



KONICA MINOLTA

Giving Shape to Ideas



Sicherheitsfunktionen – arbeiten Sie auf Nummer sicher

Sicherheitsfunktionen



Gut zu wissen, wer Bescheid weiß.

Dank technologischem Fortschritt können Kopiersysteme und Drucker heute Dokumente scannen und Faxe oder E-Mails senden. Innovative Bürosysteme erleichtern zwar heute spürbar die Arbeitsabläufe, sind aber auch gleichzeitig Risiken ausgesetzt, die selten offensichtlich sind.

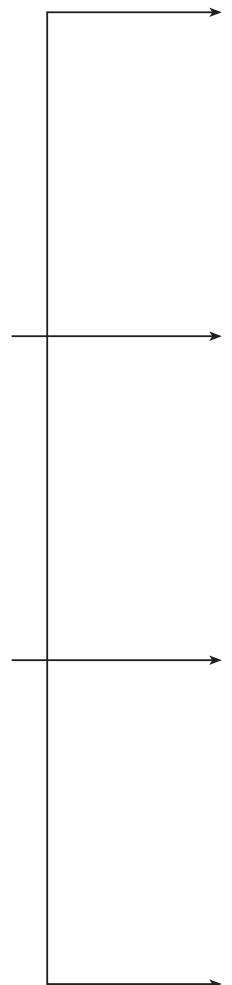
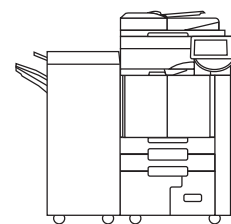
→ Eindringlinge unerwünscht

Als Teil Ihres Computernetzwerks sind Ihre Kopier- und Drucksysteme z. B. durch Hacker angreifbar, die es auf das Ausspionieren vertraulicher Unternehmensinformationen abgesehen haben.

Selbst rundum geschützte Netzwerke sind vor unerlaubten Eingriffen nicht sicher. Auch dann nicht, wenn Sie Firewalls und Antiviren-Software installieren und sicherstellen, dass nur autorisierte Personen Zugriff auf Ihr Netzwerk haben.

Doch es gibt Lösungen, mit denen Sie jede Sicherheitslücke schließen. Wir zeigen Ihnen, wie Sie sich, Ihre Mitarbeiter und Ihr Unternehmen effizient schützen. Dafür bieten wir Ihnen Funktionalitäten, bei der Sicherheit und Vertraulichkeit garantiert sind, ohne dass Sie auf den gewohnten Bedienerkomfort verzichten müssen.

→ Risikofaktoren für Unternehmen



Achtung: Hier lauern ungebetene Gäste!



Risiko 1

Auf der Festplatte und im Speicher Ihres digitalen Druckers, Kopierers oder multifunktionalen Systems bleiben auch höchst vertrauliche Informationen lange erhalten.



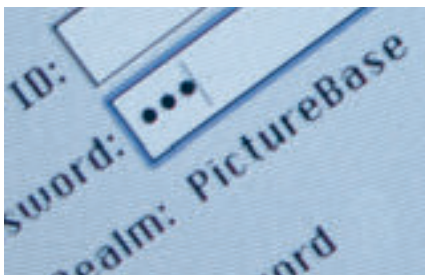
Risiko 2

Alles, was ein Hacker für den unerlaubten Zugriff auf Informationen in Ihrem Netzwerk benötigt, sind die Konfigurationseinstellungen einer ungeschützten Netzwerkkarte.



Risiko 3

Die gravierendsten Sicherheitslücken finden sich in der Regel direkt am Drucker oder Kopierer. Im Vorbeikommen kann jeder die Dokumente im Ausgabefach sehen und lesen – ob er das nun darf oder nicht!



Risiko 4

Vom gleichen System können diese vertraulichen Informationen dann auch schnell und unbemerkt per Scan-to-E-Mail oder Scan-to-Fax nach außen weitergeleitet werden.

Mit Netz und **ohne Risiko**

Eine Vielzahl unserer Systeme sind mit speziellen Sicherheitsmechanismen ausgestattet, die Ihre vertraulichen Netzwerkdaten schützen. Ab der neuesten Generation der bizhub Systeme sind die Netzwerkprotokolle IPSec und IPv6 bereits integriert. Diese Vorkehrungen gewähren nur autorisierten Personen Zugriff aufs Netzwerk und sichern die Dokumentenausgabe.

