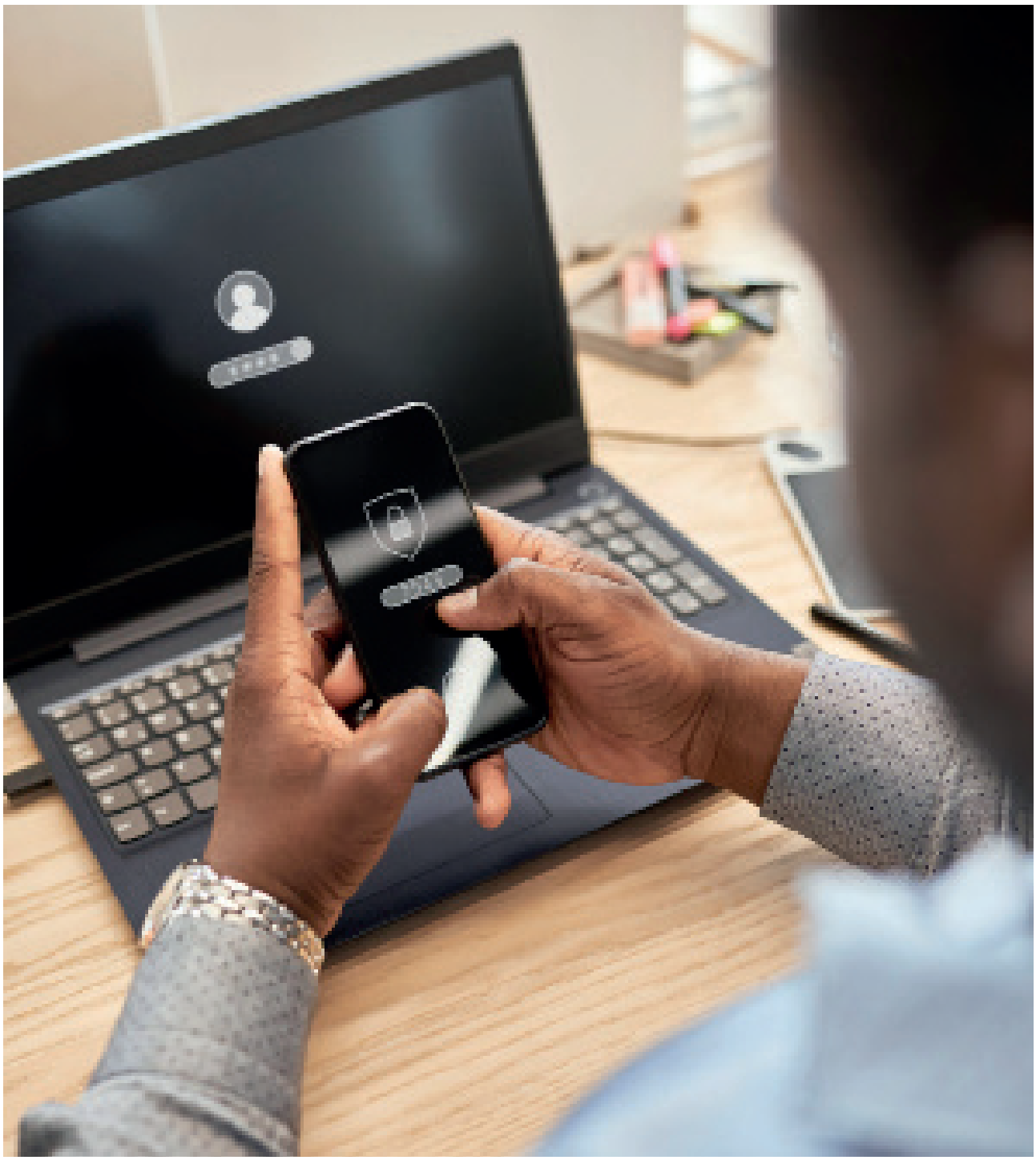


Canon

SICHERHEIT VON A BIS Z

SICHERHEIT VON A WIE AUTHENTIFIZIERUNG BIS Z WIE ZERO TRUST

Ein Whitepaper von IT-Management.today

Cyberattacken sind allgegenwärtig und treffen Unternehmen aller Branchen und Größen. Laut einer aktuellen Bitkom-Studie waren 72 % der Unternehmen in Deutschland im Jahr 2023 von Diebstahl, Industriespionage oder Sabotage betroffen – mit einer Gesamtschadenssumme von über 200 Milliarden Euro.

