



KONICA MINOLTA

SICHERHEIT

✓ Konica Minoltas branchenführende Sicherheitsstandards

Im digitalen Zeitalter hat die weltweite Kommunikation rasant zugenommen – und damit auch das Potenzial für Sicherheitsverstöße. In einer Geschäftsumgebung ist der Einsatz von Multifunktionssystemen (MFPs) aufgrund der täglichen Nutzung von Kopier-, Druck-, Scan- und Faxfunktionen als Grundkomponenten von Arbeitsabläufen auf vielen Ebenen unverzichtbar. Daher ist es sehr wichtig, dass diese Systeme vor ständigen Sicherheitsbedrohungen geschützt werden.





KONICA MINOLTAS SICHERHEITSSTANDARDS

Konica Minoltas breite Palette von Standardsicherheitsfunktionen und -optionen bildet eine leistungsfähige Basis für professionelle Lösungen – zur Erkennung und Verhinderung von Sicherheitsverstößen sowie zur Vermeidung finanzieller Folgeschäden oder Rufschädigungen auf geschäftlicher und privater Ebene. Konica Minolta hat auf diesem Gebiet Pionierarbeit geleistet und ist weiterhin Branchenführer.

MFPs bieten generell ein breites Spektrum von kombinierten Funktionen sowie Einzelfunktionen und -optionen und beinhalten daher ein ebenso breites Spektrum potenzieller Sicherheitslücken. Die in MFPs integrierten Sicherheitsfunktionen lassen sich in drei Bereiche gliedern:

- **Zugriffssteuerung/Zugriffssicherheit**
- **Datensicherheit/Dokumentensicherheit**
- **Netzwerksicherheit**

▀ Konica Minoltas Sicherheitsfunktionen auf einen Blick

Zugriffssteuerung	Kopier-/Druckkostenabrechnung Funktionseinschränkung Sicheres Drucken (gesperrte Druckaufträge) Kennwortschutz für Benutzerboxen Benutzerauthentifizierung (ID + Kennwort) Fingervenenscanner IC-Kartenleser Ereignisprotokoll
Datensicherheit	Datenverschlüsselung (Festplatte) Überschreiben von Festplattendaten Kennwortschutz für Festplatte Automatisches Löschen von Daten
Netzwerksicherheit	IP-Filter Port- und Protokollzugriffssteuerung SSL/TLS-Verschlüsselung (HTTPS) IP sec-Unterstützung S/MIME 802.1x-Unterstützung
Scansicherheit	Benutzerauthentifizierung POP vor SMTP SMTP-Authentifizierung (SASL) Sperren der manuellen Zieleingabe
Sonstige	Servicemodusschutz Administratormodusschutz Datenerfassung Sperrung unberechtigten Zugriffs Kopierschutz durch Wasserzeichen Verschlüsselte PDF PDF-Signatur PDF-Verschlüsselung durch digitale ID Kopiersperre/Kopieren mit Kennwort

GEMEINSAME KRITERIEN UND ISO 15408 EAL3

Die Bürosysteme von Konica Minolta sind fast ausnahmslos nach den Gemeinsamen Kriterien/der Norm ISO 15408 EAL3 zertifiziert.

Dies sind die einzigen international anerkannten Normen für die Prüfung und Bewertung der Sicherheit von Informationstechnik. Gemäß ISO 15408 EAL3 zertifizierte Drucker, Kopierer und Softwareprodukte haben eine strenge Sicherheitsprüfung bestanden und bieten das Sicherheitsniveau, das ein sicherheitsbewusstes Unternehmen anstreben sollte und zurecht erwarten kann.

Konica Minolta ist Branchenführer und setzt die Maßstäbe für Standardsicherheitsfunktionen!



Common Criteria Validated

„Sicherheit ist das Hauptelement der Gesamtstrategie von Konica Minolta...

