünlük. Bu üç unsur, gerekli standartları ve düzenlemeleri karşılamak için ürünve çözümlerimi tasarlarken benimsediğimizkılavuz ilkelerdir. Bu yaklaşım etkin, güvenli süreçleri sürmenin yanı sıra iş yerinde inovasyon ve büyüme sağlar.

RİCOH'UN GÜVENLİK YAKLAŞIMI

Ricoh olarak uygulamalarımızı 'CIA' gizlilik ve güvenlik ilkeleri (gizlilik, bütünlük ve kullanılabilirlik) çerçevesinde örüyoruz.



Güvenlik temel taşlarımızdan biridir. Ricoh'un sunduğu her ürün ve hizmet yerleşik güvenlik özellikleri ve yetenekleri içerir.

Ricoh, belge oluşturmayı başlangıçtan sonuna kadar güvence altına almak için eksiksiz bir güvenlik ürün ve hizmet paketi sunmaktadır.

Şimdi sırasıyla her hayati aşamayı inceleyeceğiz: kontrol, koruma, imha ve destek.

DİJİTAL İŞ YERİ GÜVENLİĞİNİN DÖRT AŞAMASI

1 KONTROL

Etkin veri kontrolleri, veri gizliliğini ve bütünlüğünü sürdürmede çok önemlidir. İşletme bilgileri birincil varlıklardır ve korunması gerekir. Günümüzün donanım aygıtları, işletme bilgileri için zayıf geçitler oluşturabilen bilgi terminalleridir. Bu yüzden Ricoh işletme verilerini kontrol etmek ve güvence altına almak için çeşitli sayıda kullanıcı yetkilendirme ve aygıt yönetimi araçları kullanmaktadır. Bunlar, fiziksel aygıtlarda belli işlevselliklere ve verilere izin sağlayan ve kısıtlayan ayarlarla ilgilidir. Herhangi bir Çok İşlevli Yazıcı (MFP) üzerinde dolaşanbilgilere çalışan erişimini kısıtlamak, belge güvenliğini sağlamada önemli bir örnek uygulamadır. Kontrol aşaması ayrıca, Ricoh'un aygıt üretici yazılımına üç kademeli yaklaşımı yoluyla, aygıtın kötü amaçlı yazılım korumasını içerir.

Yetkisiz kopya kontrolü

Ricoh, yetkisiz kopya oluşturma denemelerine karşı koruma olarak, yazılı kopya belgelerin güvenliğini sağlamak amacıyla zarif bir çözüm sunar. Kopya koruma işlevi, belgeleri arka plana gömülü olan görünmez özel desenlerle yazdırır veya kopyalar. Yazdırılan veya kopyalanan belgenin fotokopisi çekilirse ve/veya taranırsa, gömülü desenler kopyalarda görülür. Yetkisiz kopya koruma modülü MFP'nin gömülü desenleri algılamasını sağlar ve bilgi sızmasını önlemek için fotokopisi çekilen görüntüyü gri bir görüntü ile değiştirir. Bu işlev gizli bilgileri yazdırırken kullanışlıdır. Gizli bilgilerin çoğaltılmasının kısıtlanması bu tip bir bilgi sızıntısını önler.

Kilitli baskı

Bilgisayardan alınan bir belge MFP'deki sabit disk sürücüsünde depolanabilir. Ricoh kilitli baskı işlevini kullanarak, bir kullanıcı belgeyi gönderdiğinde bir şifre belirlenir ve bu şifrenin belge yazdırılmadan önce MFP'ye girilmesi gerekir. Belge sahibi aygıta ulaşana kadar belge yazdırılmayacağı için, kilitli baskı belgenin sahibinin kontrolü altında kalmasını sağlar.

Gelişmiş yakalama güvenliği

Ricoh'un gelişmiş yakalama çözümü portföyü, yakalama işleminin aşamaları arasındaki işlem katmanları boyunca değişen şifreleme ve şifre çözme katmanları sunar. Yöneticiler, bireysel kullanıcı oturumu açma veya grup kimlik bilgileri ile işlem sıralarına erişim yetkisi sağlayabilir. Güvenliğin ilave katmanları Çoklu Oturum Açma (SSO) çerçevesi için Güvenlik Koruma Biçimlendirme Dili (SAML), Kişisel Kimlik Doğrulaması (PIV) ve Ortak Anahtar Altyapısı (PKI) şifrelemesini içerir.

