The Print Security Landscape, 2022

Securing the remote and hybrid workforce

Berichtsauszug: Konica Minolta
Januar 2022

QUOCIRCA

Zusammenfassung

Der Bericht "Global Print Security Landscape 2022" von Quocirca zeigt, dass viele Unternehmen Schwierigkeiten haben, mit den Anforderungen an die Drucksicherheit in der heutigen hybriden Arbeitsumgebung Schritt zu halten. Das Drucken von zu Hause aus führt zu neuen Sicherheitsproblemen, die durch den Schattenkauf von Geräten noch verschärft werden. Für kleine und mittelständische Unternehmen ist es schwieriger, mit den Herausforderungen der Drucksicherheit Schritt zu halten, was zu einer höheren Anzahl von druckbezogenen Datenverlusten führt. In der Folge geht Vertrauen in die Sicherheit der eigenen Druckinfrastruktur verloren, insbesondere bei kleinen und mittleren Unternehmen. Der Print Security Maturity Index von Quocirca zeigt jedoch, dass die als führend eingestuften Unternehmen, die eine Reihe von technologischen und unternehmenspolitischen Maßnahmen implementiert haben, weniger Datenverluste verzeichnen und ein größeres Vertrauen in die Sicherheit ihrer Druckinfrastruktur haben. Druckhersteller und Vertriebspartner müssen ihre Sicherheitsangebote für Unternehmen aller Größenordnungen erweitern, um ihren Kunden zu helfen, die Risiken in der anbrechenden Ära des hybriden Arbeitens zu minimieren.

Die Studie basiert auf den Ansichten von 531 IT-Entscheidern in den USA und Europa. 23 % der Befragten stammten aus kleinen und mittleren Unternehmen (250 bis 499 Mitarbeiter), 29 % aus mittelgroßen Organisationen (500 bis 999 Mitarbeiter) und 47 % aus Großunternehmen (1.000+ Mitarbeiter).

Die wichtigsten Ergebnisse auf einen Blick

- **Remote-Arbeiten ist auf dem Vormarsch und erzeugt eine erweiterte Bedrohungslandschaft.** Die Ansätze zur Sicherung der Druckumgebung aus der Zeit vor der Pandemie, die sich auf eine hauptsächlich statische, bürobasierte Belegschaft konzentrierten, müssen nun auf die Unterstützung von Mitarbeitern umgestellt werden, die abwechselnd Zeit im Büro und zu Hause verbringen. Es wird erwartet, dass durchschnittlich 44 % der Mitarbeiter von zu Hause aus arbeiten werden, wenn die Büros wieder uneingeschränkt genutzt werden dürfen. Hybride Arbeitsformen stellen die IT-Teams vor erhebliche Sicherheitsherausforderungen, da die Einstiegspunkte für Angriffe zunehmen. Die Verbreitung von Schatten-IT und ungesicherten Heimnetzwerken bedeutet, dass Unternehmen ihre Sicherheitsvorkehrungen in Bezug auf die Druckumgebung neu überdenken müssen.

- **IT-Security bleibt in den nächsten 12 Monaten die wichtigste Investitionspriorität.** 53 % der Befragten geben an, dass dies eine der drei höchsten Prioritäten ist. MPS (Managed Print Services) stehen an zweiter Stelle (41 %), gefolgt von Managed IT Services (38 %) und Cloud Services (35 %). 70 % der Unternehmen gehen davon aus, dass sie ihre Ausgaben für die Drucksicherheit in den nächsten 12 Monaten erhöhen werden, und nur 11 % erwarten einen Rückgang.

