KONICA MINOLTA

İLETİŞİMİNİZİ KORUMA ALTINA ALMANIN YOLU

Konica Minolta Güvenlik Standartları

İçinde bulunduğumuz dijital çağda, küresel iletişimin daha önce eşi benzeri görülmemiş bir hızda gelişimi ve yaygınlaşmasına şahit olduk. Bunun paralelinde, güvenlik ihlali olasılığı da aynı boyutta arttı. Artık günlük baskı, fotokopi, e-posta ve faks gibi uygulamalar tüm iş ortamlarında en temel iletişim araçları haline geldi. İş akışları ise çok işlevli ofis ekipmanlarını (MFP'leri) pek çok açıdan vazgeçilmez kılmakta. Bütün bu gelişmeler, bu cihazların süregelen güvenlik tehditlerine karşı önlem alan çeşitli mekanizmalarla donatılması gereğini doğurdu.

Giving Shape to Ideas

GÜVENLİK

GÜVENLİK İHLALLERİNİN EKSİKSİZ VE HATASIZ TESPİTİ & ÖNLENMESİ

Çözümlerin güvenlik ihlallerini hem tespit etmesini hem de önlemesini istiyorsanız ve aynı zamanda gerek bireysel gerekse kurumsal seviyede finansal zararlardan ve/veya itibarınıza yönelik olası zararlardan korunmak istiyorsanız, kapsamlı standart güvenlik özellikleri ve seçenekleri yelpazesi sunan endüstri lideri Konica Minolta'ya güvenin.

Genel olarak MFP'ler kullanıcılarına tek başına ya da kombinasyon halinde kullanılabilecek çok geniş bir işlev ve seçenekler yelpazesi sunmaktadır. Bunun sonucunda, benzer genişlikte bir olası güvenlik boşlukları yelpazesi de ortaya çıkmaktadır. MFP güvenliği konusu, üç ana başlık altında gruplanabilir:

- **Erişim kontrolü / Erişim güvenliği**
- **Veri güvenliği / Belge güvenliği**
- **Ağ güvenliği**

Konica Minolta Güvenlik İşlevlerine Kısaca Göz Gezdirelim

Erişim kontrolü	Fotokopi/baskı muhasebesi
	İşlem kısıtlama
	Güvenli baskı (kilitleme özelliği)
	Kullanıcı kutusu şifreli koruma
	Kullanıcı doğrulama (Kimlik+şifre)
	Parmak dokusu tarayıcı
	IC kart okuyucu
	Etkinlik kaydı
Veri güvenliği	Veri şifreleme
	Sabit disk veri geçersiz kılma özelliği
	Sabit disk şifre koruması
	Veride kendi kendini silme özelliği
Ağ güvenliği	IP filtreleme
	Port ve protokol erişim kontrolü
	SSL/TLS kriptolama (HTTPS)
	IP sec desteği
	S/MIME
	802.1x desteği
Tarama güvenliği	Kullanıcı doğrulama
	SMTP öncesi POP
	SMTP doğrulama (SASL)
	Manuel destinasyon bloke etme özelliği
Diğerleri	Servis modunda koruma
	Yönetici modu koruma
	Veri tarama
	İzinsiz giriş kilidi
	Filigran ile kopyalamaya karşı koruma
	Şifreli PDF
	PDF imzası
	Dijital kimlik ile PDF şifreleme
	Kopya koruyucu/Kopyalama şifresi

GÜVENEBİLECEĞİNİZ **KANITLANMIŞ GÜVENLİK DEĞERLENDİRMESİ**

İhtiyaç duyduğunuz güvenliği garanti edecek çıktı cihazlarınıza gerçek anlamda güvenmek mi istiyorsunuz? Konica Minolta yazıcı ve MFP'ler ile içiniz rahat olsun - neredeyse istisnasız her biri Ortak Kriterler / ISO 15408 EAL3 standardı ve IEEE 2600.1 belgesine sahip.

