



KONICA MINOLTA

SECURITY

✓ Informatieveiligheid volgens Konica Minolta:
ver vooruit op de standaard

Wereldwijde communicatie heeft een ongekennde groei doorgemaakt. Daarmee is ook de kans op aanvallen en inbreuken op de veiligheid van bedrijfsdata sterk gestegen. In zakelijke omgevingen vormen kopieer-, print-, scan- en faxsystemen een essentieel onderdeel van de werkprocessen. Steeds vaker vervullen MFP's (multifunctionals) deze hoofdrol. Het is dan ook zaak om deze systemen goed te beveiligen en securitybedreigingen het hoofd te bieden.





KONICA MINOLTA'S BEVEILIGINGSSTANDAARDEN

Op het gebied van informatieveiligheid is Konica Minolta de onbetwiste marktleider. Met een uitgebreid aantal standaardbeveiligingsfuncties en tal van aanvullende opties zorgen we ervoor dat vertrouwelijke bedrijfsdata vertrouwelijk blijft. Onze professionele beveiligingsoplossingen signaleren niet alleen inbreuk op de beveiliging, maar voorkomen het ook. Zo kan gevoelige informatie nooit uitlekken en voor financiële en/of reputatieschade zorgen.

MFP's bieden zo veel enkelvoudige en gecombineerde functies en keuzes dat er beveiligingslekken kunnen ontstaan. Een afdoende MFP-beveiliging is dan vereist. Konica Minolta hanteert drie hoofdcategoryën:

- Toegangsbeheer / toegangsbeveiliging
- Gegevensbeveiliging / documentbeveiliging
- Netwerdbeveiliging

Alle beveiligingsfuncties van Konica Minolta op een rij

Toegangsbeheer / toegangsbeveiliging	Copy/print accounting Functiebeperking Beveiligd printen (taakvergrendeling) Beveiliging van de gebruikersbox via wachtwoord Gebruikersauthenticatie (ID + wachtwoord) Vingeraderherkenning IC-kaartauthenticatie Eventlog
Document- en gegevensbeveiliging	HDD-encryptie Overschrijven van HDD-data HDD-vergrendeling via wachtwoord Automatische verwijdering van tijdelijke data
Netwerbbeveiliging	Blokkering IP-adres Poortuitschakeling SSL/TLS-communicatie IPsec-ondersteuning S/MIME IEEE 802.1x-ondersteuning
Beveiligd scannen	Gebruikersauthenticatie POP voor SMTP SMTP-authenticatie (SASL) Handmatige bestemmingsblokkering
Overige	Beveiliging servicemodus Beveiligde administrator modus Vastlegging gegevens Blokkering van onbevoegde toegang Beveiliging tegen kopiëren via watermerk Versleutelde PDF Digitale PDF-handtekening PDF-encryptie Kopieerbewaking/wachtwoord kopiëren

HELDERE CRITERIA: ISO 15408 EAL3

Veel Konica Minolta-systemen zijn gecertificeerd conform de Algemene Criteria/ISO 15408 EAL3-normen. Dit zijn de (enige) internationaal erkende normen op het gebied van IT-beveiligingstests voor digitale kantoorssystemen.

Printers, kopieersystemen en software die voldoen aan de ISO 15408 EAL3-certificering, hebben een strenge beveiligingsevaluatie doorlopen en bieden een solide beveiliging, waarop organisaties volledig kunnen bouwen. Konica Minolta is toonaangevend in de ontwikkeling van standaardbeveiligingsfuncties.



Common Criteria Validated

“Beveiliging is het belangrijkste element binnen de strategie van Konica Minolta...”

Konica Minolta beschikt over een uitgebreide reeks aan print- en documentbeveiligingsfuncties. Veel daarvan zitten standaard op de bizhubs. Het gaat dus niet om optionele beveiligingssets. Daarmee heeft Konica Minolta het grootste assortiment in volledig ISO15408-gecertificeerde MFP's die er in de markt verkrijgbaar is.”