- **Die Abhängigkeit vom Drucken schafft einen Bedarf an wirksamer Drucksicherheit.** Trotz der raschen Digitalisierung im Laufe der Pandemie sind viele Unternehmen weiterhin auf das Drucken angewiesen. Für 64 % der Unternehmen wird das Drucken auch in den nächsten 12 Monaten wichtig oder sehr wichtig sein. 44 % gehen davon aus, dass das Druckvolumen im Büro zunehmen wird, und 41 % erwarten auch eine Zunahme des Druckvolumens zu Hause. Drucker und vernetzte Multifunktionssysteme stellen nicht nur ein Sicherheitsrisiko dar, wenn Unbefugte auf gedruckte Dokumente zugreifen, sondern auch, wenn sie ohne Absicherung in das Unternehmensnetzwerk eingebunden werden.

- **Nur ein Viertel (26 %) der Befragten ist davon überzeugt, dass ihre Druckinfrastruktur sicher sein wird, wenn die Büros wieder vollumfänglich genutzt werden.** Die Unternehmen haben Mühe, mit den Anforderungen an die Drucksicherheit Schritt zu halten: Mehr als die Hälfte (53 %) geben an, dass dies erheblich oder etwas schwieriger geworden ist. 67 % der Befragten sind besorgt über die Sicherheitsrisiken des Druckens von zu Hause aus, gegenüber 57 %, die sich über die Sicherheit des Druckens im Büro Sorgen machen.

- **Die Drucksicherheit steht auf der Sicherheitsagenda weiter unten als andere Elemente der IT-Infrastruktur.** Als größte Sicherheitsrisiken gelten Cloud- oder hybride Anwendungsplattformen, E-Mail, öffentliche Netzwerke und herkömmliche Endgeräte. Die privaten Drucker der Mitarbeiter stehen an fünfter Stelle der Sicherheitsrisiken (24 %), noch vor der Druckumgebung im Büro (21 %). Dies deutet auf ein mangelndes Bewusstsein und Bequemlichkeit hin, da die Sicherheitsschwachstellen im Zusammenhang mit Drucksystemen, die nach wie vor ein integraler Endpunkt in der IT-Umgebung aber auch Einstiegspunkt z.B. beim Scannen sind, nicht vollständig erkannt werden.

- **Es gibt deutliche Unterschiede zwischen MPS-Nutzern und Nicht-MPS-Nutzern.** Unternehmen, die einen MPS-Anbieter nutzen, erwarten ein viel größeres Wachstum des Druckvolumens und haben das größte Vertrauen in die Sicherheit ihrer Druckumgebung - obwohl sie sich der Risiken stärker bewusst sind. Sie geben auch doppelt so häufig an, dass die Bewältigung der Herausforderungen im Bereich der Drucksicherheit etwas oder sehr viel einfacher geworden ist. Die Sichtbarkeit und Kontrolle, die ein MPS bietet, scheinen die Sicherheitsbelastung für die Benutzer zu verringern. Zudem erhöhen sie die Gewissheit, dass Druckvolumen bedarfsbezogen kontrolliert variieren zu können, wodurch wiederum die Wahrscheinlichkeit sinkt, von einem Sicherheitsvorfall überrascht zu werden.

- **In den letzten 12 Monaten haben mehr als zwei Drittel (68 %) der Unternehmen Datenverluste aufgrund unsicherer Druckverfahren erlitten.** Dies hat zu durchschnittlichen Kosten von 758.878 Euro pro Datenschutzverletzung geführt. Solche bezifferten finanziellen Verluste sind für Unternehmen schon schlimm genug, aber sie haben auch viele andere negative Auswirkungen, wie den Verlust der Geschäftskontinuität, also auch länger anhaltende Geschäftsunterbrechungen nach einer Sicherheitsverletzung. Der Verlust von Kunden ist den Berichten zufolge am wahrscheinlichsten für kleine und mittlere Unternehmen. Bei großen Unternehmen ist die Wahrscheinlichkeit geringer, dass sie einen druckbezogenen Datenverlust erleiden: 36 % berichten, dass es keine Verstöße gab, im Vergleich zu 24 % der kleinen und mittleren Unternehmen. Der öffentliche Sektor ist am stärksten betroffen. Als Hauptgründe für Datenverluste wurden Schwachstellen im Zusammenhang mit Heimdruckern genannt, z. B. die unsichere Entsorgung vertraulicher Informationen durch Mitarbeitende oder das Abfangen von Dokumenten, die in der Druckumgebung zu Hause gespeichert sind.