ISO 15408 EAL3 uyumlu Ortak Kriterler Sertifikası, dijital ofis ürünlerinin IT güvenlik testleri bağlamında uluslararası kabul gören tek standarttır. ISO 15408 EAL3 uyum belgesine sahip yazıcılar, fotokopi makinaları ve yazılımların tümü, katı ve kapsamlı bir güvenlik değerlendirmesinden geçirilmiştir ve sağduyu sahibi her kurumun haklı beklentisi olan güvenlik seviyelerini karşılayacak özelliktedir.

Ortak Kriterler Sertifikası, IEEE 2600.1 uyarınca Konica Minolta'nın ofis bilgi güvenlik standardını tanımakta ve onaylamaktadır. Uluslararası bir IT güvenlik standardı olan bu sertifika, belgelendirilmiş MFP'lere ait güvenlik özelliklerinin IEEE'nin (Elektrik ve Elektronik Mühendisleri Enstitüsü) yüksek standartları ile uyumlu olduğunu onaylar. Kurum seviyesinde saklanan günlük ofis yazışmalarından gizlilik içeren bilgi ve belgelere kadar tüm veri güvenilir şekilde korunmalıdır - bu sertifika da size bunun gerçekleşeceğini garanti etmektedir.

Standart güvenlik özelliklerinde belirleyici rol oynayan Konica Minolta bu alanda endüstri lideri konumundadır.

Common Criteria Validated

"Güvenlik, Konica Minolta'nın genel stratejisinde temel bileşendir…

Konica Minolta birçoğu bizhub serisinde standart olan çok geniş bir baskı ve belge güvenliği özellikleri yelpazesi sunmaktadır. Opsiyonel güvenlik kitlerini sertifikalamak yerine, Konica Minolta piyasadaki en geniş "ISO 15408 ile tamamen sertifikalanmış" çok fonksiyonlu yazıcı yelpazesine sahip olduğu iddiasındadır."

Kaynak: Quocirca (2011), Pazar çalışması "Baskı güvenliği boşluğu kapatılıyor. Baskı güvenliğinde firmaların konumu.", s. 11. Bu bağımsız rapor bilgi teknolojileri ve iletişimin iş dünyasındaki etkilerinin araştırılması ve incelenmesi alanında (ITC) uzmanlaşmış Quocirca Ltd. tarafından hazırlanmıştır.

A'DAN Z'YE GÜVENLİK İÇİN **BİREYSEL ERİŞİM KONTROLÜ**

Her ne kadar güvenlik konusu günümüzde gerek kamuoyu gerekse kurumsal çevrelerde gündemin ilk sıralarında yer alsa da MFP'lerden kaynaklanan tehditler çoğunlukla tamamen göz ardı edilmektedir. Şirketlerin büyük bir kısmı bazı risklerin farkına varsa da bunlar büyük ölçüde ihmal edilmektedir. Bu riskler, özellikle ortak alanda konumlandırılmış MFP ya da yazıcılarda hassas belge ve bilgilere çalışanlar, müşteriler ve hatta ziyaretçilerin erişebilir olması ile daha da tehlikeli bir hal almaktadır.

Günümüz MFP'erinde yer alan gelişmiş özellikler sayesinde bilgi gerçek ya da sanal kurum sınırları içinde veya ötesinde kolayca kopyalanıp dağıtılabilir. Atılacak ilk akıllıca adım, yetkilendirilmemiş kişilerin MFP kullanımını engellemek olacaktır. Koruma amaçlı önlemler öncelikle MFP'lere erişimi kontrol altına almalıdır. İkinci adım, cihazların gerçek yaşamda kullanım şeklini yansıtan bir güvenlik politikası oluşturmak olmalıdır. Konica Minolta bunu, sistemlerin kullanıcı-dostu özelliklerini hiçbir şekilde sekteye uğratmadan başarmaktadır.

Kapsamlı Kullanıcı Doğrulaması

Doğrulamada, MFP cihazlarını kullanmaya yetkili olacak kişi ve grupların belirlenmesine ve gerekli düzenlemenin yapılmasına yönelik bir politika oluşturmakla yola çıkılır. Buna, örneğin bazı kişilerin renkli çıktı alma yetkisi olması bazılarının da olmaması gibi, erişim haklarına getirilecek kısıtlamalar dahildir.

