

Sicherheitslösungen
Zum Schutz Ihrer Daten.



Ricoh... Ihr zuverlässiger Partner

Die Innovationen in der Informationstechnologie haben die Erstellung, Verwaltung, Verteilung und Archivierung von Informationen von Grund auf verändert und radikal beschleunigt. Doch mit steigender Transparenz und Geschwindigkeit Ihrer Geschäftsabläufe steigt auch das Risiko externer beziehungsweise unautorisierter Zugriffe und Eingriffe. So können vertrauliche Dokumente trotz laufender Investitionen in Netzwerksicherheit und Firewalls immer noch in die falschen Hände geraten. Gleichzeitig stellen Gesetzgeber und Regulierungsbehörden immer strengere Ansprüche an den Datenschutz. Genug Gründe, spätestens jetzt eine unternehmensweite Sicherheitspolitik zu implementieren, die alle Informationsflüsse konsequent abdeckt.

Das Aufdecken von Sicherheitsrisiken und der kontinuierliche Schutz Ihrer Informationen sind eine komplexe Aufgabe, die bei Ricoh in kompetenten Händen liegt. Datensicherheit ist bei uns seit langer Zeit ein integraler Bestandteil der Systementwicklung. Potenzielle Sicherheitslücken werden identifiziert und proaktiv angegangen. Als Branchenführer bietet Ricoh eine umfassende Auswahl an nahtlos integrierbaren Sicherheitsfunktionen und ausgewiesene Kompetenz bei der Analyse potenzieller Sicherheitslücken in Ihren Arbeitsabläufen. Deshalb ist Ricoh Ihr zuverlässiger Partner für den Schutz vertraulicher Daten und die Überwachung Ihres gesamten Dokumentenzyklus.

Wo genau befinden sich Ihre Sicherheitslücken?

So unentbehrlich moderne Büroelektronik im heutigen Büroalltag auch ist, so groß sind auch die potenziellen Risiken einer nicht ausreichenden Absicherung dieser leistungsstarken Funktionen. In unserer vernetzten Welt tauchen immer wieder neue Bedrohungen auf, von denen einige recht offensichtlich sind. Oft liegen beispielsweise vertrauliche Dokumente frei zugänglich in Drucker-Ausgabefächern, weil der Absender durch einen Telefonanruf aufgehalten wird. Andere wiederum - wie beispielsweise Hacking oder professioneller Datendiebstahl - sind unsichtbar, aber umso gefährlicher.

ERSTELLTE DOKUMENTE

- 1 Eine unautorisierte Person öffnet und betrachtet Ihr vertrauliches Dokument.

KOMMUNIKATION ZWISCHEN PC UND GERÄT

- 2 Ein Außenstehender kann an den Drucker gesendete Daten abfangen.

DOKUMENTE

- 3 Jemand hat im Vorübergehen Einsicht in im Drucker-Ausgabefach liegende Dokumente.

- 4 Jemand kopiert unerlaubt ein Dokument.

GERÄTENUTZUNG

- 5 Eine unautorisierte Person hat Zugang zum Gerät.

SCANNEN

- 6 Jemand verteilt unrechtmäßig vertrauliche Dokumente mit der „Scan to E-Mail“-Funktion an eine falsche Adresse.

ARCHIVIERTE DOKUMENTE

- 7 Eine unbefugte Person verschafft sich Zugang zum Dokumenten-Server.

KOMMUNIKATION ZWISCHEN PC UND GERÄT

- 8 Jemand verschafft sich Zugriff auf den Datenfluss zwischen PC und Gerät.

DATEN AUF DER FESTPLATTE

- 9 Informationslecks aufgrund verbleibender Daten auf der Festplatte.

- 10 Gefährdung vertraulicher E-Mail-/Fax-Adressen.

NETZWERK

- 11 Ein unautorisierter Außenstehender verschafft sich Zugang zum Netzwerk.

- 12 Eine unautorisierte Person verschafft sich über eine kabellose Verbindung Zugang zum Netzwerk.