- **Der Print Security Maturity Index von Quocirca zeigt, dass nur 18 % der Unternehmen als Print Security Leaders eingestuft werden können, weil sie Sicherheitsmaßnahmen in mehr als sechs maßgeblich relevanten Sicherheitsbereichen umgesetzt haben.** Die Zahl der führenden Unternehmen steigt auf 22 % in den USA und sinkt auf 12 % in Frankreich, das auch die höchste Zahl von Nachzüglern (37 %) aufweist. Diejenigen, die bei der Drucksicherheit führend sind, geben wahrscheinlich einen höheren Betrag für die Drucksicherheit aus, haben weniger Datenverluste zu beklagen und berichten von einem höheren Vertrauen in die Sicherheit ihrer Druckumgebung. Bei einem Vergleich nach Branchen ist der Anteil der führenden Unternehmen im Finanzsektor am höchsten (23 %).

- **Weniger als ein Drittel (28 %) der IT-Entscheider sind mit den Sicherheitsfunktionen ihres Druckdienstleisters sehr zufrieden.** Im öffentlichen Sektor sinkt dieser Wert auf 20 %. In den USA sind die Unternehmen am zufriedensten, in Deutschland am wenigsten. IT-Entscheider, die ein MPS nutzen, sind weitaus zufriedener (42 % sind sehr zufrieden) als diejenigen, die dies nicht tun (20 %).

- **Die meisten IT-Entscheider wenden sich an Anbieter von gemanagten Sicherheitsdiensten (Managed Security Service Providers, MSSPs), wenn sie Rat und Unterstützung bei der Drucksicherheit benötigen.** MSSPs sind für 35 % der Unternehmen die wichtigste Quelle für Sicherheitsberatung, in den USA sind es sogar 40 %. Nur 18 % der IT-Entscheider insgesamt würden sich an einen MPS-Anbieter wenden, wenn es um die Sicherheit von Druckern geht, während 21 % einen Druckerhersteller konsultieren würden. Dies zeigt, dass MPS-Anbieter und Vertriebspartner enger mit MSSPs zusammenarbeiten sollten.

- **CIOs und CISOs unterscheiden sich in ihren Ansichten über die Zukunft des Druckens und ihren Umgang mit den Sicherheitsherausforderungen im Zusammenhang mit der hybriden Druckumgebung.** CISOs sind optimistischer: 53 % bzw. 58 % erwarten einen Anstieg des Druckvolumens im Büro und zu Hause, verglichen mit 42 % und 40 % der CIOs. Bemerkenswert ist, dass CIOs (32 %) und CISOs (33 %) im Vergleich zu anderen IT-Befragten die größten Bedenken in Bezug auf das Drucken von zu Hause aus haben und es als zweitwichtigstes Sicherheitsrisiko einstufen. CIOs scheinen es auch schwieriger als CISOs zu finden, mit den Herausforderungen der Drucksicherheit Schritt zu halten - 61 % gaben an, dass sie es erheblich oder etwas schwieriger finden, im Vergleich zu nur 44 % der CISOs, von denen 29 % auch angaben, dass sie es etwas oder viel einfacher finden.