Konica Minolta bietet eine breite Palette von Druck- und Dokumentensicherheitsfunktionen, von denen viele standardmäßig in die bizhub-Serie integriert sind. Statt optionale Sicherheitspakete zertifizieren zu lassen, kann Konica Minolta für sich in Anspruch nehmen, das größte Angebot an ISO 15408-zertifizierten MFPs am Markt bereitzustellen“

Quelle: Quocirca (2011), Marktstudie "Closing the print security gap. The market landscape for print security", S. 11. Diese unabhängige Studie wurde von Quocirca Ltd. durchgeführt, einem Marktforschungsunternehmen, das sich auf die geschäftlichen Auswirkungen von IT-Technologie und -Kommunikation (ITC) spezialisiert hat.



ZUGRIFFSSTEUERUNG/ ZUGRIFFSSICHERHEIT

Obwohl Sicherheitsfragen sowohl im öffentlichen Sektor als auch bei Unternehmen große Bedeutung beigemessen wird, wird das mit MFPs verbundene Sicherheitsrisiko oft völlig übersehen. Manche Risiken werden vielleicht erkannt, aber dennoch vernachlässigt, insbesondere wenn es um sensible Dokumente und Informationen geht. Das ist besonders bei MFPs und Druckern riskant, die sich in öffentlichen Bereichen befinden und Mitarbeitern, Lieferanten und sogar Besuchern zugänglich sind.

Dank der anspruchsvollen Funktionen moderner MFPs können Informationen problemlos unternehmensweit und über die physischen und virtuellen Grenzen des Unternehmens hinaus kopiert und verteilt werden. Der erste logische Schritt besteht darin, die Nutzung eines MFPs durch Unbefugte zu verhindern. Dazu sind zum einen Schutzmaßnahmen zur Steuerung des Zugriffs auf MFPs und zum anderen Sicherheitsrichtlinien bezüglich der Nutzung der Systeme im Arbeitsalltag erforderlich. Konica Minolta erreicht dies, ohne die Benutzerfreundlichkeit der Systeme einzuschränken.

Benutzerauthentifizierung

Der Authentifizierungspfad beginnt mit der Festlegung einer Richtlinie, aus der hervorgeht, welche Benutzer und Benutzergruppen mit einem MFP arbeiten dürfen. Dies kann Einschränkungen der Zugriffsrechte beinhalten; das heißt, es kann festgelegt werden, dass manche Benutzer bestimmte Funktionen, wie beispielsweise Farbdruck, nutzen können und andere nicht.

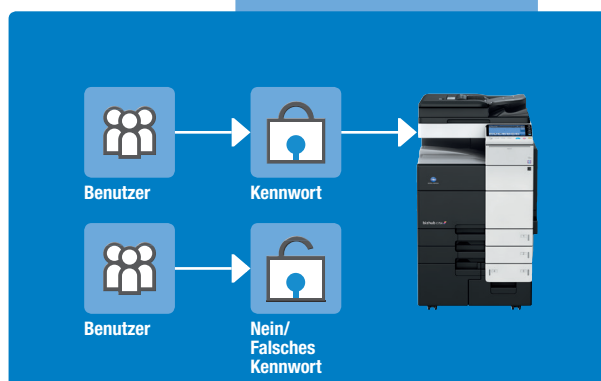
Konica Minolta stellt drei Basistechnologien für die Benutzerauthentifizierung bereit:

1. Persönliches Kennwort:

Das Kennwort, ein maximal 8 Zeichen umfassender alphanumerischer Code, wird am Bedienfeld des MFP eingegeben. Diese Codes können für Administratoren und Benutzer festgelegt werden. Ein wichtiger Aspekt ist die Möglichkeit der zentralen Verwaltung.

2. IC-Kartenauthentifizierung

Die meisten Systeme von Konica Minolta können mit einem IC-Kartenleser ausgestattet werden. Diese Geräte ermöglichen eine rasche und bequeme Authentifizierung, bei der lediglich die IC-Karte auf dem Leser oder in der Nähe des Lesers zu platzieren ist.