Konica Minolta kullanıcı doğrulaması için üç temel teknoloji sunmaktadır:

1. **Kişisel Şifre**
   Şifre 8 karaktere kadar alfa numerik bir kod olup MFP panelinde girişi yapılmaktadır. Bu kodlar idari personel ve kullanıcılar için oluşturulabilmekte ve en önemlisi merkezi olarak yönetilebilmektedir.

2. **Kimlik Kartı Doğrulama**
   Konica Minolta cihazlarının büyük çoğunluğuna bir kimlik kartı okuyucusu takılabilmektedir. Kimlik kartları süreçte kolaylık ve hız sağlar - kartın okuyucu arayüzü üzerine veya yakınına tutulması, sisteme giriş ve çıkışın sağlanması için yeterlidir.

Kullanıcı doğrulaması

3. **Biyometrik Parmak Dokusu Tarayıcı**
   Bu cihaz, sıradan parmak izi tarayıcılarının gelişmiş bir tasarımıdır. Sistem taranan parmağa ait damar yapısını bellekteki kayıt ile karşılaştırma yoluyla çalışmaktadır. Parmak dokusu, tahrifatı neredeyse imkânsız, şahsa özel fiziksel bir biyometrik özellik olması nedeniyle, kişilerin kimlik tespitinde kullanılmaktadır. Parmak izi sistemlerinin aksine parmak dokusu taraması kişi kendisi bizzat mevcut olmadan veya hayatta değilse yapılamamaktadır.

   Biyometrik parmak dokusu tarayıcısı, insanların kart taşıma ya da bir takım şifreleri hatırlama zorunluluğunu ortadan kaldırıyor.

Doğrulama bilgisi MFP üzerinde (kriptolanmış şekilde) tutulabilir ya da Windows Active Directory'deki mevcut veriden alınabilir.

Her bireyin sisteme giriş ve kullanım bilgileri sürekli kayıt edildiğinden güvenlik ihlalleri anında belirlenerek uyarı verilir.

Daha Şeffaf Bir Süreç İçin Hesap Takibi

Güvenlik nedeniyle, kullanıcı kontrolü sisteminde her kullanıcı çıktı cihazına giriş yapmak zorunda olduğundan, ortaya çıkan veri aynı zamanda kullanıcı, grup ve/veya departman gibi farklı seviyelerde etkin bir takip aracıdır. Siyah/beyaz, renkli fotokopi, tarama, faks, siyah/beyaz ya da renkli baskı, hangi cihaz işlevi kullanılırsa kullanılsın uygulamaların her biri gerek makineden gerekse uzaktan tek tek izlenebilir. Bu verinin analizi ve tespit edilen yönelimler MFP kullanımına ilişkin farklı bakış açılarından gelen sağlam bir bilgi kaynağıdır: veri uyumunun sağlanması ve yetkisiz girişlerin takibi için kullanılabileceği gibi daha da önemlisi kullanım kontrol sisteminin bir kurum/kuruluş ya da ofisteki tüm yazıcılara ve MFP'lere uygulanabilir olmasıdır.

İşlev Sınırlamaları ile Erişimin Kişiselleştirilmesi

Çeşitli MFP işlevlerini bireysel kullanıcı bazında sınırlandırmak mümkündür. Bütün Konica Minolta erişim kontrolü ve güvenlik işlevleri yalnızca maddi ve itibara yönelik zarar tehditlerine karşı daha güçlü bir savunma teşkil etmekle kalmaz, aynı zamanda daha iyi bir yönetim ve izlenebilirliğin temel taşı olarak kullanılabilir.

VERİ VE BELGELER İÇİN **KAPSAMLI GÜVENLİK**

MFP'ler ve yazıcılar genellikle personel, müşteri ya da ziyaretçilerin kolayca erişebilecekleri ortak kullanım alanlarında yer aldığından gerekli veri güvenlik politikalarının uygulanması bir zorunluluktur. MFP sabit diskinde bir süre saklanan hassas veri ile MFP tepsisinde çıktı olarak bekleyen belgeler kolaylıkla yanlış kişilerin eline geçebilir. Konica Minolta bundan kaçınmak ve tam kapsamlı belge/veri güvenliğini sağlamak amacıyla müşteriye özel güvenlik önlemleri sunmaktadır.