Anbieterprofil: Konica Minolta

Stellungnahme von Quocirca

Security ist ein wesentlicher Bestandteil des Konica Minolta Portfolios im Rahmen des intelligent vernetzten Arbeitsplatzes, das eine Reihe von Lösungen für die Anforderungen der digitalen Transformation von Unternehmen jeder Größe bietet. Das umfassende Security-Angebot geht über die Sicherheit eingebetteter Systeme hinaus und umfasst auch die Sicherheit von Dokumenten, Daten und Netzwerken. Nach eigenen Angaben verfügt das Unternehmen über ein breiteres Spektrum an Common Criteria/ISO 15408 EAL3-zertifizierten MFPs als jeder andere OEM und bietet Standardmaßnahmen zum Schutz von Dokumenten wie Datenverschlüsselung, sicheres Löschen, Kopierschutz mit Wasserzeichen und PDF-Signaturen. Zusätzlich zu seinem hardwarenahen Fokus auf Sicherheit hat Konica Minolta globale Partnerschaften mit HPE, Sophos und Microsoft geschlossen, um über seine Business-IT-Lösung Workplace Hub, Managed Infrastructure Services und Managed Application Services sowie Managed Security Services erstklassige Hardware-, Security- und IT-Lösungen anzubieten.

Besonders hervorzuheben sind die maßgeschneiderten Drucksystem Security Services - bizhub SECURE -, die seit 2011 angeboten und kontinuierlich ausgebaut werden, sowie die zusätzlichen Sicherheitsebenen, die durch die Optionen bizhub SECURE Platinum und bizhub SECURE Ultimate angeboten werden. Darüber hinaus hat Konica Minolta im vergangenen Jahr seine Kunden aktiv auf seine cloudbasierte Plattform für sicheres Druckmanagement umgestellt. Dies bietet flexible Optionen, je nachdem, ob ein Kunde eine vollständig in der Cloud gehostete oder eine hybride Cloud- und On-Premise-Infrastruktur sucht. Die Plattformen sind sowohl lokal als auch global verfügbar.

Ergänzt wird dies durch eines der umfangreichsten Angebote an IT-Services eines Druckerherstellers. Konica Minolta hat die Messlatte für die Integration von verwalteten IT-Services in ein traditionelles, druckerzentriertes Portfolio hoch gelegt. Der breit gefächerte Ansatz bietet einen umfassenden Service im Bereich der Cybersicherheit, der Unternehmen dabei hilft, das Eindringen in ihr Netzwerk zu erkennen, einzudämmen und zu analysieren, einschließlich Angriffen durch Malware, Ransomware oder Hacker. In Deutschland und Österreich bietet Konica Minolta im Rahmen von Security Consulting Angeboten Bewertungen der Cybersicherheit an. Auch regional spezifische Analysen der Cybersicherheit wie beispielsweise HIPAA-Bewertungen in den USA, um die Datenschutzanforderungen des Gesundheitssektors zu erfüllen, sowie Finanzbewertungen für Kommunalbanken, um die PCI-Compliance-Anforderungen zu erfüllen, sind im weltweiten Portfolio von Konica Minolta verankert.

Quocirca ist der Ansicht, dass sich Konica Minolta über sein traditionelles Drucksicherheitsangebot hinaus durch sein umfassendes Fachwissen im Bereich der IT-Services deutlich von einigen seiner wichtigsten Wettbewerber abhebt, insbesondere auf dem KMU-Markt. Eine Chance für Konica Minolta besteht darin, integrierte professionelle Cybersecurity Services zu entwickeln, die das Drucken umfassen und eingehende Sicherheitsbewertungen in einer Multivendor-Flottenumgebung (für Heim- und Bürogeräte) beinhalten. Durch die Nutzung seiner ausgereiften Managed-IT-Services-Kapazitäten und seiner IT-Expertise kann Konica Minolta potenziell eines der umfassendsten Angebote an Cybersecurity Services auf dem Druckermarkt anbieten.

Security Highlights

Umfassende Hardware-Sicherheit
Die Systeme von Konica Minolta erfüllen eine Reihe von Sicherheitszertifizierungen und wurden Penetrationstests unterzogen. So hat beispielsweise die bizhub i-Serie von Konica Minolta die Penetrationstests von NTT DATA, einem international führenden IT-Dienstleister, und der Sicherheitsabteilung von NTT Ltd. bestanden. Bei den Tests der Systeme wurden keine Schwachstellen gefunden. Darüber hinaus verfügen die bizhub-Multifunktionssysteme von Konica Minolta über eingebettete Sicherheitsfunktionen, die durch bizhub SECURE erweitert werden, was eine zusätzliche Ebene umfassenden Schutzes bietet.