Benutzerauthentifizierung



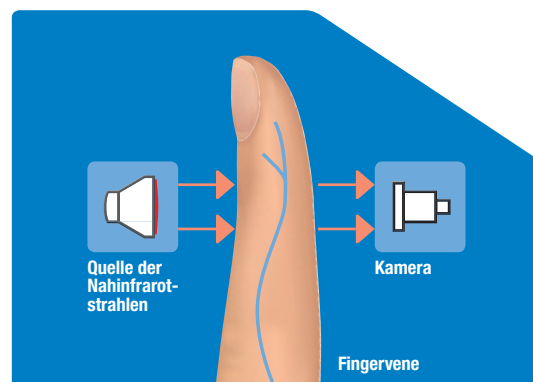
3. Biometrischer Fingervenenscanner

Dieses hochmoderne Gerät stellt eine Weiterentwicklung gegenüber herkömmlichen Fingerabdruckscannern dar. Seine Funktionsweise basiert auf dem Vergleich des Bildes gescannter Fingervenenumuster mit im Speicher vorhandenen Bildern. Die Fingervene ist eine praktisch nicht fälschbare biometrische Information und stellt somit ein zur Identifizierung einer Person geeignetes Merkmal dar. Im Gegensatz zu einem Fingerabdruck kann eine Fingervene nicht gescannt werden, ohne dass die betreffende Person physisch anwesend und am Leben ist. Der biometrische Fingervenenscanner macht das Einprägen von Kennwörtern oder Mitführen von Karten überflüssig.

Die Authentifizierungsinformationen können entweder (verschlüsselt) auf dem MFP gespeichert oder aus dem Windows Active Directory abgerufen werden. Aufgrund der kontinuierlichen Datenprotokollierung in Bezug auf Zugriff und Nutzung eines Geräts werden Sicherheitsverstöße sofort erkannt und markiert.

■ Kostenstellenverwaltung

Da sich jeder Benutzer gemäß den Benutzerverwaltungs- bzw. Sicherheitsrichtlinien beim Ausgabegerät anmelden muss, ergibt sich aus den daraus generierten Daten eine effiziente Überwachungsmöglichkeit auf Benutzer-, Gruppen- und/oder Abteilungsebene. Alle genutzten Funktionen, sei es Schwarzweiß- oder Farbkopieren, Scannen oder Faxen, Schwarzweiß- oder Farbdruck, können am System oder per Fernzugriff einzeln nachverfolgt werden. Aus der Analyse dieser Daten ergeben sich zuverlässige Informationen bezüglich verschiedener Aspekte der MFP-Nutzung, sodass die Einhaltung der Richtlinien forciert und unberechtigter Zugriff nachverfolgt und vor allem die Nutzung der gesamten Drucker- und MFP-Flotte in der Unternehmens- bzw. Büroumgebung überwacht werden kann.



■ Funktionssteuerung/ Funktionseinschränkung

Verschiedene MFP-Funktionen können für einzelne Benutzer eingeschränkt werden. Alle Zugriffssteuerungs- und Sicherheitsfunktionen von Konica Minolta bieten nicht nur größere Sicherheit vor Bedrohungen, die finanzielle Schäden oder Rufschädigung nach sich ziehen können, sondern können auch als Grundlage für bessere Kontrolle und Nachprüfbarkeit dienen.

DOKUMENTEN-/DATEN-SICHERHEIT

Angesichts der Tatsache, dass sich MFPs und Drucker oft in öffentlichen Bereichen befinden, wo sie Mitarbeitern, Lieferanten und Besuchern zugänglich sind, müssen geeignete Datensicherheitsrichtlinien zur Anwendung kommen. Andernfalls könnten vertrauliche Daten, die beispielsweise eine gewisse Zeit auf der Festplatte des MFPs gespeichert werden oder in gedruckter Form im Ausgabefach des MFPs liegen, in falsche Hände geraten. Konica Minolta bietet eine Reihe maßgeschneiderter Sicherheitsfunktionen zur Gewährleistung der Dokumenten- und Datensicherheit an.

■ Sicherheit von Festplattendaten

Die meisten Drucker und MFPs sind mit Festplatten und Hauptspeichern ausgestattet, die potenziell vertrauliche, über längere Zeiträume angesammelte Daten im Gigabyte-bereich speichern können.