HDD (Sabit Disk Sürücüsü) Güvenliği ile Boşluklar Dolduruluyor

Birçok yazıcı ve MFP'lerde uzun kullanım süreleri boyunca toplanmış gigabitler dolusu bilgiyi saklayabilecek sabit diskler ve bellekler bulunmaktadır.

Bunlar arasında yer alması muhtemel hassas kurumsal bilginin korunmasına yönelik güvenilir koruma sistemleri mutlaka oluşturulmalıdır. Konica Minolta sistemlerinde çok sayıda örtüşen ve iç içe geçen özellik bu güvenceyi sağlamaktadır:

- **Otomatik Silme İşlevi**
  Otomatik silme işlevi, sabit disk üzerinde saklanan veriyi önceden belirlenmiş dönemlerde siler.

- **Dahili HDD'nin Şifre ile Korunması**
  HDD çıkarıldıktan sonra sabit disk üzerindeki gizli ve özel bilgileri de içeren verinin okunması için bir şifre belirlenebilir. Şifre cihazla eşleştirilmiştir. Böylece HDD cihazdan çıkarıldıktan sonra üzerindeki bilgiye erişim mümkün değildir.

- **HDD Üzerine Verinin Yeniden Yazılması**
  Bir sabit sürücünün formatlanmasında en güvenli seçenek HDD üzerine verinin yeniden yazılmasıdır. Bu da çok sayıda standarda uygun şekilde yapılır.

- **HDD Kriptolama**
  Konica Minolta cihazlarındaki HDD'ler üzerindeki veri 128-bit'lik bir kriptolama algoritması kullanılarak saklanabilmektedir. Bu özellik, kurumsal veri koruma politikalarını en iyi şekilde gerçekleştirmektedir. Kriptolanmış bir HDD üzerindeki veri, HDD MFP'den fiziksel olarak çıkarılsa bile okunamaz/çekilemez.

Belgelerin Güvenli Baskı ile Korunması

Çıktı cihazlarına ilişkin güvenlik riskini göz ardı etmek hata olur: en basit seviyede, çıktı tepsisinde bekleyen belgeler, o sırada civarda bulunan kişilerce bile görülebilir ve hatta okunabilir. Yetkisi bulunmayan kişilerin gizli bilgilere erişiminin daha kolay bir yolu yoktur. Güvenli baskı işlevi, basılacak her belge için kullanıcı tarafından bir şifre oluşturulmasını gerektirdiğinden belge güvenliğini garanti etmektedir. Baskı işlemi, ancak şifre çıktı cihazına girildikten sonra başlayacaktır. Bu, gizli belgelerin yanlış kişilere ulaşmasını engellemenin basit ancak etkin bir yoludur.

Bireysel Doğrulama ile Baskı

Touch & Print sistemi parmak dokusu tarayıcı ya da kimlik kartı okuyucusu ile doğrulama yapmaktadır. Çıktısı alınmak istenen belgenin baskı işlemi, kullanıcı kimlik kartını kart okuyucusuna okutma ya da parmak damarı taraması ile MFP'de doğrulama yapar yapmaz başlamaktadır. Bu özelliğin avantajı hızlı olmasıdır: Güvenli baskı için kimlik ve şifre ihtiyacını ortadan kaldırarak süreci hızlandırır.

Yetkisiz Baskının Engellenmesi

Kopya güvenliği özelliği, baskı sırasında çıktı ve kopyalara bir filigran ekler. Orijinal çıktıda gözle görülmesi neredeyse imkânsız olan filigran, belge kopyalanmak istendiğinde arka plandan ön plana çıkarak bunun bir kopya olduğunu belirtir.

Kopya Koruması ile Kontrol Sizde

Kopya Koruması/Kopyalama Şifresi, bir belgenin kopyalanmasını engellemek üzere baskı sırasında orijinal belge üzerine bir filigran eklemektedir. Korumalı orijinal üzerinde neredeyse görünmez olan bu filigran, söz konusu belgenin kopyalanması seçeneğini bloke eder. Kopyalama Şifresi özelliği Kopya Koruması'nı geçersiz kılar ve MFP paneline doğru şifre girildiğinde sistem kopyalama işlemine izin verir.