Mit diesem Servicepaket bietet Konica Minolta die sichere Integration seiner MFPs in die Infrastruktur des Kunden an. Das bedeutet, dass dieser Service zum einen die sicherere Konfiguration der MFPs und Drucker entsprechend vordefinierter Konfigurationen beinhaltet. Konica Minolta betrachtet die jeweilige Kundenumgebung aber auch individuell und prüft, wie sich ihre Systeme optimal in die bestehende Kundenstruktur (z.B. E-Mail-Server, verwendete Protokolle) integrieren lassen und konfiguriert die Systeme nach den bestmöglichen Sicherheitsstandards. Andererseits gibt Konica Minolta gleichzeitig auch eine Empfehlung für eine sichere Umgebung ab (z.B. Empfehlung für ein sichereres Protokoll). Darüber hinaus findet eine permanente Sicherheitsüberwachung auf Einhaltung der definierten Standards statt.

bizhub SECURE unterstützt Endanwender bei der Einrichtung eines erweiterten Passwortschutzes und von Hardware-Sicherheitsmaßnahmen. Der bizhub SECURE-Dienst kann auf jedem Konica Minolta bizhub-Multifunktionssystem aktiviert werden, entweder vor Ort oder vor der Auslieferung. Zu den Funktionen gehören die Verschlüsselung des gesamten HDD/SSD-Inhalts, das Sperren der HDD/SSD und das Überschreiben temporärer Daten sowie das automatische Löschen von Daten in elektronischen Ordnern. bizhub SECURE Platinum und SECURE Ultimate bieten weitere Sicherheitsebenen wie Audit-Protokolle und regelmäßige System-Scans.

bizhub SECURE Ultimate enthält BitDefender-Technologie. Die optionale BitDefender Antiviren-Erweiterung scannt automatisch alle übertragenen und empfangenen Daten in Echtzeit auf potenzielle Malware und Viren, so dass sie vor externen Bedrohungen geschützt bleiben. Die Antiviren-Erweiterung benachrichtigt den Benutzer, wenn ein potenzielles Risiko für das MFP besteht, meldet, dass ein Virus erkannt wurde und blockiert den aktivierten Auftrag. Zusätzlich zum Echtzeit-Scan kann bei Bedarf ein manueller Scan zur Virenerkennung gestartet und ein zeitgesteuerter Virenscan nach individuellen Voreinstellungen aktiviert werden. Wichtig ist, dass diese Schutzfunktionalität unabhängig von der Anwendung funktioniert, aus der der Auftrag kommt. Sie schließt auch Verbindungen zur Cloud oder USB-Verbindungen ein und beeinträchtigt weder die Verarbeitungsleistung noch die Performance des MFP.

Konica Minolta bietet auch den bizhub SECURE Notifier an, der sicherstellt, dass die Einstellungen unverändert bleiben und das System in einem sicheren Zustand bleibt. Im Falle eines Vorfalls sendet die Anwendung eine Benachrichtigung und es können Gegenmaßnahmen ergriffen werden.