Bron: Quocirca (2011), marktonderzoek “Closing the print security gap. The market landscape for print security”, pag. 11. Dit onafhankelijke rapport is opgesteld door Quocirca Ltd., een onderzoeks- en analysebedrijf dat gespecialiseerd is in de zakelijke impact van informatie-technologie en communicatie.



TOEGANGSBEHEER EN TOEGANGSBEVEILIGING

Hoewel beveiliging vaak hoog op de agenda staat binnen publieke en commerciële organisaties, wordt het beveiligingsrisico van MFP's vaak onderschat. Sommige risico's worden onderkend, maar tegelijkertijd vaak verwaarloosd – en dat terwijl het gaat om vertrouwelijke documenten en informatie. Vooral MFP's en printers die zich in openbare ruimtes bevinden en toegankelijk zijn voor medewerkers en bezoekers, behelzen een mogelijk gevaar.

De eerste logische stap is voorkomen dat onbevoegden de MFP kunnen bedienen – een preventie maatregel om de toegang tot MFP's te beheeren. Eerste logische stap is om te voorkomen dat onbevoegden de MFP kunnen bedienen – een preventieve maatregel dus om de toegang tot MFP's te beheeren. Daarnaast moet er een beveiligingsbeleid worden opgesteld, waarin staat hoe de systemen in de praktijk worden gebruikt. Konica Minolta zorgt voor afdoende maatregelen, zonder dat de gebruiksvriendelijkheid van de systemen in het geding komt.

Gebruikersauthenticatie: Wie bent u?

De weg naar authenticatie begint met het opstellen van een beleid dat vastlegt welke (groepen) gebruikers de MFP's mogen bedienen. Sommige gebruikers hebben volledige toestemming en toegang, andere gebruikers hebben beperkte toegangsrechten en kunnen niet alle functies gebruiken.

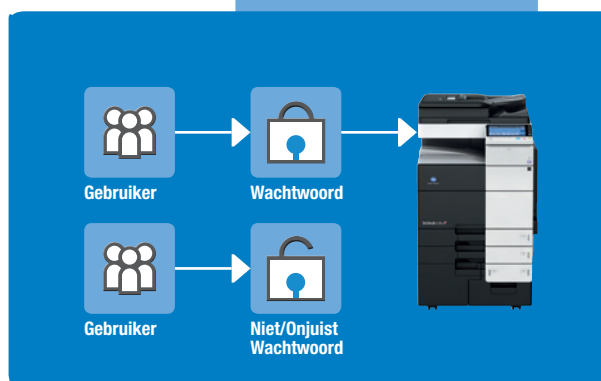
Konica Minolta biedt drie basistechnologieën voor gebruikersauthenticatie:

1. Persoonlijk wachtwoord

Het wachtwoord – een alfanumerieke code van maximaal 8 tekens – moet worden ingevoerd op het bedieningspaneel van de MFP. Deze codes kunnen worden aangemaakt voor beheerders en gebruikers. Belangrijk aspect is dat ze centraal kunnen worden beheerd.

2. IC-kaartauthenticatie

De meeste Konica Minolta-systemen kunnen worden uitgerust met een IC-kaartlezer. Deze zijn ontworpen voor gemak en snelheid. Wie de IC-kaart op of naast de lezerinterface houdt, kan de MFP gebruiken.



Gebruikersauthenticatie



3. Vingeraderherkenning

De geavanceerde methode van vingeraderherkenning heeft een grote meerwaarde vergeleken met de veelgebruikte vingerafdrukscanners. Dit systeem vergelijkt namelijk de afbeelding van de gescande vingeraderpatronen met de afbeeldingen in het geheugen. Vingeraders zijn biometrisch en niet te vervalsen. Dit is dus dé manier om een persoon te identificeren op basis van een individueel fysiek kenmerk. In tegenstelling tot vingerafdruksystemen kunnen vingeraders niet worden gescand zonder dat de persoon daadwerkelijk aanwezig is. Dankzij de vingeraderherkenning hoeven mensen geen wachtwoorden te onthouden of pasjes bij zich te dragen.

