RICOH
imagine. change.

Datenschutz und Informations-sicherheit

Security Solutions

Sicherheit geht vor

Moderne Multifunktionssysteme (MFP) ermöglichen effiziente und abteilungsübergreifende Workflows rund um das gedruckte und digitale Dokument. Doch wo viele Personen mit demselben System arbeiten, sollte auch der Schutz vor unbefugtem Zugriff gewährleistet sein. Ricoh bietet hier verschiedene Lösungen.

Im modernen Büro sind netzwerkfähige MFP nicht mehr wegzudenken. Oft liegen jedoch Verträge, Gehaltsabrechnungen, Finanzberichte oder ähnlich kritische Dokumente frei zugänglich im Druckerausgabefach. Sie können nicht nur eingesehen, sondern auch unerlaubt kopiert, gescannt oder über Scan-to-E-Mail weitergeleitet werden.

Ein Sicherheitskonzept für die Bürokommunikation kann verhindern, dass solche Dokumente in die falschen Hände geraten und minimiert dadurch die Gefahr wirtschaftlicher Schäden.

Die Technik dafür ist da

MFP können, wenn es um die Sicherheit von Daten und Dokumenten geht, oft weitaus mehr, als es den Anschein hat. Authentifizierung, Festplattenverschlüsselung, Kopierschutz oder Datenüberschreibung schützen Druckdaten vom Start des Druckjobs bis zur Ausgabe des Dokuments.

Wichtig für das Sicherheitskonzept ist ein durchgängiger, unternehmensweiter Ansatz. Die beste Datenlöschungseinheit nutzt nichts, wenn Ausdrucke offen zugänglich im Ausgabefach liegen.

Mit Berechtigung

Dass nur berechtigte Personen vertrauliche Dokumente drucken, kopieren, scannen oder faxen können, gewährleistet z. B. eine Nutzer-Authentifizierung. Ricoh verfolgt dabei die Strategie, seine Lösungen in bestehende Authentifizierungssysteme einzubinden. Der Anwender benötigt nur eine einzige Karte, mit der er sich morgens im Unternehmen anmeldet, in der Kantine bezahlt und sich an den Ausgabesystemen ausweist. Über die Locked-Print-Funktion werden Druckdaten auf der Festplatte des Systems gespeichert, bis sie der Nutzer mit einer ID-Karte freigibt. Die Authentifizierung kann auch über die Eingabe eines PIN erfolgen.

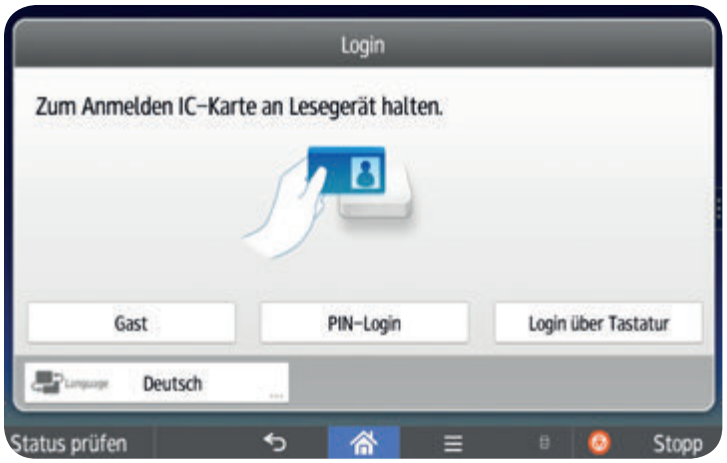
Mittels einer LDAP (Lightweight Directory Access Protocol)-Anwendung können Dokumente über die Scan-to-E-Mail-Funktion ausschließlich an registrierte Empfänger und nicht an manuell eingegebene E-Mail-Adressen geschickt werden.

Sind Internetzugänge für den externen Zugriff auf ein MFP eingerichtet, wie z. B. an Universitäten, ist es ratsam, Dokumente generell mit Passwortschutz auf dem Dokumentenserver abzulegen, damit sie nicht von Dritten eingesehen werden können.

Grundsätzlich sollte der Zugriff auf Drucksysteme über das Internet eingeschränkt werden, etwa durch eine Firewall. Eine Zugangsbeschränkung von IP-Adressen ist auch direkt am Multifunktionssystem möglich.