Sicherheitsorientierte Cloud Print Services
Das Konica Minolta Cloud Print Service Portfolio umfasst mehrere Optionen zur Unterstützung und Erhöhung der Sicherheit der Kunden. Die Sicherheit von Daten und Dokumenten wird durch Verschlüsselung und die Nutzung zertifizierter Datenzentren, Follow-me-Authentifizierung, rollenbasierte Zugriffskontrollen sowie kontrollierten Gastzugang gewährleistet. Um den allgemeinen Bedenken hinsichtlich Datenschutzes und Privatsphäre zu begegnen, beschränkt Konica Minolta die gemeinsame Nutzung von Daten. Nur Daten und Metadaten, die für die Ausführung eines Dienstes erforderlich sind, werden vom System erfasst und verarbeitet und mit geeigneten Technologien gesichert. Die Verwendung der TLS-Technologie gewährleistet, dass die Daten bei der Übertragung sicher sind, und die Akkreditierung nach ISO 27001 bietet eine unabhängige Garantie dafür, dass die Systeme nach den Sicherheitsgrundsätzen von Cloud-first entwickelt und betrieben werden und dass robuste Prozesse vorhanden sind, um Abwehrmechanismen aufzubauen und potenzielle Datensicherheitsprobleme zu vermeiden.

Erweiterte Remote Monitoring Services
Konica Minoltas Remote Monitoring und Management Services (RMM) bieten eine zentralisierte Überwachung und Verwaltung der IT-Infrastruktur, einschließlich Serverhardware, Speicher, von Konica Minolta bereitgestellte Anwendungen, Betriebssysteme und zugehörige Netzwerkinfrastruktur. Dies umfasst Bereiche wie Backup- und Antiviren-Services, Server- und Anwendungsüberwachung in Echtzeit, End-to-End-Audit-Trail für festgestellte Probleme und etwaige Interventionen von Konica Minolta, Management Services und regelmäßige server- und anwendungsspezifische Monitoring Services.

Auf lokaler Ebene und weltweit für seine Global Business Kunden bietet Konica Minolta Drucker- und MFP-Flottenbewertungen über Systemüberwachungs-Tools an, die auch jedes System eines Drittanbieters scannen, das die Standard-Drucker-MIB unterstützt. Die weltweit am häufigsten eingesetzte Plattform ist SiteAudit von Netaphor. Der SiteAudit Security Monitor scannt die Netzwerkeinstellungen und bietet ein Dashboard, das die gefährdeten Systeme auf der Grundlage eines Bewertungssystems für Netzwerkschwachstellen anzeigt. Die Echtzeitbewertungen weisen u.a. auf veraltete Einstellungen wie SNMP v1/v2, veralteten und abgelehnten SSL- und TLS-Einstellungen, FTP, SMBv1 usw. hin. Auf der Grundlage des Berichts über die Netzwerkschwachstellen bietet Konica Minolta seinen Kunden Empfehlungen und Dienste zum System- und Netzwerkschutz an. Zu den Empfehlungen gehören Änderungen der Port- und Protokolleinstellungen sowie Aktualisierungen der SNMP-Konfiguration.

Normalerweise benötigen Unternehmen Sicherheitsbewertungen für ihr gesamtes Netzwerk und die darin befindlichen Geräte - nicht nur für Drucker. Mit den Diensten von Konica Minolta wie Endpoint Protection, Threat Detection und MIDR bietet Konica Minolta dies an und plant den kontinuierlichen Ausbau des Angebots.

Portfolio an Security-Produkten und -Services

Hardware
Alle Konica Minolta Office- und Produktionsdrucksysteme entsprechen der ISO 15408. Die Produkte sind nach dem neuesten modernen, globalen Common Criteria-Standard zertifiziert - dem Hardcopy Protection Profile v1.0 - nach NIST/NIAP in den USA und JISEC/IPA in Japan.

Key Features sind:

- **Erkennung von Einbrüchen während der Laufzeit**
  - Bitdefender: zur Erkennung und Verhinderung des Eindringens von Malware
  - Schutz vor Firmware-Manipulationen: Erkennung und Unterbindung von Firmware-Manipulationen
  - SIEM: zur Analyse/Benachrichtigung über ein Eindringen
  - bizhub SECURE Notifier: zur Erkennung von Verletzungen der Sicherheitsrichtlinien durch unbefugten Zugriff (bald mit ShieldGuard)
- **Geräteüberwachung.** Fleet RMM: Fleet-Monitoring und -Management für eine breite Palette von Netzwerk- und Sicherheitsaspekten von Geräten. Das Tool bietet eine Funktion zur Verteilung von Gerätevorlagen für die gesamte Flotte sowie eine Scan- und Reset-Funktion. Das System überwacht die Geräteeinstellungen und wenn ein Gerät nicht mit der Vorlage übereinstimmt, bietet es die Möglichkeit, es zurückzusetzen und zu den ursprünglichen Vorlageneinstellungen zurückzukehren.
- **Sicheres Drucken durch Benutzerauthentifizierung.** Die Systeme unterstützen Passwort, ID-Karten-Authentifizierung sowie einen biometrischen Fingervenenscanner.
- **Kontoverfolgung.** Die Nutzung kann in der gesamten Flotte überwacht werden, und die Daten können zur Einhaltung der Vorschriften und zur Verfolgung von unbefugtem Zugriff verwendet werden.
- **Zugangskontrolle und Sicherheitsfunktionen.** Bieten mehr Sicherheit vor Bedrohungen und können auch zur Erleichterung einer besseren Verwaltung und verbesserten Rechenschaftspflicht eingesetzt werden.
- **Informationen protokollieren.** Ermöglicht die sofortige Erkennung von Sicherheitsverstößen und unterstützt die Abrechnung und Kostenzuweisung nach Benutzer und Abteilung.
- **Job Log Utility.** Bietet umfassende elektronische Protokolle zur Nachverfolgung von Benutzeraktivitäten.
- **Automatische Löschfunktion.** Löscht die auf der Festplatte gespeicherten Daten nach einer bestimmten Zeit.
- **Passwortschutz der internen HDD.** Das Auslesen der Daten auf der Festplatte erfordert nach dem Entfernen der Festplatte die Eingabe eines Passworts. Das Passwort ist mit dem System verknüpft, so dass die Daten nach dem Entfernen der Festplatte nicht mehr zugänglich sind.
- **Sicherheit des Inhalts.** Copy Guard ist eine Kopierschutzfunktion, die verdeckte Sicherheitswasserzeichen wie "Privat" oder ein Datum im Hintergrund druckt, um unbefugtes Kopieren zu verhindern, und ein Kopierschutzmuster auf allen gedruckten Blättern einbettet. Wird mit einem System, das die Copy Guard Funktion unterstützt, versucht, ein kopiergeschütztes Blatt zu kopieren, wird ein Kopierschutzmuster gescannt, der Kopiervorgang abgebrochen und der Auftrag gelöscht. Externe Print Management Anwendungen können so programmiert werden, dass sie die Übertragung blockieren, wenn das gescannte oder gedruckte Dokument sensible oder vertrauliche Informationen enthält.
- **bizhub.** Der *bizhub SECURE* Service kann auf jedem Konica Minolta bizhub-Multifunktionssystem der i-Serie aktiviert werden, entweder vor Ort oder vor der Auslieferung.

- **bizhub SECURE:**
  - Änderung des Admin-Passworts
  - Verschlüsselung des gesamten HDD/SSD-Inhalts
  - Sperrung von HDD/SSD
  - Überschreiben temporärer Daten
  - Automatischen Auftragslöschung
  -
- **bizhub SECURE Platinum:**
  - Ändern des Administrator-Passworts
  - Verschlüsseln des gesamten Inhalts der bizhub-Festplatte
  - Erstellen eines sicheren alphanumerischen Kennworts zum Sperren der bizhub-Festplatte
  - Time bizhub Multifunktionssystem zum automatischen Löschen von Material in elektronischen Ordnern
  - Deaktivieren von unsicheren und unerwünschten Services, Protokollen und Ports
  - Aktivieren von SSL auf dem bizhub (selbstsigniertes Zertifikat)

- Aktivieren der Netzwerkbenutzer-Authentifizierung und der automatischen Abmeldung von Benutzer- und Administratorkonten
- Aktivierung der Audit-Protokolle