Gömülü yetkilendirme kontrolleri

Ricoh ürünleri arasındaki aygıt erişimi ve kimlik doğrulama protokolleri merkezi olarak yönetilebilir. Mevcut yöntemler arasında kimlik kartı, pin numarası, ağda oturum açma veya yukarıdakilerin çok faktörlü bir kombinasyonu bulunur. Çok faktörlü kimlik doğrulaması güvenliği artırır ancak yoğun kullanıcıları yavaşlatabilir. Çoklu Oturum Açma (SSO) kullanıcılara çeşitli aygıtlara sorunsuzca erişim sağlayarak bu duruma yardımcı olur. Ayrıca, kullanıcıların belgelerine erişmesi için kolay bir yol sağlayan Ricoh'un Hızlı Kimlik Doğrulaması, kart tabanlı okut -geç kimlik doğrulama yazılımı, aygıtlarımıza önceden yüklenmiştir. Bir NFC okuyucunun/yazıcının kullanılması, MFP'ye erişimi güvence altına alırken ve kontrol ederken kullanıcının oturum açma işlemini büyük ölçüde kolaylaştırır. Bu çeşit bir erişim ayrıca müşteri tarafından belirlendiği üzere aygıt işlevlerine kullanıcı erişimini kısıtlamak için mevcut MFP izinleriyle uyumlu şekilde çalışır.

Streamline NX (SLNX)

Ricoh Streamline NX platformu içerisindeki aygıt yöneticisi modülü, Ricoh'un bir ağdaki aygıtları yönetmeye ve izlemeye yarayan yazılımıdır. Yazılım, yöneticilerin önceden paketlenmiş şablonları ve özel parametreleri kullanan aygıtlar için güvenlik ayarlarını görüntülemelerini veya yapılandırmalarını sağlar. Önemli güvenlik ayarları; protokolleri etkinleştirme/devre dışı bırakma, IP adresi ayarları, Sistem yöneticisi kullanıcı parolaları, uyarılar için e-posta adresleri, şifreleme ayarları ve daha fazlasını içerir. SLNX ayrıca müşterinin politikasına dayanan uyumluluk içerisinde olmayan herhangi bir yazıcıyı rapor eder.

Aygıtın kötü amaçlı yazılım koruması

Ricoh, cihazlarındaki kötü amaçlı yazılım korumasına üç katmanlı bir yaklaşımda bulunur. Öncelikle, Ricoh aygıtları yalnızca Ricoh'a özgü bir makine dili veya işletim sistemi kullanarak çalıştırılabilir. İkinci olarak, aygıt yazılımında kötü amaçlı oynama yapılmasını önlemek amacıyla, herhangi bir üretici yazılımı güncellemesi özel olarak bu Ricoh makine dilinde yazılmalı ve onaylanmalıdır. Son olarak, her üretici yazılımı güncellemesi dijital olarak Ricoh tarafından imzalanmalıdır. Bu üç adımlı yöntem kullanılarak, onaylanmayan üretici yazılımı Ricoh aygıtlarına yüklenemez, böylece kötü amaçlı yazılım, casus yazılım ve virüsler etkin şekilde ortadan kaldırılır.

Fiziksel belge güvenliği

En iyi güvenlik uygulamaları her zaman karışık değildir. Ofisler yoğun yerlerdir ve yazılı kopya belgeleme hem hırsızlık hem de çalışanların ihmali anlamında önemli bir iş riski teşkil eder. Ricoh yazılı kopya belgelere yetkisiz erişimi önlemek için çeşitli ilave fiziksel güvenlik seçeneği sağlar. Örneğin, kağıt çekmecelerinin kilitlenmesi, sağlık hizmeti ortamındaki reçete şablonları gibi hassas kağıt stoklarında hırsızlık yapılmasını önler. Tüm kablolar için kapama plakası takılması da ayrıca iç tehditlerden gelebilecek kurcalama riskini önler. Güvenli bir belge yayımlama (Print-to-me) çözümü, alınmayan çıktı riskini ortadan kaldırmak için belgelerin yalnızca sahibi mevcutken yazdırılmasını sağlar.

2 KORUMA

Yeni ve mevcut düzenleyici gereklilikler kapsamında, işletmeler hem bilgilerin çalınmaması veya sızmaması için bilgi gizliliğini, hem de değiştirilememesi için sürekli bütünlüğü sağlamalıdır. Bunu gerçekleştirmek için işletmeler hassas belgelere erişimi kısıtlamalıdır. Bu, yetkisiz değiştirme ve tahrifatı önler. Ayrıca işletme içerisindeki hedeflenen veya fırsatçı tehditlere karşı koruma görevi görür.