Um sensible Unternehmensdaten zu schützen, sind zuverlässige Sicherungsmechanismen erforderlich. Bei Systemen von Konica Minolta bieten eine Reihe sich überschneidender und ineinandergreifender Funktionen diesen Schutz:

– Automatische Löschfunktion:

Durch die automatische Löschfunktion werden auf der Festplatte gespeicherte Daten nach Ablauf einer bestimmten Zeitspanne gelöscht.

– Kennwortschutz der internen Festplatte:

Das Auslesen von Daten, die natürlich auch vertraulicher Art sein können, erfordert nach dem Ausbau der Festplatte die Eingabe eines Kennworts. Das Kennwort ist mit dem System verknüpft.

Das bedeutet, dass ein Zugriff auf die Daten nach dem Ausbau der Festplatte aus dem System nicht möglich ist.

– Überschreiben der Festplatte:

Die sicherste Methode zum Formatieren einer Festplatte besteht darin, die Festplattendaten zu überschreiben. Dies geschieht nach verschiedenen Standards.

– Festplattenverschlüsselung:

Auf Festplatten, die in Konica Minolta-System integriert sind, können die Daten in verschlüsselter Form auf der Basis eines 128-Bit-Algorithmus gespeichert werden. Diese Funktion erfüllt Datensicherheitsrichtlinien in Unternehmen. Sobald eine Festplatte verschlüsselt wurde, können die Daten auch nach dem Ausbau der Festplatte aus dem MFP nicht gelesen bzw. abgerufen werden.

■ Sicheres Drucken

Ausgabegeräte gelten als Sicherheitsrisiko – ein Risiko, das nicht unterschätzt werden sollte: Im einfachsten Fall können Dokumente, die im Ausgabefach liegen, selbst von unbeteiligten Personen, die sich zufällig in der Nähe des Systems aufhalten, gelesen werden. Es gibt für Unbefugte keinen einfacheren Weg, Zugang zu vertraulichen Informationen zu erhalten. Funktionen für sicheres Drucken stellen eine Möglichkeit dar, Vertraulichkeit von Dokumenten zu wahren, da sie vor dem Ausführen eines Druckauftrags die Festlegung eines Kennworts erfordern. Die Funktion für sicheres Drucken erfordert die Eingabe des Kennworts direkt am Ausgabegerät. Andernfalls wird der Druckvorgang nicht gestartet. Dies ist eine einfache und effektive Möglichkeit, zu verhindern, dass vertrauliche Dokumente in falsche Hände geraten.



Touch & Print/ID & Druck

Touch & Print basiert auf der Authentifizierung durch den Fingervenenscanner oder IC-Kartenleser, während die Funktion ID & Druck Benutzerauthentifizierung über ID und Kennwort erfordert. Das Drucken des Auftrags erfolgt unmittelbar am Gerät, aber erst nachdem der Benutzer über eine am Kartenleser aufgelegte Karte authentifiziert oder über den Fingervenenscanner identifiziert wurde. Der Vorteil dieser Funktion besteht darin, dass keine zusätzliche ID mit Kennwort erforderlich ist.

Kopierschutz

Durch die Kopierschutzfunktion wird den Ausdrucken und Kopien beim Drucken ein Wasserzeichen hinzugefügt. Das Wasserzeichen ist auf dem Originalausdruck kaum zu sehen, erscheint aber auf Kopien im Vordergrund, um sie als solche kenntlich zu machen.

Kopiersperre/Kopieren mit Kennwort

Durch diese Funktion wird dem Original während des Druckvorgangs ein verstecktes Sicherheitswasserzeichen hinzugefügt, um ein Kopieren des Dokuments zu verhindern. Dieses Wasserzeichen ist auf dem geschützten Originaldokument kaum zu erkennen, verhindert aber ein Kopieren des Dokuments, da das System für diesen Vorgang gesperrt ist. Durch die Funktion 'Kopieren mit Kennwort' kann die Kopiersperre umgangen werden, das heißt, es können Kopien erstellt werden, wenn das richtige Kennwort am Bedienfeld des MFP eingegeben wird.