PDF'lerde Akıllı Kriptolama

Kriptolanmış PDF'ler bir kullanıcı şifresi ile korunmaktadır: PDF'i basma, kopyalama ya da içerik ekleme izni, MFP üzerinde tarama esnasında yapılandırılabilir.

PDF Dijital İmzası

Bu özellikle, PDF'e tarama sırasında bir dijital imza eklenebilmektedir. Bu özellik, bir PDF yazıldıktan sonra yapılan değişiklikleri izlemek için de kullanılabilir.

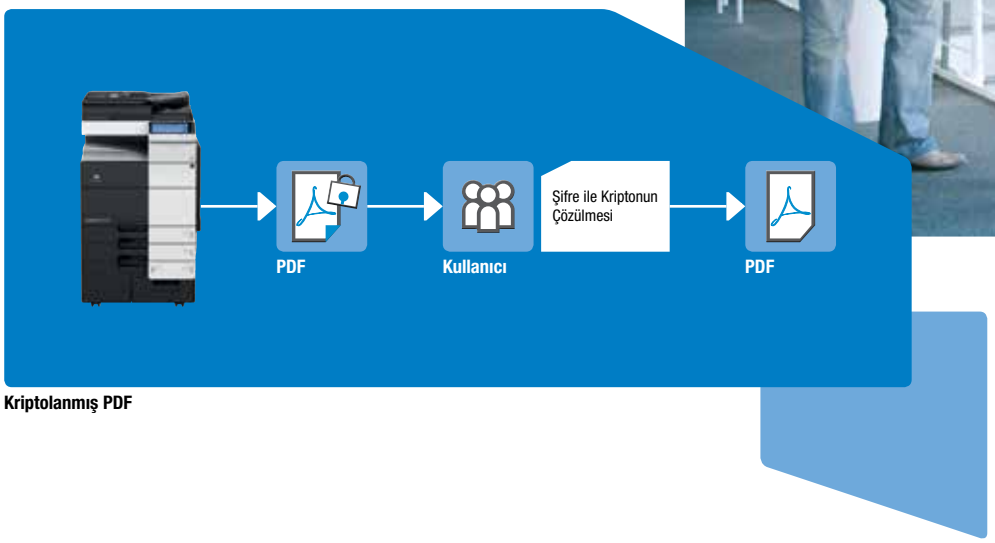
Güvenli Faks Alma

Aktive edildiğinde, alınan tüm fakslar korumalı kullanıcı kutusunda saklanabilir.

Kullanıcı Kutusu Güvenliği

Bireysel ya da grup bazında yapılandırılabilen kullanıcı kutuları, belgelerin çıktısı alınmadan önce MFP sabit diskinde güvenle saklanmasına olanak sağlar.

Kullanıcı kutuları 8 basamaklı bir alfa numerik şifre ile korunabilir. Doğru şifre girildiğinde, kutudaki belgelere erişmek/görüntülemek mümkündür. Bu sistem gizli belge ve veriye yetkisiz erişimi etkin şekilde sınırlamaktadır.



Kriptolanmış PDF

AĞINIZI KORUYUN

İletişim ve bağlanabilirlik günümüz iş dünyasının vazgeçilmezleri. Konica Minolta'nın ofis cihazları bu gerçeği dikkate alarak ağ ortamlarına kolay entegrasyonu sağlayacak sistemlerle donatılmıştır. Bildiğiniz gibi ağ yazıcıları ve çok işlevli ofis ekipmanları (MFP) baskı, fotokopi, ağ üzerinde belge/veri tarama, e-posta gönderme gibi özellikleri bünyesinde barındıran sofistike birer belge-işlem merkezi haline geldi.

Bu ve benzeri yapılanmalar, teknoloji güvenliği sağlanmadığı takdirde, ofisiniz için risk oluşturmaktadır. İşte bu sebeple, herhangi bir ağ aygıtında karşılaşacağınız güvenlik tehditleri ve politikaları bu sistemler için de geçerlidir. Gerek iç gerekse dış ağ saldırılardan kaynaklanabilecek tehlikelere karşı önlem almak gerekmektedir. Konica Minolta tüm cihazlarınızın güvenliğini, en katı güvenlik standartlarıyla uyumlu çok sayıda önlem alarak garanti etmektedir. Bu önlemler arasında şunlar sayılabilir:

IP Adresini Bloke Etmek

IP adresini filtreleme yeteneği bulunan bu temel sistem içi güvenlik duvarı ile protokol ve port erişimini kontrol edebilirsiniz.