Mobil çalışma herhangi bir siber güvenlik senaryosuna karmaşıklık katar. Herhangi bir konumdan dosya paylaşımını uygun hale getirmek için yerinde ilave güvenlik tedbirleri alınmalıdır. Bu dosyalar depolama halinde oldukları kadar ağlar üzerinde ve aygıtlar arasında güvenli olmalıdır. Güçlü şifreleme teknolojisi verileri kullanım ömürleri boyunca etkin olarak izleyebilir ve koruyabilir. Bu, doğal olarak belgelere uygulanır ancak depolanan parolalar, makro ayar ve adres defterleri gibi çok önemli güvenlik unsurlarına kadar uzar. Yerinde şifreleme ile, korsanlar ağınıza erişse bile kullanışlı bilgiyi çekmek için mücadele ederler, böylece bir ihlal durumunda bile bilgi bütünlüğü korunur.

Kesintisiz çalışma çoğu endüstri için en önemli konudur. Doğal afetler gibi öngörülemeyen olaylar doğrudan iş riski oluşturur. Bu senaryoda özellikle kağıt üzerindeki belgeler zarar görmeye yatkındır. Dijitalleştirilmiş belgeler için güvenli, bulut tabanlı bir depo kullanmak, doğal ve insan kaynaklı afetlerde önemli bir esneklik katar. Ancak, bu dijital verileri korumak için uygun güvenlik adımlarının atılması gerekir.

Önemli veri şifreleme

Aygıtlar arasında dolaşan bilgileri korumak için, bir Ricoh MFP sabit diskine gelen veya burada bulunan herhangi bir veri için şifreleme etkinleştirilebilir. Yerleşik yazılım seçenekleri, kullanıcının ortak anahtar altyapı (PKI) anahtarı yoluyla taranmış ve yazdırılmış dosyalar için uçtan uca şifreleme sağlar. Bu, müşterinin BT ortamı içerisindeki 'bağlantıyı izinsiz izleme' şeklindeki saldırılara karşı koruma sağlar.

İlave güvenlik için, daha sonra veri kullanım ömrünün 'imha' aşamasında daha detaylı olarak açıklayacağımız, Ricoh'un Veri Üzerine Yazma Güvenlik Sistemi (DOSS) ile baskı verisinin de ayrıca sürekli olarak üzerine yazılır.

Bios ve işletim sistemi koruması

Ricoh MFP'lerde kurcalamaya dayanıklı bir donanım güvenliği modülü olan Güvenilir Platform Modülü (TPM) kullanılır. TPM şifreleme işlevleri gerçekleştirir ve şifreleme verilerini güvenli bir şekilde depolar. Ricoh, sabit disk şifreleme anahtarını ve MFP'lerin dijital sertifikalarını koruyan kök şifreleme anahtarını depolamak için TPM'yi kullanır. Modül ayrıca, çalışmasına izin vermeden önce MFP'nin üretici yazılımı orijinalliğini doğrulayarak yöneticilerin güvenilir bir ön yükleme işlemi gerçekleştirmelerini sağlar.

Üretici yazılımı doğrulaması

Kök anahtar ve şifreleme işlevleri her zaman TPM içerisinde yer alır ve güvenlik duvarının dışından değiştirilemez, böylece ürünlerimizin suiistimal edilmesi veya kötü amaçlı olarak üzerinde oynanması önlenir. Bu işlem MFP'nin üretici yazılımı, aygıt kimliği ve sabit disk güvenliği için yüksek seviyede doğrulama sağlar. Bu, Ricoh'un MFP ürünlerinin Ricoh müşterilerinin güvenlik menfaatlerini gözetilerek tasarlandığını gösteren güzel örneklerden biridir.

Parola yönetimi

Ricoh aygıtları, her biri aygıtlar üzerinde farklı rollere ve ayrı parolalara sahip olmak üzere, birden fazla yönetici kullanıcı ile yapılandırılabilir. Bu kullanıcılara ait parolalar, web tabanlı yönetim araçlarını kullanarak uzaktan yapılandırılabilir ve düzenli olarak doğrulanabilir. Bu işlem, çeşitli işletme düzenlemelerinde mevcut bir gereklilik olan 'görevler ayrılığı ilkesini' mümkün kılar.