TELEFON-/FAXLEITUNG

- 13 „Anzapfen“ von Telefon-/Faxleitungen.

BUCHHALTUNG

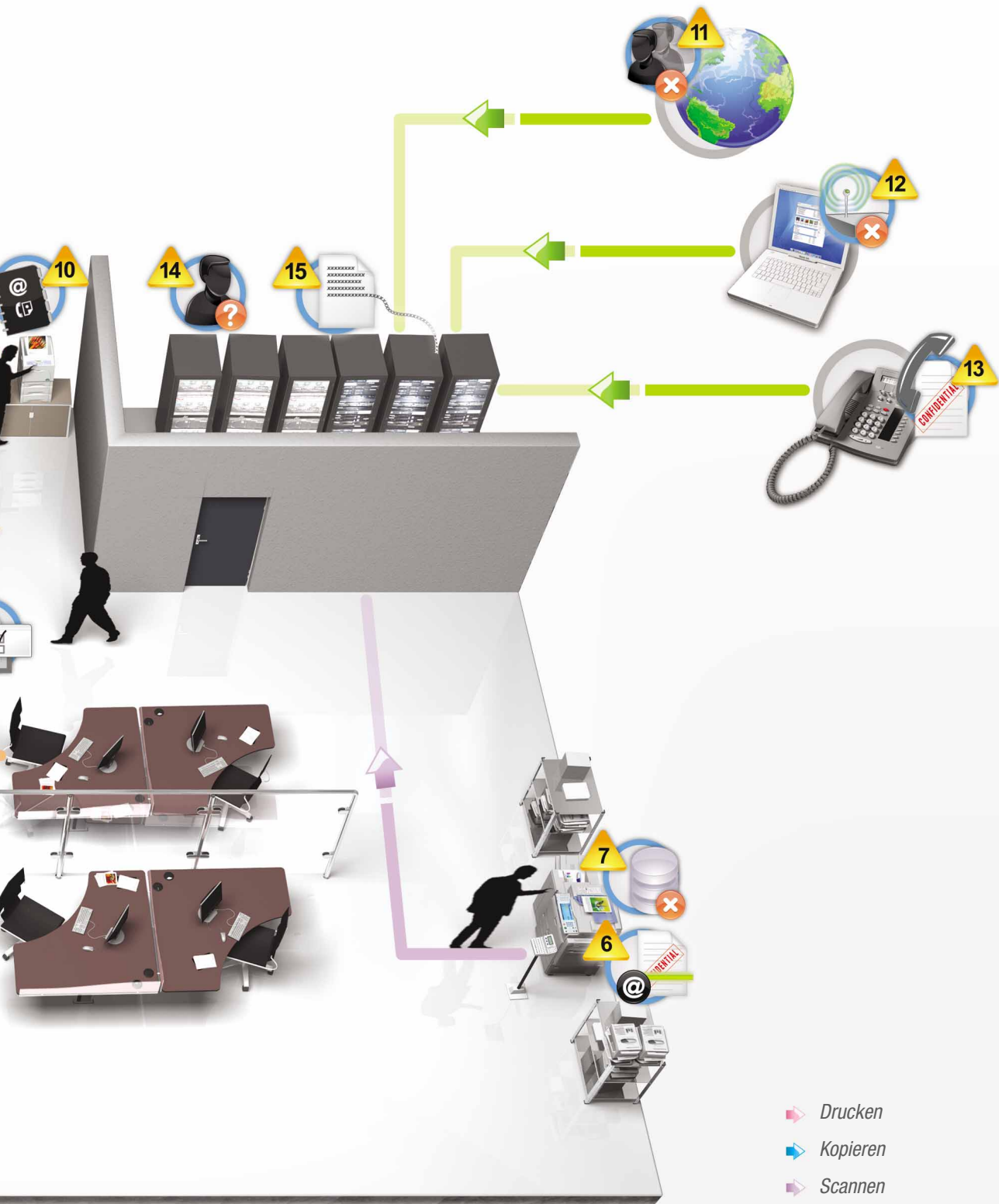
- 14 Ineffiziente oder unerlaubte Nutzung von Netzwerkgeräten.