➔ Zugriffs- und Kostenkontrolle

Bei den bizhub Systemen können Sie bis zu 1.000 Kostenstellen und Benutzerkonten hinterlegen, mit denen Sie individuell für verschiedene Benutzer unterschiedlichste Rechte definieren, z. B. wer in Farbe drucken oder andere Funktionen nutzen darf. Indem Sie zusätzlich die Benutzer den einzelnen Kostenstellen zuordnen, gewinnen Sie einen optimalen Überblick über die entstandenen Kosten.

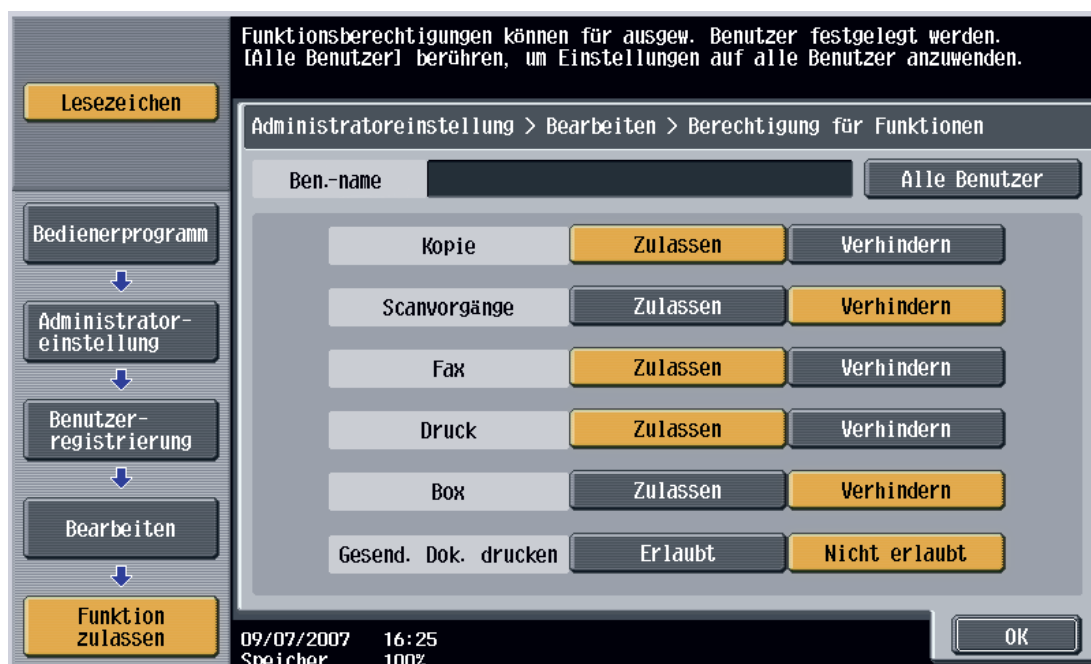
Wer ein bizhub System nutzen will, muss sich mit Benutzernamen und Kennwort authentifizieren. Ohne die wird der Zugriff zum System automatisch verwehrt. Die Benutzer-Authentifizierung kann lokal auf den bizhub Systemen erfolgen oder auch über den Windows NT/2000/2003 Server. Die Benutzerdaten werden durch betriebssystemspezifische Mechanismen (z. B. NTLM oder Kerberos) geschützt.

➔ Biometrische Authentifizierung

Mit der neuesten bizhub Generation kann eine Authentifizierung mittels Fingervenenscan erfolgen, d. h. der Anwender muss nicht mehr seinen Anmeldenamen und sein Passwort eingeben, sondern kann sich einfach durch Abtasten der Fingervenensstruktur anmelden.

➔ PDF-Verschlüsselung

Dank der standardmäßig integrierten PDF-Verschlüsselung kann direkt beim Scannen die Dokumentenberechtigung festgelegt werden, ob z. B. das Dokument beim Öffnen durch Kennwort geschützt ist oder ob es gedruckt, verändert oder mit Notizen versehen werden darf. Diese Berechtigungen sind auch im Acrobat Reader sichtbar.





Ihre Daten bleiben **unter sich**

→ E-Mail

Abhängig vom Modell werden neben den Standardprotokollen (SMTP, POP und IMAP) auch ESMTP und APOP verwendet. Beide fragen z. B. beim Senden einer E-Mail Benutzerdaten zur Authentifizierung am Mail-Server ab und verschlüsseln beim Abrufen einer E-Mail die Account-Informationen. Zusätzlich wird auch die Funktion POP vor SMTP unterstützt. Bei der neuesten bizhub Generation kommt ergänzend zu den vorhandenen Sicherheitsmechanismen S/MIME zum Einsatz.