Kullanıcı erişim kısıtlaması

Ricoh'un kullanıcı yönetimi aracı sistem yöneticilerinin kullanıcı erişim ayrıcalıklarını kısıtlamalarını sağlar. Örneğin yönetici, seçilen kullanıcılara MFP'nin kayıtlı adres defterine erişim sağlamak için ayrıcalıkları ayarlayabilir. Bu, ofis aygıtlarındaki kişisel bilgilere ve depolanan kayıtlara yetkisiz erişimi engeller.

Kullanıcı kilitleme işlevi

Oturum açma işlemi sırasında yanlış parolalar arka arkaya girildiğinde, Ricoh MFP'ler birinin parolayı kırmaya çalışıp çalışmadığına erişim sağlayabilir. Bu durumda, söz konusu kullanıcı adını engelleyen kilitleme işlevi tetiklenir. Engellenen kullanıcı adı, sonradan doğru parola ile birleşse bile doğrulanamaz. Kilit, korsanları etkin olarak engelleyecek şekilde yalnızca belli bir süre sonra veya yönetici tarafından kaldırılabilir.

3 İMHA

Verilerin güvenli olarak ortadan kaldırılması kapsamlı siber güvenlik savunmasının önemli bir parçasıdır. Veriler kurumdan çıktığında işletme sorumluluklarının sona erdiğini düşünme hatasına kolaylıkla düşülebilir. Ancak birçok düzenleme, sonradan olabilecek bir hırsızlık veya suiistimal riskini ortadan kaldıracak şekilde, veri imhasının kapsamlı bir işlem olmasını şart koşar. Bu kanıtlanana kadar, bir işletmenin veri yükümlülükleri sona ermez.

Ömrünü tamamlayan ve iade edilen ofis aygıtları genellikle işletme bilgileri için kabul edilmeyen bir risk oluşturur. Ricoh ömrünü tamamlamış bu yazıcılardan verileri kaldırmak için sertifikalı ve denetlenebilir bir hizmet sunmaktadır. Bu, kaydedilen ağ ayarları, kullanıcı verileri, sabit disk verileri ve hatta aygıt üzerinde kalan çıkartmalar gibi gözden kaçan materyalleri kapsar. Bunların yapılmaması, işletmeler için gizli şirket ve personel bilgilerinin açığa çıkması gibi önemli bir risk teşkil eder. Ancak mevzuata uyumluluğu sürdürmek amacıyla, bu süreç aygıtın ömrü boyunca da sürekli olarak devam etmelidir. Bu durum işletmelerin sorumlu oldukları veriler üzerinde maksimum derecede kontrol sahibi olmalarını sağlar.

Görüntünün üzerine yazma: Veri Üzerine Yazma Güvenlik Sistemi (DOSS)

MFP sabit diskleri, iş işleme için belge verilerinin görünmeyen görüntülerini belleklerine depolayarak etkin şekilde çalışır. Ricoh'un Veri Üzerine Yazma Güvenlik Çözümü, sonraki iş başlamadan önce sürekli olarak bunların üzerine yazılmasını sağlar. Böylece herhangi biri sabit diske kötü amaçlı olarak erişirse, önceki işlerden geride kalan herhangi bir veri 'ayak izine' erişim sağlayamaz. Ricoh'ta 20 yıldan fazla süredir bu en iyi güvenlik tedbiri uygulamasını sunduğumuz için gurur duymaktayız.

Kullanım ömrü sonu temizleme hizmeti

Ricoh, endüstri sertifikalı güvenlik çözümlerini kullanarak, aygıttaki tüm bellek modüllerinin ve disk depolama birimlerinin kurtarılmaz şekilde silindiği bir kullanım ömrü sonu hizmeti olan Tam Veri Temizleme Hizmetini sunmaktadır. Ricoh'un BT Hizmetleri ayrıca çeşitli seviyelerde sertifikalı silme hizmetlerini içeren kapsamlı bir donanım imha hizmeti de sunmaktadır.

Sabit disk değişimi ve çıkarılabilir depolama birimi

Ricoh ayrıca müşteriler kiralama sonunda donanımı iade ettiklerinde yeni, boş bir sabit disk ile değiştirerek, sabit disklerini kaybetmemelerini sağlayan bir sabit disk imha hizmeti de sunar. Bu, işletmelere veri ortamları üzerinde eksiksiz, gösterilebilir bir kontrolü garanti eder.