ARCHIVIERTE DOKUMENTE

- 15 Ihre Daten sind verloren.

Dokumentensicherheit als ganzheitlicher Ansatz





-  Drucken
-  Kopieren
-  Scannen
-  Schützen Sie das Gerät
-  Schützen Sie das Netzwerk

Durchdachte Lösungen

Neben optimaler Nutzung und effizienter Verwaltung ihrer Informationen wird der wirksame Datenschutz immer mehr zum Erfolgsfaktor im Wettbewerb. Mit den Sicherheitslösungen von Ricoh sind Ihre Daten von Beginn an bis zur Dokumentenausgabe geschützt - und das ohne Beeinträchtigung Ihrer Arbeitsabläufe. Neben einer großen Auswahl an serienmäßig integrierten Sicherheitsfunktionen bietet Ricoh branchenführende Lösungen für jede Art von Risiko. Optimal geschützte Daten machen Sie zu einem zuverlässigen Partner und verschaffen Ihnen so einen nachhaltigen Wettbewerbsvorsprung.

1 Dokumentenschutz durch sichere Geräteeinstellungen.

2 **Verschlüsselung von Druckdaten** mit SSL-Technologie via IPP (Internet Printing Protocol) macht abgefangene Daten unbrauchbar.

3 Geschützte Dokumente

- **Locked Print™:** Druckfreigabe erfolgt erst nach Eingabe Ihres Passworts am Drucker. Verhindert unbefugtes Einsehen/Mitnehmen Ihrer vertraulichen Dokumente.
- **Secure Document Release:** Ein Druckauftrag wird vom Server gelöscht, wenn er nicht innerhalb eines bestimmten Zeitlimits abgerufen wird.

4 **Schutz vor unautorisiertem Kopieren** mit der **Kopierschutz-Einheit:** Bei unbefugtem Kopieren entstehen unlesbare Ergebnisse.

5 Authentifizierung

- **Benutzerauthentifizierung:** 4 Methoden (Windows®, LDAP, Basic Code und Benutzercode)
- **Authentifizierung über ein externes Gerät:** Karte/PIN-Code
- **Administratorauthentifizierung.**

6 Sicheres Scannen

- **Beschränken der manuellen E-Mail-Adressen-Eingabe** damit Dokumente nur an autorisierte Empfänger versendet werden können.
- **Verschlüsselung eingescannter Daten** mit SSL-Technologie zur Abwendung von Hacker-Angriffen.

7 **Zugriffsbeschränkung auf Dokumentenserver** und Vergabe von Benutzerrechten zum Schutz gespeicherter Informationen.

8 **Verschlüsselung von Geräteeinstellungen** mit SSL-Technologie (Secure Sockets Layer) via SNMP v3 zur Abwehr von Datendiebstahl.

9 **Sicherung der Festplatte** durch Überschreiben aller temporären Druck-, Kopier- und Scandaten (**Datensicherheits-Kit**).

10 **Verschlüsselung des Adressbuchs** zur Vermeidung von unerlaubtem Einsehen/Lesen registrierter Daten.

11 Unerlaubten Netzwerkzugang limitieren

- **Netzwerkprotokollbeschränkung:** Systemadministratoren können nicht benötigte Protokolle deaktivieren.
- **IP-Filter:** Einschränkung von unbefugtem Gerätezugriff durch Einschränkung zugelassener IP-Adressbereiche.

12 **Überwachung kabelloser Verbindungen** mit WPA; Bestätigung bei einem Authentifizierungsserver erforderlich.

13 **Schutz gegen unbefugten Zugriff auf Telefon-/Faxleitungen** durch Beenden der Verbindung, wenn versucht wird, über ein Terminal ohne G3-Protokoll eine Verbindung herzustellen.

14 Sichere Rückverfolgung

- **Auftragsprotokollierung:** Rückverfolgen von Druck-, Kopier- und Faxaktivitäten einzelner Benutzer.
- **Beobachtung der Netzwerkaktivität:** Behalten Sie ein Dokument von Anfang bis Ende im Auge.