Einfallstore für solche Bedrohungen gibt es viele, allen voran unsichere Passwörter, veraltete Softwareversionen und schlecht konfigurierte Netzwerke.

Was jedoch oft übersehen wird: Auch Multifunktionsgeräte wie Drucker sind beliebte Angriffspunkte. Laut der Print Security Landscape 2023 von Quocirca waren 61 % der Datenverluste im vergangenen Jahr sogar unmittelbar mit dem Dokumentendruck verbunden.

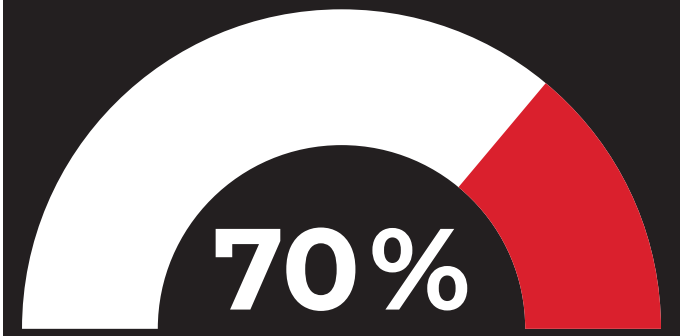
Verwunderlich ist dies nicht, denn heutige Drucker sind Hochleistungswerkzeuge mit Betriebssystemen sowie ans Netzwerk und Internet angeschlossenen Festplatten. Verstärkt wird die Anfälligkeit der Unternehmen noch durch Remote-Arbeit: Private Drucker im Homeoffice, die bei Firmware-Updates nicht berücksichtigt werden, stellen ein potenzielles Risiko dar.

Spätestens hier wird klar: Drucker können als Einfallstor das gesamte Unternehmen gefährden. Deshalb heißt es, Drucklösungen und Unternehmenssysteme gleichermaßen gut zu schützen. Wie dies gelingt, verraten wir Ihnen im Folgenden.

61%

Die Mehrheit der Unternehmen erlitt einen Datenverlust, der direkt mit dem Druck von Dokumenten verbunden war

Unternehmen werden weiterhin nicht auf das Drucken verzichten können.



geben an, dass der Druck im nächsten Jahr entscheidend oder sehr wichtig für ihr Geschäft sein wird

Durchschnittlich

27 %

der IT-Sicherheitsvorfälle sind unmittelbar mit Dokumenten im Papierformat verknüpft

Die Top 3 der Herausforderungen in der Drucksicherheit:

1. **Aufrechterhalten der Sicherheit von Druckmanagement-Software**
2. **Schutz vertraulicher/ sensibler Informationen vor dem Druck**
3. **Gewährleisten eines sicheren Druckens in Heim- und Remote-Umgebungen**

5 SCHUTZFAKTOREN FÜR DIE UNTERNEHMENS-SICHERHEIT

Für eine umfassende Sicherheit sowohl der Drucklösung als auch der Unternehmenssysteme sorgen insbesondere folgende Maßnahmen:

1 Schutzfaktor 1: Informationssicherheit

Informationssicherheitslösungen sind elementar, wenn es darum geht, Daten jederzeit vor unbefugtem Zugriff und Verlust zu schützen und die Einhaltung von Vorschriften in jeder Phase des Dokumentenlebenszyklus zu gewährleisten. Zu einem ganzheitlichen Informationssicherheitsansatz gehören vor allem diese Aspekte:

Zentrales Flottenmanagement:
Spezifische Systemmanagement-Software ermöglicht es, Systemeinstellungen, Sicherheitsrichtlinien, Kennwörter, Zertifikate und Firmware zu aktualisieren und netzübergreifend auf die Druckerflotte zu übertragen.

So spart das IT-Team wertvolle Zeit. Zugleich ist die Sicherheit der Unternehmensinfrastruktur jederzeit auf dem neuesten Stand.

Managed Print Services:
Managed Print Services unterstützen dabei, die Druckerinfrastruktur kontinuierlich zu optimieren und Effizienzen stetig zu steigern.

Zu den Dienstleistungen gehören etwa die detaillierte Analyse der Druckund Dokumentenworkflows, maßgeschneiderte digitale Transformationsstrategien und die regelmäßige Wartung der Druckerflotte.

Nutzerzugangskontrollen:
Zugangskontrollen stellen sicher, dass der Druck erst nach Authentifizierung des Nutzers (etwa über PIN-Codes) erfolgt. So können lediglich autorisierte Personen auf Druckjobs und gespeicherte Dokumente zugreifen, und vertrauliche Dokumente bleiben nicht mehr unbeaufsichtigt im Ausgabefach liegen. Zudem verbessern sich so die Haftungs- und Kontrollmöglichkeiten.