4 DESTEK

İşletmeler büyüdükçe, aygıtlar ve ağlar arasındaki bağlantı sayısı da kaçınılmaz şekilde büyür. İşletmelerin bu altyapı büyümesinin güvenlik riski oluşturmamasını sağlayacak stratejilere ihtiyacı vardır. İşletmeler, hedeflenen ve fırsatçı saldırılara karşı önceden tedbir alabilmek için sistemlerindeki zayıf noktalardan haberdar olmalıdır.

Genellikle özel bir BT güvenlik uzmanının işletmenin altyapısını analiz etmesi ve bu güvenlik açıklarını belirlemesi gerekir. Birçok işletme için yalnızca siber güvenlik ortamlarını yönetmek için gerekli bilgiye sahip kurum içi bir BT personeli sağlamak elverişli bir seçenek değildir. Bu yaklaşımın maliyetleri ve işe yaramaması genelde bu işletmeleri tehlikeli bir eylemsizliğe iter.

Ricoh'un BT destek hizmeti, BT tedarik ve yapılandırma hizmetlerinin yanı sıra siber güvenlik sürecini desteklemek amacıyla uzaktan izleme, hizmet masası ve geçiş yönetimi yetenekleri sunmaktadır. Siber güvenlik işletme risklerini bütünsel bir şekilde anlamaya dayanır. Ricoh'un Güvenlik Olay Yanıt Ekibi (SIRT) hayati tehdit istihbaratının dünya genelindeki müşterilerle paylaşılmasını ve etkili yanıtların anında koordine edilmesini sağlar.

Altyapı güvenlik değerlendirmesi

Ricoh'un Streamline NX (SLNX) aygıt yöneticisi işlevselliği, paha biçilmez güvenlik politikası denetim işlevini gerçekleştirmek için tasarlanmıştır. SLNX, BT yöneticilerinin aygıtları şirketin politikasına göre kurmasını, bu ayarları dağıtmasını ve görselleştirilmiş bir rapor ile ayarları analiz etmesini sağlayan bir işlevsellik sunar. SLNX ayrıca bir aygıt şirket politikası ile uyumluluk dışına çıktığında yönetimi uyarabilir.

Baskı güvenlik optimizasyonu

Ricoh, aygıta bağlı güvenlik açıklarını belirlemek için profesyonel ve yönetilen danışma hizmetleri ile birlikte kapsamlı bir Baskı Güvenlik Optimizasyonu (PSO) sunar. Bu, mevcut durum görünümünü veren grafiksel bir sihirbaz bulunan web tabanlı bir araçtır ve Ricoh'un riski azaltmak maksadıyla ürün önerilerinde bulunmasını sağlar.

Ürün Güvenlik Olay Yanıt Ekibi (PSIRT)

Ricoh'un yeni tehditlere karşı aktif yanıtı ve etkin karşı tedbirlerin geliştirilmesi Ricoh'un Ürün Güvenlik Olay Yanıt Ekibi (PSIRT) tarafından yönetilir. Bu, tüm ürün paketimizin (donanım ve yazılım) sürekli olarak güncellenmesini ve yeni belirlenen tehditlere ve güvenlik açıklarına karşı korunmasını sağlamak için Ricoh'un kullandığı bir programdır. Bu program global ölçekte sürekli olarak yüksek seviyede bir hizmeti devam ettirmemize ve Ricoh ürünlerindeki güvenlik açığı sorunlarının etkisini minimize etmemize yardımcı olur.

Destekleyici belgeler

Hazırlık ve eğitim herhangi bir siber güvenlik kurulumunun en önemli unsurudur. Yedek belgeler, kullanıcı kılavuzları, güvenlik teknik incelemeleri ve eğitim öğelerinin tümü müşteriye tedarik edilmelidir. Siber güvenlik ortamının birçok öğesinde olduğu gibi, gösterilebilir uyumluluk çok önemlidir ve bu belgeler bir işletmenin esasını korumada kilit bir rol üstlenir.

RICOH NASIL YARDIMCI OLABİLİR?

Ricoh'un tüm BT ve baskı ortamı arasında endüstri lideri güvenlik çözümleri sağlamasındaki eşsiz konumu, kısmen, değişen piyasa koşulları üzerinde güçlü bir anlayış sağlamaya ve buna bağlı olarak rotamızı geliştirmeye dayanmaktadır. Çözümlerimiz, tüm bilgiyi tüm kullanım ömrü boyunca korumak ve bu raporda anlatılan dört veri güvenliği alanında yakından söz sahibi olmak için tasarlanmıştır.