15 **Planmäßige Backups** zur Vermeidung des Verlusts archivierter Daten.

Akkreditierungs-lösungen für den Zugriff Dritter: Garantierte Sicherheit

Sicherheitslösungen von Ricoh berücksichtigen sowohl den notwendigen Zugang zu Dokumenten als auch deren Schutz vor unbefugtem Zugriff. Unsere kontinuierlichen Anstrengungen auf dem Gebiet der Sicherheitssysteme garantieren Ihnen zuverlässige Lösungen nach höchsten internationalen Standards. Setzen Sie deshalb auf Ricoh, wenn es um die Planung und Realisierung einer ganzheitlichen Sicherheitsstrategie für Ihre Informationsflüsse geht.

Sichere Organisation: ISMS

ISMS (Information Security Management System) ist ein übergreifendes System zur Verwaltung der Informationssicherheit. Es hilft Unternehmen und Organisationen, die Vertraulichkeit, Intaktheit und Abrufbarkeit ihrer wertvollen Informationen aufrechtzuerhalten. Da es sich nicht nur auf die Sicherheit von Computersystemen beschränkt, bietet ISMS ein ganzheitliches Risikomanagement. Es legt grundlegende Sicherheitsrichtlinien für den Umgang mit Informationen fest, implementiert und realisiert Geschäftspläne und führt periodische Neubewertungen von Zielvorstellungen durch.

Sicheres Produkt: Common Criteria (ISO15408)

Common Criteria (ISO15408) ist ein international anerkannter Standard, der Sicherheitsanforderungen definiert und Verfahren zur Sicherheitsprüfung von IT-Systemen und Software festlegt. Diese standardisierten Evaluierungen verifizieren die Produktangaben des jeweiligen Anbieters und schaffen damit eine sichere Entscheidungsgrundlage für den Einsatz eines bestimmten Produkts in sicherheitskritischen Umgebungen. Die Zertifizierung umfasst neben Design und Funktion den gesamten Lebenszyklus des Produkts einschließlich Produktion, Versand, Verkauf, Installation und Service.

ISMS-Zertifizierung

Um unseren Kunden die volle Sicherheitsgarantie für unsere Produkte geben zu können, arbeitet die Ricoh-Gruppe an einer weltweiten Einführung des ISMS. Über 100 Betriebe der Ricoh-Gruppe weltweit haben sich bereits strengen Tests unterzogen und die ISMS-Zertifizierung (BS7799 Teil 2) erhalten.

ISO15408-Zertifizierung

Ricoh hat für sein Datensicherheits-Kit die ISO15408-Zertifizierung erhalten. Die Wirksamkeit dieser Lösung ist somit unabhängig bestätigt.



www.ricoh-europe.com/security

RICOH

Weitere Informationen erhalten Sie von:



Nach ISO9001 : 2000 zertifiziert
Nach ISO14001 zertifiziert

Ricoh trägt zur Erhaltung der wertvollen natürlichen Ressourcen der Erde bei.

Alle Marken- und/oder Produktnamen sind Warenzeichen der jeweiligen Eigentümer.

Änderungen der technischen Daten und des Designs vorbehalten. Aus drucktechnischen Gründen kann die Gehäusefarbe von der in diesem Prospekt gezeigten Farbe geringfügig abweichen.

Copyright © 2006 Ricoh Europe B.V.
Alle Rechte vorbehalten. Inhalt und/oder Gestaltung dieser Broschüre dürfen ohne vorherige schriftliche Genehmigung durch Ricoh Europe B.V. weder modifiziert, umformuliert, vollständig oder auszugsweise vervielfältigt noch anderweitig verwendet werden.

RICOH EUROPE B.V.
P.O. Box 114, 1180 AC Amstelveen,
The Netherlands
Phone: +31 (0)20 54 74 111
Fax: +31 (0)20 54 74 222

www.ricoh-europe.com

GER/EUR - B1106N - 261357