PDF-Verschlüsselung

Verschlüsselte PDFs sind durch ein Benutzerkennwort geschützt: Die Berechtigung, das PDF-Dokument zu drucken oder kopieren sowie die Berechtigung, Inhalte hinzuzufügen, kann während der Scanphase am MFP eingerichtet werden.

PDF mit digitaler Signatur

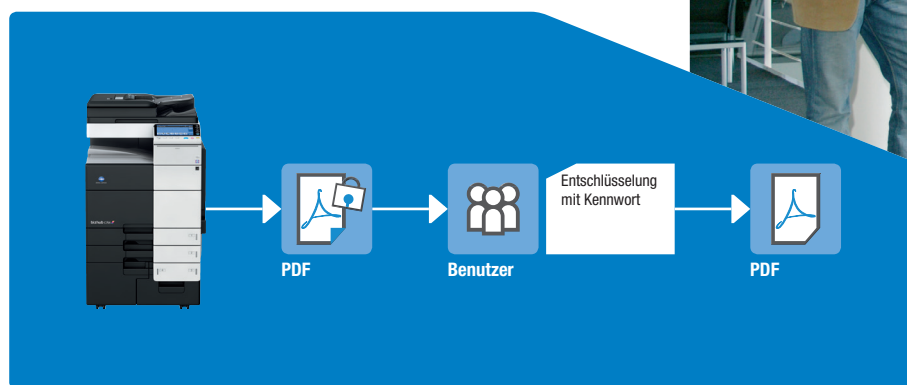
Diese Funktion ermöglicht das Hinzufügen einer digitalen Signatur zum PDF-Dokument während des Scanvorgangs. Dadurch können alle nach dem Erstellen eines PDF-Dokuments vorgenommenen Änderungen nachverfolgt werden.

Faxempfang

Wenn die entsprechende Funktion aktiviert ist, können empfangene Faxdokumente in einer geschützten Box vertraulich gespeichert werden.

Boxsicherheit

Boxen sind sowohl für Einzelpersonen als auch für Gruppen verfügbar und ermöglichen das sichere Speichern von Dokumenten auf der Festplatte des MFP vor der Ausgabe des Druck- oder Kopierauftrags. Boxen können mithilfe eines achtstelligen alphanumerischen Kennworts geschützt werden. Nach Eingabe des richtigen Kennworts ist der Zugriff auf Dokumente in der Box bzw. die Anzeige dieser Dokumente möglich. Durch dieses System wird sichergestellt, dass vertrauliche Dokumente und Daten nur von entsprechend autorisierten Personen angesehen werden können.



Verschlüsselte PDF

NETZWERKSICHERHEIT

In modernen Unternehmensumgebungen wie in der heutigen Geschäftswelt im Allgemeinen sind Kommunikation und Konnektivität unverzichtbar. Bürosysteme von Konica Minolta sind für die Einbindung in Netzwerkumgebungen konzipiert. Beispielsweise wurden Netzwerkdrucker und Multifunktionssysteme (MFPs) so weit entwickelt, dass sie als anspruchsvolle zentrale Dokumentverarbeitungsknoten innerhalb des Netzwerks fungieren, über die Dokumente und Daten an Netzwerkziele gedruckt, kopiert und gescannt sowie E-Mails gesendet werden können. Dieses Szenario bedeutet auch, dass diese Bürosysteme denselben Sicherheitsrisiken ausgesetzt sind und denselben Sicherheitsrichtlinien entsprechen müssen wie jedes andere Netzwerkgerät und bei Nichteinhaltung ein Risiko darstellen. Um Schwachstellen in Bezug auf interne und externe Angriffe über das Netzwerk zu vermeiden, stellt Konica Minolta sicher, dass alle Systeme den strengsten Sicherheitsstandards entsprechen. Dies geschieht durch eine Reihe von Maßnahmen:

Sperrung von IP-Adressen

Über eine grundlegende interne Firewall wird eine IP-Adressfilterfunktion und Steuerung des Protokoll- und Portzugriffs bereitgestellt.