Yeni çözümlerin oluşturulabileceği veya mevcut çözümlerin uygun hale getirileceği sektörel gereklilikler de dahil olmak üzere, piyasa ihtiyaçlarını analiz etmekten sorumlu konu uzmanları tahsis ettik.

Bizler ayrıca güvenlik merkezli çözümleri düzenlemek ve dağıtmak için dahili kapasitemizi geliştirmeyi taahhüt ettik. Bu amaçla, hizmet geliştirme organizasyonumuz içerisinde yeni yönetim, risk yönetimi, uyumluluk ile birlikte siber güvenlik hizmetlerine odaklanmış özel ekipler oluşturduk.

Kullanıcı kimlik doğrulaması ve yetkilendirme

- Kilitli baskı
- Kimlik doğrulaması için standart gömülü yazılım
- Kullanıcı kimlik doğrulaması / erişim kısıtlaması
- Çoklu oturum açma
- Birden fazla yönetici rolü
- PDF parola koruması (taranan belge için parola)
- Yetkisiz kopya koruması
- IP-aralığı tabanlı erişim kontrolü
- Güvenli aygıt ve baskı yönetimi
- PKI (Ortak Anahtar Altyapısı) / Akıllı Kart desteği
- Güvenli yazdırma (print2me / kilitli baskı)

Aygıtın kötü amaçlı yazılım koruması

- Sunucular
- Kötü amaçlı yazılıma açık değil veya daha az açık
- SOP – Android'in kuvvetlendirilmiş sürümü
- MFP için makine işletim sisteminde (makine kontrol dili) Ricoh'a özgü sürüm
- 3 katmanlı yaklaşım – dijital imza, Ricoh aracı ile indirme, özel kontrol dilinde yazılması gerekliliği

Sabit disk imhası

- Sabit disk imhası, görüntü üzerine yazma,
- Tam Veri Temizleme Hizmeti
- Kullanım ömrü sonu hizmeti: bellek modülleri, depolama birimi içerisinde veri imhası

Aygıt yönetimi

- Kota ayarı / hesap kısıtlaması
- DMNX – güvenlik denetimi, parola yönetimi, izleme, uyarma için tek ekran bölmesi

Bios ve işletim sistemi koruması

- Güvenilir Platform Modülünü (TPM) kullanan güvenli ön yükleme

Görüntünün üzerine yazma ve çıkarılabilir depolama ortamı

- Disk Üzerine Yazma Güvenlik Sistemi (DOSS)
- Çıkarılabilir sabit disk

Veri şifreleme

- TPM ile sabit disk şifreleme
- TPM ile şifreleme anahtarları
- PKI anahtarını kullanarak baskı ve tarama dosyalarını uçtan uca şifreleme
- FIPS sertifikalı HDD (Federal Bilgi İşleme Standartları)
- Yazdırma için uçtan uca şifreleme
- Tarama için uçtan uca şifreleme

Firmware güncellemeleri ve parola yönetimi

- Uzak parola denetimi
- Kullanıcı kilitleme işlevi
- TPM ile firmware doğrulaması

Endüstri standartları ile uyumluluk

- ISO 27001 Sertifikasyonu
- Seçilen ürünler için IEEE 2600.2 Sertifikasyonu
- Seçilen ürünler için ISO 15408 Sertifikasyonu
- Güvenlik belgeleri ve eğitimi

RİCOH'UN AYGIT GÜVENLİĞİNE KATMANLI YAKLAŞIMI

MFP sağlayıcı rolünün, donanımın işlem tabanlı, tek boyutlu olarak sağlanmasının çok ötesinde, mevcut veri yönetimine doğru evrim geçirdiği şüphe götürmez. MFP'lerin kapasitelerinin kapsamı artık çoklu kanal girişlerinden bilgi yakalamaktan, yakalanan verilerin sınıflandırılmasına ve iş akışı entegrasyonuna, güvenli, korunan depolama ve analize kadar genişlemiştir. Tutulan kayıtları kayıp, çalıntı ve kurcalama riskleriyle karşı karşıya bırakan iç ve dış tehditlerin yanı sıra çeşitli ağır düzenleyici kuralların ve muhafaza gerekliliklerinin olduğu bu karmaşık ortamda, çok işlevli yazıcılarınızın ve bağlandıkları sistemlerin size mümkün olan en iyi korumayı sağlaması için çok katmanlı bir aygıt güvenliği yaklaşımı benimsemekteyiz.