Die SSL (Secure Sockets Layer)-Verschlüsselung der Druckdaten und die Verarbeitung über ein gesichertes Netzwerk-Protokoll sorgen dafür, dass kein unbefugter Außenstehender den Datenstrom eines Druckauftrags im Netzwerk abfängt und die Informationen ausliest. Vertrauliche und sensible Daten werden auf diese Weise mit einem erheblich höheren Maß an Sicherheit verschickt.

Ist die Verschlüsselungseinheit für die Festplatte aktiviert, werden alle Daten verschlüsselt, sobald man sie auf der Festplatte ablegt.



Zielsicher Scannen

Mehr Sicherheit ist auch gegeben, wenn Prozesse vereinfacht und dadurch Anwenderfehler minimiert werden. Mit Hilfe der Softwarelösung GlobalScan NX oder StreamLine NX von Ricoh kann der Anwender schon beim Scanvorgang am System mit einem Knopfdruck festlegen, an welche Empfänger die Dokumente verschickt werden sollen.

Der Nutzer kann ebenfalls mit einem Knopfdruck entscheiden, ob er gescannte Dokumente per E-Mail verschicken oder an einen Fax-Server beziehungsweise an sein Dokumentenmanagement-System senden will.

Dank der Kopierschutzeinheit gehören auch unerlaubte Kopien von geschützten Dokumenten der Vergangenheit an: Geschützte Seiten werden beim Scannen, Kopieren oder Ablegen auf dem Dokumentenserver unleserlich oder speziell mit Wasserzeichen gekennzeichnet, ungeschützte Seiten bleiben weiterhin normal kopierbar.

Sicherheit geht vor

Moderne MFP sind in der Regel mit Festplatten ausgestattet. Die Integration von Festplatten ermöglicht viele Funktionen und gewährleistet so eine höhere Effizienz. Zu diesen Funktionen gehören z. B. der vertrauliche Druck, der Dokumentenserver oder der Einsatz von Java-Applikationen.

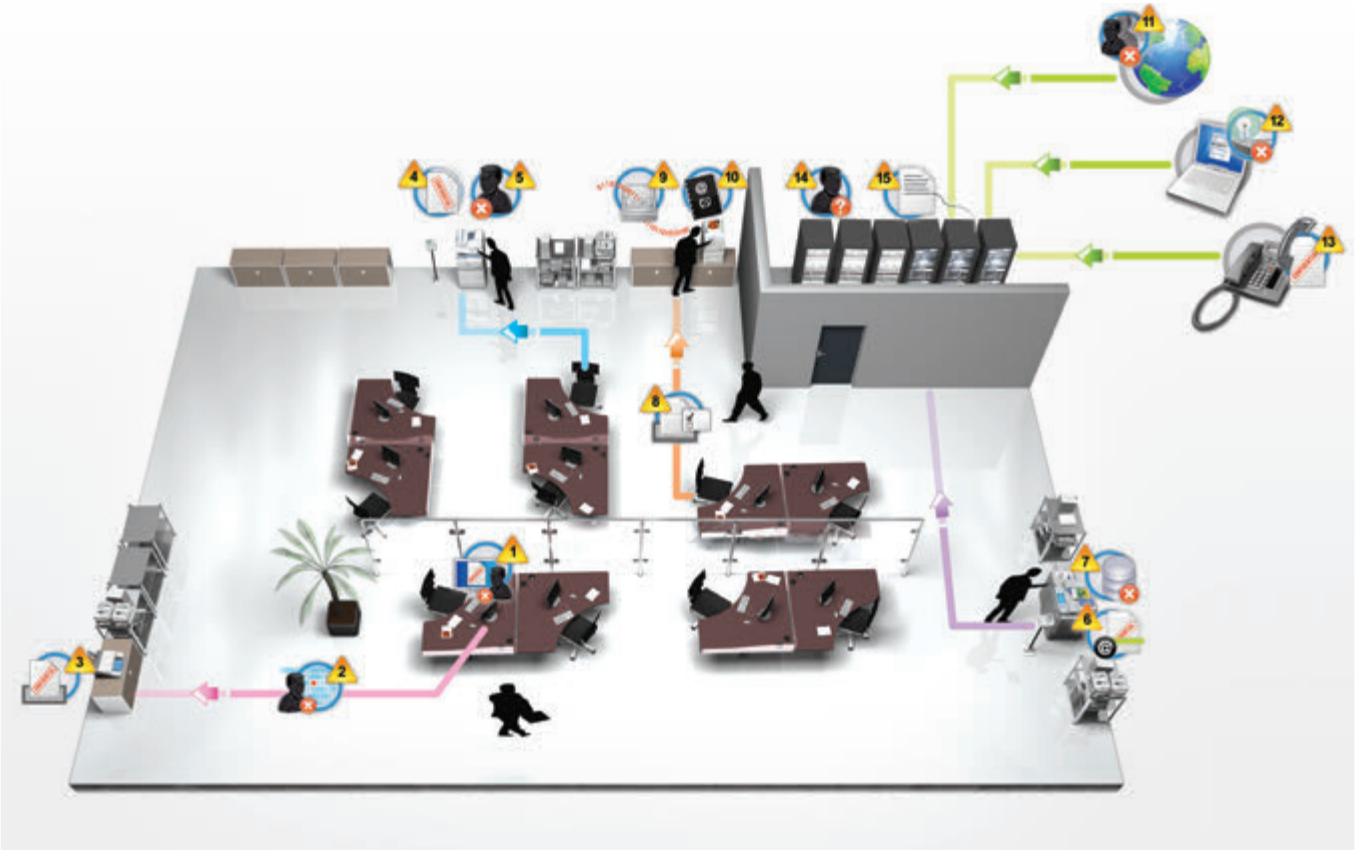
Im Gegensatz zu Festplatten, die beispielsweise in Computern eingesetzt werden, verfügen die Festplatten, die in MFP von Ricoh zum Einsatz kommen, über ein spezielles, herstellereigenes File-System und ein individuelles Komprimierungsverfahren für den Datenbereich. Darüber hinaus wird der Indexbereich der Festplatte nach Beendigung eines Jobs oder beim Reset des Systems automatisch gelöscht.