→ LDAP

Bei der LDAP-Konfiguration muss ein Standard-Benutzerkonto mit Passwort angegeben werden, welches bei der LDAP-Suche am Server abgefragt wird. Durch Verschlüsselung der Anmeldung mittels MD-5/GSS-SPNEGO sowie SSL sind Passwörter nicht auslesbar. Das System steht auf diesem Wege nur autorisierten Benutzern zur Verfügung – Missbrauch ausgeschlossen.

→ IP-Filter

Mittels IP-Filtern kann der Systemadministrator IP-Adressbereiche konfigurieren und so genau definierten Benutzergruppen den Zugriff auf bestimmte Systeme ermöglichen oder verweigern. Diese leistungsstarke Firewall verhindert jeden verbotenen Zugriff auf Konfigurationen oder Netzwerkeinstellungen Ihrer Kopierer und Drucker. Zusätzlich zu den IP-Filtern können auch einzelne Ports, wie z. B. FTP, SMTP etc., separat deaktiviert werden.

→ Web-Zugriff

Wo erforderlich, sichert ein SSL-Zertifikat (HTTPS-Zugang) die PageScope Web Connection. Das „Abhören“ einer Verbindung durch Dritte wird so unmöglich. Auf Administrator-Ebene ist der Zugriff generell passwortgeschützt.



Höchste Standards dank **Common Criteria-ISO/IEC 15408**

Konica Minolta bietet Ihnen multifunktionale Ausgabesysteme, die der Common-Criteria-Evaluierung entsprechen und den aktuellen Sicherheitsstandard ISO 15408 EAL3 erfüllen.

- Der Common-Criteria-Standard ist festgelegt in der ISO-Norm ISO/IEC 15408 und ermöglicht eine objektive Bewertung der Sicherheit von IT-Produkten sowie eine grenzübergreifende Anerkennung von Prüfung und Zertifizierung.
- Die Zertifizierung ISO/IEC 15408 ist in 7 EALs (Evaluation Assurance Level) aufgeteilt: Level 1 stellt lediglich eine Richtlinie für Sicherheitsaspekte dar, während Level 7 als höchste Stufe z. B. die Datenverschlüsselung zwingend vorschreibt.
- Common Criteria gibt dem Endanwender eine Liste mit Anforderungen an die Definition und Evaluierung von IT-Sicherheit an die Hand, die einen international gültigen Vergleichsmaßstab bildet.

- Konica Minolta bietet eine Auswahl an multifunktionalen Systemen, die gemäß CC ISO/IEC 15408 EAL 3 zertifiziert sind; auch alle zukünftigen Systeme gehören dazu.

Kopierer, Drucker und Software mit dieser Zertifizierung wurden genau auf ihren Sicherheitslevel geprüft und garantieren die von Ihnen erwartete Datensicherheit. Für Sie bedeutet das: Mit Druckern und Kopierern von Konica Minolta bleiben Ihre vertraulichen Daten vertraulich!

Intern alles **bestens geregelt**

→ **Verschlüsselung**

Durch ein sogenanntes Encryption Board werden Daten, die auf die Festplatte geschrieben werden, mit einer Verschlüsselung bis zu 128 Bit vor eigenmächtigem Zugriff geschützt und sind so für Unbefugte absolut nicht verwendbar.

→ **Sicherung der Festplatte**

Nach dem Löschen des Dateinamens bleiben Informationen erhalten. Erst eine Datenüberschreibung der Festplatte der bizhub Systeme nach dem VSITR-Standard löscht Ihre Daten endgültig und verhindert Datendiebstahl. Auch gegen eine unbefugte Verwendung in einem anderen System ist die interne Systemfestplatte geschützt – für den Ausbau ist die Eingabe eines individuellen PIN-Codes direkt am System erforderlich.

→ **Dokumentenserver**

Dank der Dokumentenserverfunktion kann ein berechtigter Nutzer unterschiedlich generierte Jobs (z. B. Druck-, Scan-, Kopierjobs) in seiner Box ablegen, nach Wunsch kombinieren und so neue Dokumente zusammenstellen. Der Zugriff auf jede Box ist nur nach Eingabe des individuellen Benutzernamens und des zugehörigen Passworts möglich. Dies verhindert einen unbefugten Zugriff von nicht autorisierten Personen.

→ **Logfiles**

Logfiles machen alle am System durchgeführten Aktivitäten genau nachvollziehbar. Alle Bedienschritte werden exakt protokolliert, z. B. wann welcher Benutzer welche Datei gedruckt oder gescannt hat, jedoch ohne die Inhalte der jeweiligen Dateien anzuzeigen.