- **bizhub SECURE Ultimate:**
  - Ändern des Administrator-Passworts
  - Verschlüsseln des gesamten Inhalts der bizhub-Festplatte
  - Erstellen eines sicheren alphanumerischen Kennworts zum Sperren der bizhub-Festplatte
  - Time bizhub Multifunktionssystem zum automatischen Löschen von Material in elektronischen Ordnern
  - Deaktivieren von unsicheren und unerwünschten Services, Protokollen und Ports
  - Aktivieren von SSL auf dem bizhub (selbstsigniertes Zertifikat)
  - Aktivieren der Netzwerkbenutzer-Authentifizierung und der automatischen Abmeldung von Benutzer- und Administratorkonten
  - Aktivierung der Audit-Protokolle
  - Aktivierung von Echtzeit-Scanning
  - Einrichten regelmäßiger Scanzeiten

Über Quocirca

Quocirca ist ein globales Marktforschungsunternehmen, das sich auf die Analyse der Konvergenz von Print und Digital Technologien am zukünftigen Arbeitsplatz spezialisiert hat.

Seit 2006 spielt Quocirca eine einflussreiche Rolle bei der Beratung von Kunden im Hinblick auf die großen Veränderungen auf dem Markt. Unsere Beratungs- und Forschungsleistungen stehen an der Spitze des sich schnell entwickelnden Marktes für Druckdienstleistungen und -lösungen und genießen das Vertrauen von Kunden, die nach neuen Strategien für den Umgang mit bahnbrechenden Technologien suchen.

Quocirca hat in vielen Bereichen der aufstrebenden Märkte Pionierarbeit geleistet. Vor mehr als 10 Jahren waren wir die ersten, die die Marktlandschaft für Managed Print Services (MPS) analysiert haben, gefolgt von der ersten globalen Wettbewerbsanalyse des Marktes für Drucksicherheit. In jüngster Zeit hat Quocirca seinen führenden und einzigartigen Ansatz auf dem Markt untermauert und die erste Studie veröffentlicht, die sich mit der intelligenten, vernetzten Zukunft des Drucks am digitalen Arbeitsplatz befasst. Die Studie Global Print 2025 bietet einen unvergleichlichen Einblick in die Auswirkungen der digitalen Umwälzungen, sowohl aus der Sicht von Führungskräften der Branche als auch aus der Perspektive der Endverbraucher.

Weitere Informationen unter: www.quocirca.com.

Haftungsausschluss:
Dieser Bericht wurde von Quocirca unabhängig verfasst. Während der Vorbereitung dieses Berichts hat Quocirca mit einer Reihe von Lieferanten gesprochen, die in den behandelten Bereichen tätig sind. Wir bedanken uns für ihre Zeit und ihre Erkenntnisse.

Quocirca hat bei der Erstellung dieser Analyse Informationen aus verschiedenen Quellen erhalten. Diese Quellen umfassen die Anbieter selbst, sind aber nicht beschränkt auf sie. Obwohl Quocirca versucht hat, die von den einzelnen Anbietern erhaltenen Informationen so weit wie möglich zu überprüfen, kann Quocirca nicht für etwaige Fehler in den gelieferten Informationen verantwortlich gemacht werden.

Obwohl Quocirca alle möglichen Schritte unternommen hat, um sicherzustellen, dass die in diesem Bericht enthaltenen Informationen wahrheitsgetreu sind und die tatsächlichen Marktbedingungen widerspiegeln, kann Quocirca keine Verantwortung für die endgültige Zuverlässigkeit der Angaben übernehmen. Quocirca lehnt daher ausdrücklich alle Garantien und Ansprüche in Bezug auf die Gültigkeit der hier präsentierten Daten ab, einschließlich aller Folgeschäden, die einer Organisation oder Person entstehen, die auf der Grundlage dieser Daten handelt.

Alle Marken- und Produktnamen sind Warenzeichen oder Dienstleistungsmarken der jeweiligen Inhaber.