1. Aygıt

Ricoh modelinin kalbinde aygıt yatar. Bu aygıtlar ana gereklilik olarak güvenli bir biçimde tasarlanmış, üretilmiş ve tamamlanmıştır. Ricoh'a özgü işletim sistemi, kullanıma hazır birçok ticari işletim sisteminde bulunan güvenlik açıklarını paylaşmaz ve aygıtlarımız standart olarak IEEE2600.2 sertifikalıdır. Sabit disk şifreleme ve disk üzerine yazma güvenliği işlenen verilerin gizli kalmasını sağlar.

2. Akıllı İşletim Ekranı (SOP) kullanıcı arayüzü sağlar

MFP ile aynı biçimde, SOP Ricoh'a özgü bir işletim sistemi kullanır. Gereksiz bileşenler yüklenmez ve kök erişimi mevcut değildir. Ricoh, SOP'nin girişiyle aygıt güvenliğinin zayıflamamasını sağlamak için çok çalışmıştır.

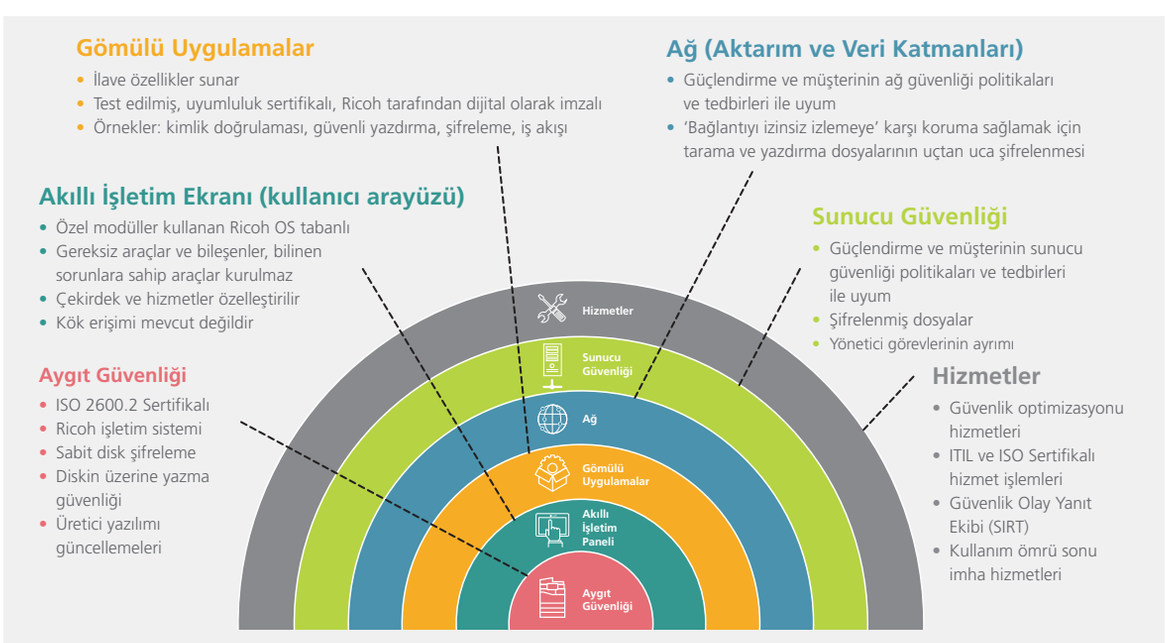
3. Akıllı Uygulamalar

Bu uygulamalar iş akışı ve veri yakalama dahil olmak üzere kullanıcıya ilave işlevsellik sağlayacak şekilde SOP'ye gömülebilir. Bazı uygulamalar önemli güvenlik özellikleri sağlar. Bunlar güvenli baskı yeteneği, kart erişimi ve şifrelemeyi içerir. Uygulamalar Ricoh veya Ricoh Geliştirici Programı üyeleri tarafından geliştirilmiştir ve tüm uygulamaların Ricoh Uyumluluk testini geçmesi ve SOP'de çalışmadan önce dijital olarak imzalanması gerekir.

4. Ağ ve Sunucular

BT altyapısını kimin yönettiğine bakılmaksızın, Ricoh ürünlerimizin ve hizmetlerimizin sizin BT ve ağ güvenliği politikalarınızla uyumlu olmasını sağlar. Baskı ve tarama dosyalarının uçtan uca şifrelenmesi, sunuculardaki verilerin şifrelenmesi ve yönetici görevlerinin ayrımı 'bağlantıyı izinsiz izleme' ve 'içeriyle bağlantılı eylemlere' karşı koruma sağlamak için kullanılan tekniklerdir.