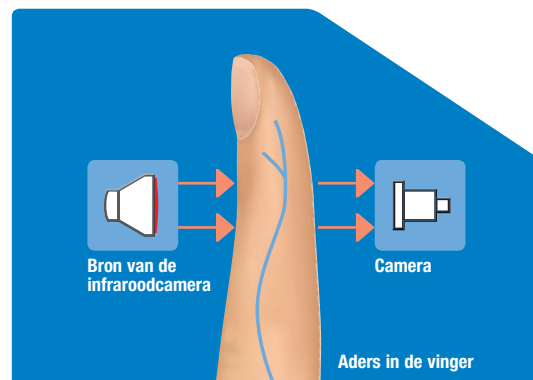
De authenticatiegegevens kunnen worden opgeslagen op de MFP (versleuteld) of ze kunnen uit de bestaande gegevens in de Windows Active Directory worden gehaald. Omdat toegangs- en gebruikersgegevens voortdurend voor elk afzonderlijk systeem worden vastgelegd, worden aanvallen en inbreuken meteen ontdekt en gemeld.

■ Bijhouden van accounts

Omdat elke gebruiker zich moet aanmelden op de MFP, vormen de verzamelde gegevens een efficiënte manier om de beveiliging op een aantal niveaus in de gaten te houden. Bijvoorbeeld per gebruiker, groep of afdeling. Welke van de systeemfuncties ook wordt gebruikt – kopiëren in zwart-wit of kleur, scannen of faxen, afdrukken in zwart-wit of kleur – alles kan individueel worden bijgehouden, zowel binnen het systeem als op afstand. Analyses van deze gegevens bieden u waardevolle informatie over het gebruik van de MFP vanuit verschillende perspectieven. U kunt de gegevens bijvoorbeeld toepassen om de naleving van het beleid in de gaten te houden en om onbevoegde toegang aan het licht te brengen. Bovendien kunt u het gebruik van alle printers en MFP's in de zakelijke omgeving monitoren.

■ Afschermen van functies

Het is mogelijk om bepaalde functies van de MFP voor individuele gebruikers af te schermen. De functies voor toegangsbeheer en beveiliging van Konica Minolta bieden hierdoor grote bescherming tegen oneigenlijk gebruik en voorkomen daarmee mogelijke financiële of reputatieschade.



Prima geregeld

DOCUMENT- EN GEGEVENSBEVEILIGING



Omdat MFP's en printers vaak in openbare ruimtes staan en toegankelijk zijn voor medewerkers en bezoekers, is het essentieel om slimme beveiligingsmaatregelen te nemen. In situaties waarin vertrouwelijke gegevens bijvoorbeeld worden opgeslagen op de harddisk van de MFP, of wanneer vertrouwelijke documenten in de uitvoerlade van de MFP liggen, zijn gegevens niet beschermd en kunnen ze in verkeerde handen vallen. Konica Minolta kent verschillende beveiligingsvoorzieningen, die document- en dataveiligheid garanderen.

■ bizhub SECURE

De meeste printers en MFP's zijn uitgerust met harddisks en een geheugen waarin gigabytes aan vertrouwelijke data – over een lange periode verzameld – worden opgeslagen. Het is dus belangrijk om betrouwbare beveiligingsmaatregelen te treffen die de veiligheid van gevoelige informatie waarborgen. Konica Minolta biedt hiervoor bizhub SECURE, een behapbaar pakket aan beveiligingsoplossingen waarmee u doeltreffend alle data op de harddisk (HDD) afschermt en beschermt.