Für Kunden mit erhöhtem Sicherheitsbedarf kommen bei Ricoh zertifizierte Lösungen zum Einsatz. Zuverlässigen Schutz gewährleistet dabei das Data-Overwrite-Security-Kit (DOS-Kit). Es löscht alle temporären Druck- und Kopierdaten, die auf der internen Festplatte des Systems gespeichert sind, direkt nach der Anwendung durch vielfache Überschreibung mit Null- und Zufallsdaten. Die Überschreibung wird automatisch gestartet, sobald der Druckauftrag abgeschlossen ist.

Ricoh bietet darüber hinaus die Möglichkeit, die MFP-Festplatten durch eine spezielle Löschstation nach verschiedenen Verfahren durch Überschreibung zu löschen. Hier kann zwischen einer siebenmaligen Überschreibung der Daten mit dem sogenannten BSI-Verfahren (Bundesamt für Sicherheit in der Informationstechnik) oder dem DoD Verfahren (Department of Defence) gewählt werden.

Kunden, die das DOS-Kit verwenden, können alternativ die gesamte Festplatte am Ende der Vertragslaufzeit bis zu neunmal mit Zufallszahlen überschreiben lassen.

Wo genau befinden sich Ihre Sicherheitslücken?



1 ERSTELLTE DOKUMENTE
Eine unautorisierte Person öffnet und betrachtet Ihr vertrauliches Dokument.

2 KOMMUNIKATION VON PC UND SYSTEM
Ein Außenstehender kann an den Drucker gesendete Daten abfangen.

3 DOKUMENTE
Jemand hat im Vorbeigehen Einsicht in die im Drucker-Ausgabefach liegenden Dokumente.

4 Jemand kopiert unerlaubt ein Dokument.

5 GERÄTENUTZUNG
Eine unautorisierte Person hat Zugang zum Gerät.

6 SCANNEN
Jemand sendet unrechtmäßig vertrauliche Dokumente mit der »Scan to E-Mail«- Funktion an eine falsche Adresse.

7 ARCHIVIERTE DOKUMENTE
Eine unbefugte Person verschafft sich Zugang zum Dokumentenserver.

8 KOMMUNIKATION VON PC UND SYSTEM
Jemand verschafft sich Zugriff auf den Datenstrom zwischen PC und Ausgabesystem.

9 DATEN AUF FESTPLATTE
Informationslecks aufgrund verbleibender Daten auf der Festplatte.

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

11 NETZWERK
Ein unautorisierter Außenstehender verschafft sich Zugang zum Netzwerk.

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

13 TELEFON-/FAXLEITUNG
»Anzapfen« von Telefon-/Faxleitungen.

14 CONTROLLING
Ineffiziente oder unerlaubte Nutzung von Netzwerkgeräten

15 ARCHIVIERTE DOKUMENTE
Ihre Daten sind verloren.

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 PrintTM: Druckfreigabe erfolgt erst nach Eingabe Ihres Passworts am Drucker. Verhindert unbefugtes Einsehen/Mitnehmen Ihrer vertraulichen Dokumente.
- 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, Basis- und Benutzercode)
- Authentifizierung über ein externes Gerät: Karte/PIN-Code
- Administratorauthentifizierung.