Verschlüsselung:
Ebenfalls unabdingbar ist die Verschlüsselung der Daten – sowohl bei der Übertragung zwischen dem Drucker und dem verbundenen Gerät (z. B. dem PC) als auch bei der Speicherung auf den Druckern selbst. Dies schützt die Daten vor unbefugtem Zugriff und beugt Datenverlust vor.

Zusatzfunktionen:
Weitere Funktionen sorgen für ein zusätzliches Quantum an Sicherheit. So etwa die Beschränkung der Sendeziele (etwa auf solche im Adressbuch oder bestimmte Domains) oder die Deaktivierung der automatischen Adressvervollständigung, die den Versand von Dokumenten an falsche Ziele verhindert.

2 Schutzfaktor 2: Systemsicherheit

Systemsicherheit ist ein entscheidender Faktor für das Aufrechterhalten des Geschäftsbetriebs und den Schutz sensibler Daten. Unternehmen sollten unter anderem diese Vorkehrungen treffen, damit ihre Systeme rundum sicher sind:

Schutz der Geräte:
Ein absolutes Muss sind regelmäßige Updates für sowohl die Firmware als auch die Software der Drucker. Nur so lassen sich Sicherheitslücken zeitnah schließen, so dass Hackern & Co. keine Angriffsfläche mehr geboten ist.

Zero-Trust-Netzwerke:
Die Drucker sollten in ein Netzwerk integriert sein, das dem Zero-Trust-Prinzip folgt. Bei diesem Ansatz wird jedes Gerät auf seine Zugriffsrechte überprüft. So können nur autorisierte Drucker auf das Druckernetzwerk zugreifen.

Proaktive Überwachung und Protokollierung:
Eine Überwachung der Druckaktivitäten und Protokollierung dieser erlaubt es, verdächtige Vorgänge frühzeitig zu erkennen und schnell auf Sicherheitsvorfälle zu reagieren.

Zugriffskontrollsysteme:
Ebenfalls sinnvoll ist es, über entsprechende Systeme festzulegen, wer Zugriff auf welche Drucker erhält. So lässt sich der Zugang zu sensiblen Informationen kontrollieren. Einschränkungen auf Abteilungsoder Projektebene können zusätzlich zur Sicherheit beitragen.

Sicherer Remote-Zugriff:
Verschlüsselte Verbindungen und sichere Netzwerkprotokolle wie WPA3 und VPN gewährleisten eine sichere Kommunikation und verschaffen Remote-Mitarbeitern einen zuverlässigen sowie störungsfreien Zugang zu den Druckern.

3 Schutzfaktor 3: Sichere Hard- und Software

Für den Schutz der IT-Infrastruktur sind sowohl sichere Hardwarelösungen als auch zukunftsweisende Software von zentraler Bedeutung:

Sichere Hardwarelösungen:
Mit modernsten Sicherheitstechnologien ausgestattete Drucker, Scanner und multifunktionale Systeme sind das A und O für umfassenden Schutz.

Sichere Business-Software:
Moderne Business-Software sorgt für Integrität und Authentizität geschäftlicher Dokumente und Daten. Systemsignaturen an PDF- oder XPS-Scans etwa erlauben es, die Herkunft und Echtheit des Dokuments zu überprüfen. Eine an der Datei angebrachte digitale Nutzersignatur wiederum ermöglicht es, den Unterzeichner eindeutig zu identifizieren.

4 Schutzfaktor 4: Security Services

Fortschrittliche Sicherheits-Services sind unerlässlich, um die IT-Infrastruktur gegen vielfältige digitale und physische Bedrohungen zu schützen. Zu den geeigneten Maßnahmen zählen vor allem die folgenden:

Maßgeschneiderter Schutz für die IT-Infrastruktur über den gesamten Lebenszyklus:
Dazu zählt das automatische Aufspielen von Firmware-Updates ebenso wie fortschrittliche Bedrohungserkennung, kontinuierliche Überwachung und schneller Support, der Sicherheitslücken rasch schließt und die IT-Infrastruktur optimiert.

Device Hardening Service:
Ein solcher Service hilft dabei, sicherheitsrelevante Features optimal zu konfigurieren.