– Wijziging administrator password

Met het instellen van een administrator password schermt u het beheergedeelte van de MFP af voor overige gebruikers.

– Automatische verwijdering van tijdelijke data

Met de functie 'automatisch verwijderen' kunnen gegevens op de harddisk na een bepaalde periode volledig worden gewist.

– HDD-vergrendeling via een wachtwoord

Is de harddisk verwijderd, dan kan deze alleen nog worden gelezen door het invoeren van een wachtwoord. Het wachtwoord is gekoppeld aan het systeem en de gegevens zijn dus niet meer toegankelijk na verwijdering van de harddisk.

– Overschrijven van HDD-data op basis van tijdsinstelling

De veiligste methode om een harddisk te formatteren, is door de gegevens te overschrijven. Dit wordt gedaan volgens vooraf vastgestelde normen.

– HDD-encryptie

Op de harddisks waarmee Konica Minolta-systemen zijn uitgerust, kunnen gegevens versleuteld worden opgeslagen. Dit gebeurt op basis van een versleutelings-systeem met een 128-bits algoritme. Deze functie voldoet volledig aan een stringent beveiligingsbeleid. Zodra de harde schijf versleuteld is, kunnen de gegevens niet worden gelezen, zelfs niet als de harde schijf uit de MFP wordt verwijderd.

■ Beveiligd printen

Uitvoersystemen zoals MFP's vormen in principe een beveiligingsrisico: iedereen kan de documenten in de uitvoerlade bekijken. Er is geen eenvoudigere manier voor onbevoegden om toegang te krijgen tot vertrouwelijke informatie. De functie 'beveiligd printen' zorgt ervoor dat documenten beveiligd blijven, omdat de persoon die de afdrukopdracht uitvoert een wachtwoord moet instellen vóórdat er kan worden afgedrukt. Wie wil afdrukken, moet het wachtwoord rechtstreeks op het uitvoersysteem intoetsen, anders wordt de opdracht niet afgedrukt. Een eenvoudige en effectieve manier om te voorkomen dat vertrouwelijke documenten in verkeerde handen vallen.



Touch & Print/ID & Print

'Touch & Print' is gebaseerd op authenticatie door middel van vingeraderherkenning of met een IC-kaartlezer. Voor gebruikersauthenticatie via ID & Print daarentegen is een ID en een wachtwoord vereist. Het afdrukken van de opdracht kan worden uitgevoerd op het systeem, maar alleen nadat de gebruiker bij de MFP is geverifieerd door een IC-kaart voor de kaartlezer te houden, of door een ID-bevestiging met vingeraderherkenning. Het voordeel van deze functie is dat er geen behoefte meer is aan een extra ID en een wachtwoord voor beveiligd afdrukken.

Digitale PDF-handtekening

Met deze functie kan tijdens het scannen een digitale handtekening worden toegevoegd aan de PDF. Nadat de PDF is gemaakt, kunnen eventuele wijzigingen worden bijgehouden.

Faxen ontvangen

Wanneer deze functie is geactiveerd, kunnen ontvangen faxberichten vertrouwelijk worden opgeslagen in een beveiligde gebruikersbox.

Beveiliging tegen kopiëren

De functie 'beveiliging tegen kopiëren' voegt tijdens de afdrukprocedure een watermerk toe aan prints en kopieën. Het watermerk is nauwelijks zichtbaar op de originele afdruk, maar wordt het document gekopieerd, dan komt het watermerk naar voren om aan te geven dat het om een kopie gaat.

Kopieerbewaking/wachtwoord kopiëren

Deze functie voegt tijdens het afdrukken een verborgen watermerk toe aan het originele document om te voorkomen dat er kopieën van het document worden gemaakt. Het watermerk is bijna niet zichtbaar op het originele document. Nogmaals afdrukken is niet mogelijk, omdat het systeem door het watermerk meteen blokkeert. De functie 'wachtwoord kopiëren' heeft voorrang op de functie 'kopieerbewaking'. Wordt het juiste wachtwoord ingevoerd op het bedieningspaneel van de MFP, dan kan het document met watermerk alsnog worden gekopieerd.