→ **Vertrauliches Drucken**

Um zu verhindern, dass gerade gedruckte Dokumente in der Ausgabe des Systems unbefugt gelesen werden, bieten die digitalen multifunktionalen Systeme von Konica Minolta eine Funktion für vertrauliches Drucken. Damit bleiben Ihre Druckjobs in der Warteschlange und werden erst dann produziert, wenn Sie Ihr individuelles Passwort direkt am System eingeben.





KONICA MINOLTA



Common Criteria Validated

➔ Überblick Sicherheitsfunktionen

	bizhub	C35	C224 C284 C364 C454 C554	C654 C754 PRO C754	36 42	223 283 363 423 552 652	501	601 751	PRO C6000L C6000	PRESS C6000 C7000 C8000****	PRO 1051 1200/P	PRO 951
Zugriffskontrolle												
Zertifizierung ISO 15408 EAL3	x	x	x	x	x	x	x	x	x	x	x	x
Kostenstellen Kopien/Druck	x	x	x	x	x	x	x	x	x	x	x	x
Funktionsbeschränkung (Druck/Kopie/Scan/Fax/Box)	x**	x	x	x**	x	x	x	x	x	x	x	x
Biometrische Authentifizierungsoption (Fingervenenscan)	-	x	x	-	x	x	x	-	-	-	-	-
Vertrauliches Drucken	x	x	x	x	x	x	x	x	x	x	x	x
Kartenauthentifizierungsoption	x	x	x	x	x	x	x	x	x	x	x	x
Ereignisprotokoll	x	x	x	x	x	x	x	x	x	x	x	x
Datensicherheit												
Datenverschlüsselung (Festplatte)	x	x	x	x	x	x	x*	x*	-	-	-	-
Festplatten Daten-Überschreibung	x	x	x	x	x	x	x	x	x	x	x	x
Festplatten passwortgeschützt	-	x	x	-	x	x	x	x	x	x	x	x
Integrierte Firewall												
IP-Filter	x	x	x	x	x	x	x	x	x	x	x	x
Zugriffskontrolle über Protokoll- und Port-Deaktivierung	x	x	x	x	x	x	x	x	x	x	x	x
SSL/TLS-Verschlüsselung (HTTPS)	x	x	x	x	x	x	x	x	x	x	x	x
Scannen												
Benutzerauthentifizierung	x	x	x	x	x	x	x	x	x	x	x	x
POP vor SMTP	x	x	x	x	x	x	x	x	x	x	x	x
SMTP-Authentifizierung (SASL)	x	x	x	x	x	x	x	x	x	x	x	x
S/MIME	x	x	x	x	x	x	x	-	-	-	-	-
Andere												
Geschützter Technikermodus	x	x	x	x	x	x	x	x	x	x	x	x
8-stelliges Passwort	x	x	x	x	x	x	x	x	x	x	x	x
Abschaltung bei unautorisiertem Zugriff	-	x	x	-	x	x	x	-	-	-	-	-
Kopierschutz via Wasserzeichen	-	x	x	x***	x	-	-	-	-	-	-	-
Verschlüsseltes PDF	-	x	x	-	x	x	x	-	-	-	-	-

* (mit) Zubehör

** keine Box-Funktion

*** nur Druck

**** Scan-Funktion nur mit PF-705

Alle Angaben bezüglich der genannten Grammaturen und Papierformate beziehen sich auf von Konica Minolta empfohlene Druckmedien. Alle technischen Daten zur Papierkapazität beziehen sich auf DIN-A4-Papier mit einem Gewicht von 80 g/m². Alle technischen Daten zu den Scan-, Kopier- und Druckgeschwindigkeiten beziehen sich auf DIN-A4-Papier, das quer im Mehrfachseiten- und Simplex-Modus gescannt, kopiert oder gedruckt wurde. Das max. monatliche Ausgabevolumen beschreibt unterjährige Produktionsspitzen. Einige der Produktabbildungen enthalten optionales Zubehör. Konica Minolta übernimmt keine Gewähr für genannte Preise und Spezifikationen. Technische Änderungen vorbehalten. Die Unterstützung sowie Verfügbarkeit der aufgeführten Spezifikationen und Funktionalitäten kann abhängig von Betriebssystemen, Applikationen, Netzwerkprotokollen sowie Netzwerk- und Systemkonfigurationen variieren. Alle anderen Marken- und Produktnamen sind eingetragene Warenzeichen oder Markennamen des jeweiligen Herstellers. Konica Minolta übernimmt bezüglich dieser Produkte keine Haftung oder Garantie.

Ihr Konica Minolta Business Solutions Partner:



Konica Minolta
Business Solutions Deutschland GmbH
www.konicaminolta.de/business