6 Sicheres Scannen

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

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

8 Verschlüsselung der Kommunikation für die Systemverwaltung mit SSL-Technologie (Secure Sockets Layer) oder mittels SNMP v3 zur Abwehr von Datendiebstahl.

9 Sicherung der Festplatte durch Überschreibung aller temporären Druck-, Kopier- und Scandaten (DOS-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 Sicherung kabelloser Netzwerkverbindungen (Wi-Fi) durch WPA2 AES (Wi-Fi Protected Access) und 802.1x.

13 Schutz gegen unbefugten Zugriff auf Telefon-/Faxleitungen durch Beendigung der Verbindung bei Verbingungsaufbau zum Teminal ohne gültiges G3-Protokoll.

14 Sichere Rückverfolgung

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

15 Planmäßige Backups zur Vermeidung des Verlusts archivierter Daten.

Das Dokument im Fokus

So unentbehrlich moderne Informationstechnologien im heutigen Arbeitsalltag auch sind, die potenziellen Risiken einer nicht ausreichenden Absicherung ihrer leistungsstarken Funktionen sind nicht zu unterschätzen.

In unserer vernetzten Arbeitswelt treten immer wieder neue Sicherheitsrisiken 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, jedoch umso gefährlicher.

Nachhaltige Sicherheit durch ISMS

Für Ricoh gehören die eigenen Informationen und die Informationen der Kunden zu den wichtigsten Werten, die das Unternehmen besitzt. Deshalb hat Ricoh ein Informationssicherheits-Managementsystem (ISMS) aufgebaut, das die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherstellt.

ISMS ist ein übergreifendes System zur Gewährleistung und Aufrechterhaltung der Informationssicherheit. Da es sich nicht nur auf die Sicherheit von Computersystemen beschränkt, bietet das 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, die zu einer nachhaltigen und kontinuierlichen Verbesserung des Systems beitragen.

Die Leitsätze für Informationssicherheit von Ricoh:

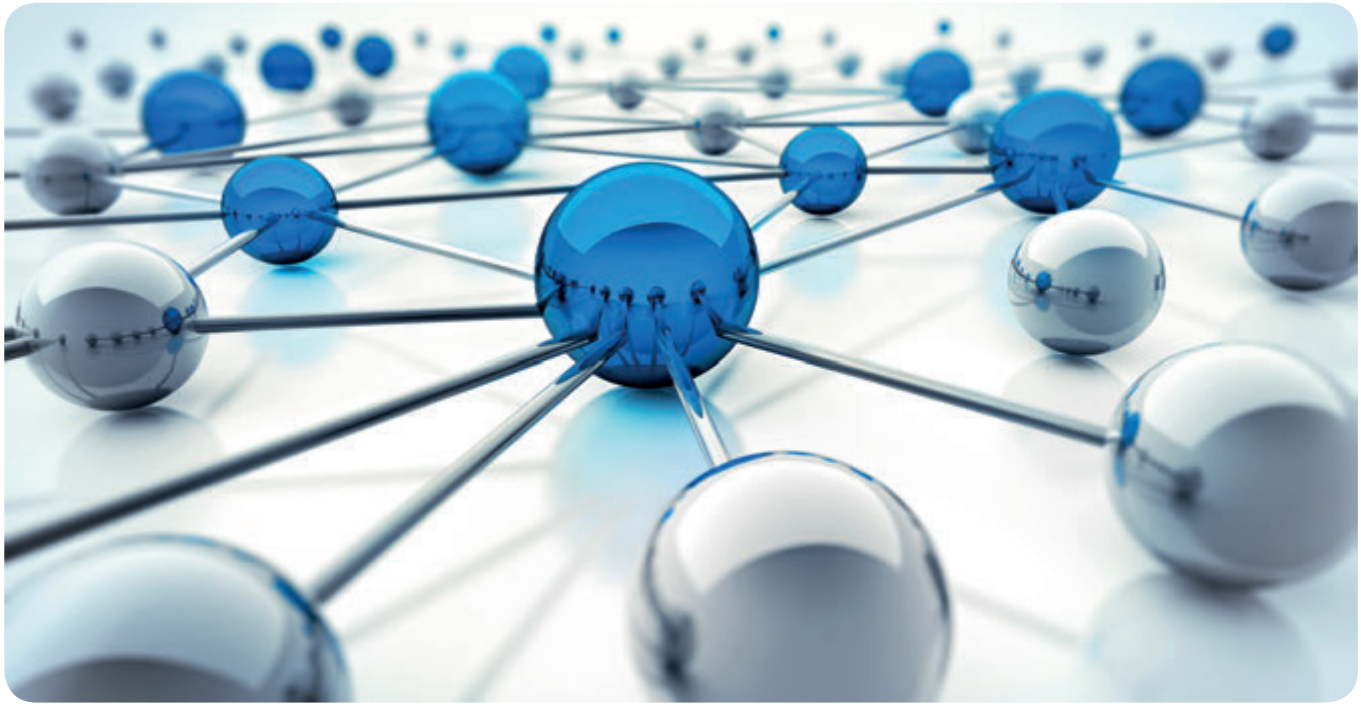
- Ricoh ist sich bewusst, dass allen Mitarbeiterinnen und Mitarbeitern eine entscheidende Rolle bei der Durchführung und Aufrechterhaltung des ISMS zukommt. Die Führungskräfte sind Vorbild und unterstützen ihre Mitarbeiterinnen und Mitarbeiter aktiv, damit diese ihrer Verantwortung im Bezug auf interne und externe Informationen nachkommen.