Geniş bir yelpazedeki güvenlik hizmetleri tüm tekliflerimizi kapsamaktadır. Bunun içinde müşterilere belge ve bilgi güvenliklerini izleme, optimize etme ve yönetme konularında yardımcı olmak için danışmanlık ve yönetilen hizmetler bulunur. Ayrıca, kullanımı sona eren müşteri aygıtlarının RAM ve HDD'sinin imhadan önce silinmesini sağlayan bir dizi kullanım ömrü sonu hizmetlerimiz bulunmaktadır.



RİCOH DİJİTAL İŞ YERİNİ NASIL KORUR

İş dünyasında veri hacmi arttıkça güvenlik açıkları, saldırılar ve yasal cezaların da arttığı bilinen bir gerçektir, buna bağlı olarak da müşterilerimizin birtakım temel güvenlik endişeleri vardır. Verileri gizli, güvenli ve üzerinde oynama yapılamaz halde tutmak süreklilik isteyen bir mücadeledir. Örneğin, Ricoh'ta bizler her ay 8 milyar güvenlik duvarı saldırısını püskürtmekteyiz. On binlerce global, ulusal ve endüstri veri düzenlemesi bulunmaktadır ve işletmelerin bunların her biriyle uyumlu olduklarını sürekli kanıtlamaları gerekir. Anlaşılır biçimde, her ölçekteki organizasyon, tüm dijital iş yerini kapsayan bir portföyde güvenli kalmalarına yardımcı olabilecek, güvenebilecekleri bir ortak aramaktadır.

Ricoh, işletmelerin karşılaştığı çeşitleri riskleri azaltmak için geniş yelpazede çözümler geliştirmiştir. Bilgi güvenliği tehdit durumu inanılmaz derecede hızlı evrim geçirdiği için, Ricoh hizmetlerimizi daha da geliştirip teslim etmek için 'müşterinin sesi' programlarından yararlanmaktadır.

Müşteri Danışma Kurullarımız ana stratejik odak grupları olarak çalışır. Bunları, müşterilerimizin faaliyetlerini şekillendiren eğilimleri, faktörleri ve öncelikleri daha iyi anlamak için kullanırız. Teknoloji Danışma Konferanslarımız ana karar vericilerden gelen çok önemli bilgileri sağlar. Ricoh'un mühendislik ve Ar-Ge ekipleri, fikirler, konseptler ve prototipler hakkında değerli müşteri geri bildirimlerini almak için bu konferansları kullanırlar. Son olarak, Ricoh dikey ve genel piyasa müşterileri için yeni ve gelişmiş güvenlik özellikleri geliştirmek için bireysel müşterilerle işbirliği yapar. Bu müşteri merkezli yaklaşım, ürün yol haritamızı onaylamamıza ve müşterilerimizin global hizmet ve destek ağından yararlanmalarına yardımcı olur.

Modern dijital iş yeri, karşılaştıkları siber tehditler kadar dinamik ve içerisindeki çalışma pratikleri kadar esnek olmalıdır. İşte bu yüzden iş yerlerini olanaklı kılmak için müşterilerimizin seçtiği teknoloji içerisinde siber güvenliğin sorunsuzca çalışması gerektiğine inanırız. Organizasyonumuzun her kademesinde ISO 27001'e uyumluluk taahhüdümüz ve ürünlerimizde IEEE 2600 sertifikasyonuna sahip olmanın yanı sıra sadece Ricoh'a özgü işletim sistemi kullanılması, Ricoh'ta en iyi güvenlik kontrollerinin mevcut olduğunu göstermektedir; işletmenizi yapılandırmak ve büyütmek için seçim yapmak ise size kalmıştır.

Güvenlik tehditleri, yasal gereklilikler ve karmaşık sektör standartları; siber riskten dolayın itibar açısından ve mali açından e zarar görme potansiyelinin daha önce hiç bu kadar büyük olmadığını yansıtmaktadır. Artık işletmenizin saldırıya en yatkın varlıklarını güvence altına almanıza ve ilerideki amaçlarınızı korumanıza yardımcı olması için güvenilir bir ortak ile çalışmanın vakti gelmiştir.

RICOH
imagine. change.

www.ricoh.tr