Port Yönetimi

Sistem yöneticiniz port ve protokolleri doğrudan makina üzerinde ya da işlem kolaylığı açısından uzak bir lokasyondan açabilir, kapatabilir, etkinleştirebilir ya da devre dışı bırakabilir.

Güvenli E-Posta İletişimi

Konica Minolta MFP'lerinin büyük bir kısmında, MFP'den belirtilen alıcılara giden e-postaların güvenliğini sağlamak amacıyla S/MIME (çok amaçlı internet posta uzantılarının güvenliği) bulunmaktadır. S/MIME e-postaları ve içeriğini bir güvenlik sertifikası ile kriptolayarak e-posta trafiğinizi güvence altına alır.

Ağ Doğrulama

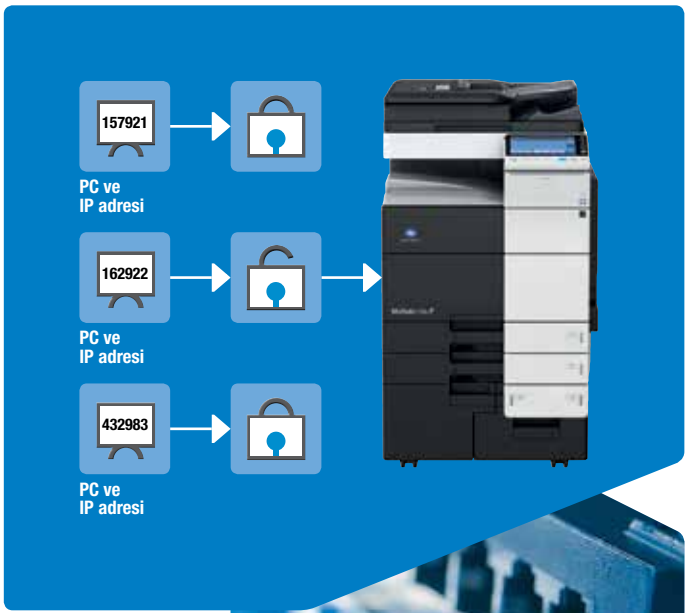
IEEE802.1x ailesinde tanımlanan standartlar WAN ve LAN'lara ağ erişimi kontrolünü sağlayan, geçerliliği kabul edilmiş port-temelli doğrulama standartlarıdır. Bu standartlar doğrulama talepleri dışında her türlü ağ iletişimini (DHCP ya da HTTP) yetkilendirilmemiş cihazlara kapatarak ağınızı etkin şekilde korur.

İletişimin Korunması

Bu protokol size, örneğin çevrim içi yönetim araçları ve Windows Active Directory aktarımı dahil olmak üzere, cihazlar üzerinden gönderilen ve alınan tüm iletişim modellerinde koruma sağlar.

Kriptolu Ağ İletişimi

Ayrıca, bizhub cihazlarının büyük bir kısmı MFP'leriniz üzerinden gönderilen ya da alınan her türlü ağ verisini kriptolamak amacıyla IPsec uygulamasını desteklemektedir. IP güvenlik protokolü, yerel İntranetiniz (sunucu, müşteri bilgisayarı) ile cihazlarınız arasındaki her türlü ağ iletişimini kriptolar.



IP adresi filtreleme

Konica Minolta Turkey İş Teknolojileri A.Ş.
Genel Müdürlük: Şerifali Mah. Barbaros Cad. Hattat Sok. No:19 34775 Ümraniye / İstanbul T: +90 216 528 56 56 F: +90 212 253 49 69
Antalya Bölge Ofisi: Kızılsaray Mah. 88. Sok. Mustafa Korkut Apt. No:10/2 Muratpaşa / Antalya T: +90 242 248 39 49 - 248 74 14 F: +90 242 248 55 14