- Ein Schulungssystem stellt sicher, dass alle Mitarbeiterinnen und Mitarbeiter die erforderlichen Qualifikationen erlangen, um ihre Aufgaben in Übereinstimmung mit den Anforderungen des ISMS durchführen zu können.

- Informationsrelevante Gesetze und Richtlinien sowie vertragliche Vereinbarungen werden von Ricoh ermittelt, geprüft und umgesetzt.

- Durch ein Risikomanagement gewährleistet Ricoh die Angemessenheit und Wirksamkeit seiner Sicherheitsmaßnahmen und Managementpraktiken. Diese orientieren sich an den Auswirkungen eines möglichen Sicherheitsvorfalls bei Ricoh, seinen Kunden, Geschäftspartnern oder anderen Interessengruppen.

- Ricoh erfasst sicherheitsrelevante Vorfälle, prüft den Betrieb und die Effektivität des ISMS und strebt dessen kontinuierliche Verbesserung an.



Zertifizierte Sicherheit

Zertifizierung nach ISO 27001

Um unseren Kunden die volle Sicherheitsgarantie für unsere Produkte geben zu können, und gleichzeitig zu zeigen, dass unser Unternehmen insgesamt eine Organisation ist, welche den größten Wert auf Sicherheit, Integrität und Datenschutz legt, hat Ricoh Deutschland ein ISMS nach ISO 27001 erfolgreich eingeführt und implementiert. In regelmäßigen internen und externen Audits wird ständig überprüft, ob die im ISMS festgelegten Prozesse und Sicherheitsrichtlinien eingehalten werden.

Common Criteria (ISO15408)

Common Criteria ist ein international anerkannter Standard, der Sicherheitsanforderungen definiert und Verfahren zur Sicherheitsprüfung von IT-Systemen und Software festlegt. Diese standardisierten Prüfverfahren verifizieren die Produktangaben des jeweiligen Herstellers 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, Lieferung, Verkauf, Installation und Service.

Security Solutions

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. Ricoh bietet Ihnen eine umfassende Auswahl an nahtlos integrierbaren Sicherheitslösungen und eine ausgewiesene Kompetenz bei der Analyse potenzieller Sicherheitslücken in Ihren Arbeitsabläufen. Ricoh ist Ihr zuverlässiger Partner für den Schutz vertraulicher Daten und die Sicherheit Ihres gesamten Dokumenten-Workflows.

RICOH
imagine. change.

RICOH DEUTSCHLAND GmbH
Vahrenwalder Straße 315, 30179 Hannover
Telefon 0511 6742-0, Telefax 0511 6742-2100

www.ricoh.de

Artikelnummer 4202 / Stand: 12/2017