Beveiliging van de gebruikersbox

Gebruikersboxen zijn bedoeld voor personen en groepen om documenten veilig op te slaan op de harddisk van de MFP, voordat de print- of kopieeropdracht wordt uitgevoerd. Gebruikersboxen kunnen worden beschermd met een alfanumeriek wachtwoord van acht tekens. Wordt het juiste wachtwoord ingevoerd, dan zijn alle documenten in de gebruikersbox toegankelijk. Dit effectieve systeem zorgt ervoor dat vertrouwelijke documenten en gegevens alleen voor bevoegde personen toegankelijk zijn.

PDF-encryptie

Versleutelde PDF's zijn beschermd met een gebruikerswachtwoord: tijdens de scanprocedure op de MFP kan de toestemming om een PDF te printen of te kopiëren worden ingesteld.



PDF



Gebruiker



Decoderen met wachtwoord



PDF

NETWERKBEVEILIGING

Communicatie en connectiviteit zijn essentieel in de bedrijfsomgeving. Konica Minolta biedt systemen die geheel probleemloos aansluiten op de netwerkomgeving. Onze netwerkprinters en MFP's zijn zodanig doorontwikkeld dat ze kunnen fungeren als geavanceerde en geïntegreerde documentverwerkingshubs binnen een netwerk – met mogelijkheden van afdrucken, kopiëren en scannen tot en met distributie naar een netwerkbestemming of verzending als e-mail. Dit houdt wel in dat deze technologie ook de beveiligingstoets moet kunnen doorstaan en moet voldoen aan hetzelfde beveiligingsbeleid als alle andere netwerk-systemen. Geen beveiliging vormt een te groot risico. Om zowel interne als externe aanvallen op het netwerk te voorkomen, zorgt Konica Minolta dat alle systemen voldoen aan de strengste beveiligingsnormen. Daarvoor bieden we onder meer de volgende mogelijkheden:

■ Blokkering IP-adres

Een interne basisfirewall biedt de mogelijkheid om IP-adressen te filteren en de toegang tot protocollen en poorten te beheren.

■ Poortuitschakeling

In de beheermodus kunnen poorten en protocollen worden geopend, gesloten, ingeschakeld en uitgeschakeld. Dit kan rechtstreeks op het systeem of op afstand.

■ S/MIME

De meeste MFP's van Konica Minolta ondersteunen S/MIME (secure/multipurpose internet mail extensions) om de communicatie via e-mail van de MFP naar geselecteerde ontvangers te beveiligen. S/MIME beveiligt het e-mailverkeer door het e-mailbericht en de inhoud ervan te versleutelen met een beveiligingscertificaat.

■ SSL/TLS-communicatie

Het SSL/TLS-protocol beveiligt de communicatie van en naar het systeem met bijvoorbeeld online beheertools en Windows Active Directory-overdrachten.

■ IPsec-ondersteuning

De meeste bizhub-systemen bieden ook IPsec-ondersteuning om te zorgen dat alle netwerkgegevens die van en naar een MFP worden verzonden, volledig zijn beveiligd. Het IP-beveiligingsprotocol versleutelt alle netwerkcommunicatie tussen het lokale intranet (server, client-pc) en het systeem zelf.

■ IEEE 802.1x-ondersteuning

De standaarden die worden beschreven in de IEEE802.1x-familie, zijn de erkende, op poorten gebaseerde authenticatiestandaarden voor beheer van netwerktoegang voor WAN's en LAN's. Deze standaarden zorgen ervoor dat het netwerk is beveiligd door eventuele netwerkcommunicatie (bijv. DHCP of HTTP) met onbekende systemen uit te schakelen – authenticatieverzoeken daargelaten.