Port-Deaktivierung

Im Administratormodus können Ports und Protokolle direkt am System oder per Fernzugriff geöffnet, geschlossen, aktiviert und deaktiviert werden.

S/MIME

Die meisten MFPs von Konica Minolta unterstützen S/MIME (secure/multipurpose internet mail extensions) für die sichere E-Mail-Kommunikation vom MFP zu den angegebenen Empfängern.

S/MIME wird für sicheren E-Mail-Verkehr durch Verschlüsselung der E-Mail-Nachricht und ihres Inhalts mithilfe eines Sicherheitszertifikats verwendet.

SSL/TLS-Kommunikation

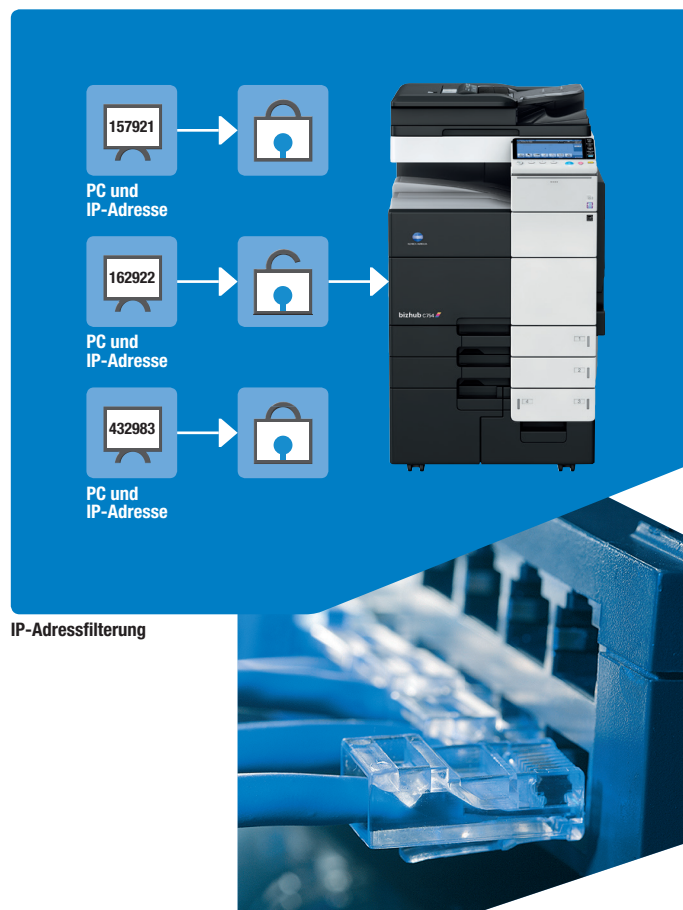
Dieses Protokoll schützt vom System ausgehende und an das System gerichtete Kommunikation und deckt beispielsweise Online-Verwaltungstools und Windows Active Directory-Übertragungen ab.

IPsec-Unterstützung

Die meisten bizhub-Systeme unterstützen auch IPsec und gewährleisten somit vollständige Verschlüsselung von Netzwerkdaten, die vom MFP aus oder zum MFP übertragen werden. Durch das IP-Sicherheitsprotokoll werden alle Netzwerkübertragungen zwischen dem lokalen Intranet (Server, Client-PC) und dem System verschlüsselt.

IEEE 802.1x-Unterstützung

Die in der IEEE802.1x-Familie definierten Normen stellen den anerkannten portbezogenen Authentifizierungsstandard für die Steuerung des Netzwerkzugriffs auf WLANs und LANs dar. Durch diese Standards wird Netzwerksicherheit durch Beenden von Netzwerkübertragungen (z. B. DHCP oder HTTP) auf nicht autorisierte Geräte (mit Ausnahme von Authentifizierungsanforderungen) gewährleistet.



IP-Adressfilterung