Dies minimiert die Angriffsfläche und stärkt die Gesamtresilienz der IT-Infrastruktur. Optionen reichen idealerweise von Basiskonfigurationen zum Schutz gegen allgemein bekannte Bedrohungen bis hin zu maßgeschneiderten Varianten.

Data Removal Services:
Auch das Data Removal am Ende der Nutzungsdauer gehört zu einem hochklassigen Service. Bei diesem werden alle Daten von den Druckgeräten entfernt und Geräte wieder in den Auslieferungszustand versetzt.

79 %
der Unternehmen investieren in die Printinfrastruktur

35 %
haben Probleme bei der Aktualisierung der Firmware

54 %
wollen ein allumfassendes System (egal, ob vom Systemhaus oder Printing-Experten)

5 Schutzfaktor 5: Absichern der IT-Infrastruktur

Sichere Drucklösungen (s. Schutzfaktoren 1–5), sind jedoch nur ein Teil der Wahrheit. Zu einer umfassenden Unternehmenssicherheit zählt auch die Cybersecurity. Umso wichtiger wird diese im Hinblick auf die EU-Richtlinie NIS2, die ein einheitliches Schutzniveau gegen Cyberangriffe auf kritische Infrastrukturen (KRITIS) schaffen soll.

Was genau ist NIS2?
NIS2 berührt ca. 30.000 deutsche KRITIS-Institutionen und -Unternehmen mit mindestens 50 Mitarbeitern oder einem Jahresumsatz von 10 Millionen EUR, die als „besonders wichtig“ (essential) oder „wichtig“ (important) eingestuft sind. Betroffene Einrichtungen müssen sowohl die Betriebskontinuität sicherstellen als auch eine wirksame Reaktion auf solche Bedrohungen gewährleisten.

Dazu gehört auch die Umsetzung angemessener Sicherheitsmaßnahmen zum Schutz ihrer Netzwerk- und Informationssysteme. Ebenso verpflichtet NIS2 KRITIS-Betreiber dazu, dafür zu sorgen, dass auch ihre Lieferkette keine Angriffspunkte für Hacker & Co. bietet – und wirkt sich daher auf weitaus mehr Unternehmen als nur KRITIS aus.

Auf Cybersicherheit spezialisierte Unternehmen bieten dahingehend umfassende Lösungen: den Schutz vor Malware und Phishing sowie Managed-Detection-and-Response-Dienste (MDR). Bei Managed Detection and Response (MDR) handelt es sich um einen umfassenden Sicherheitsdienst, der fortschrittliche Bedrohungen durch eine Kombination aus menschlicher Expertise und innovativer Technologien wie Machine-Learning-Modellen erkennt und darauf reagiert.

Der Service umfasst Rund-umdie-Uhr-Überwachung, das Erkennen selbst hochkomplexer, manuell gesteuerter Hackerangriffe und die Analyse und Reaktion auf Sicherheitsvorfälle durch ein spezialisiertes Team von Sicherheitsexperten. Ziel ist es, Bedrohungen schnell zu erkennen, zu analysieren und zu neutralisieren, um die IT-Infrastruktur eines Unternehmens zu schützen und Sicherheitsvorfälle effektiv zu managen. Solche Tools und Services unterstützen die Einhaltung der NIS2-Richtlinie und gewährleisten die Sicherheit der Unternehmensinfrastruktur.

360-SICHERHEITSLÖSUNGEN AUS EINER HAND

Auch der Drucker ist nicht mehr als ein spezialisierter Computer – und als solcher in Sicherheitskonzepten zu berücksichtigen. Für besonders hohe Sicherheit sorgt eine 360°-Lösung aus einer Hand, die Systeme und Netzwerke schützt, die Vertraulichkeit und Integrität von Dokumenten gewährleistet und zudem Schutz vor Cyberangriffen leistet. Durch integrierte Maßnahmen wie Authentifizierung, Systemverwaltung, vorausschauende Sicherheit und Zugangskontrollsysteme bietet Canon umfassende Sicherheit mit modernsten Technologien. Gemeinsam mit starken Partnern bietet Canon bestmögliche Sicherheit. So ist Ihr Unternehmen beim Drucken optimal geschützt – von A wie Authentifizierung bis Z wie Zero Trust.

Sie möchten mehr über unsere Services erfahren?
Ihr Canon-Ansprechpartner vor Ort berät Sie gern!

Canon Deutschland GmbH
Europark Fichtenhain A10
47807 Krefeld
Tel.: +49 2151 3450
canon.de

© Canon Deutschland GmbH
Stand: 2024

Diese Whitepaper wurde für die Canon Deutschland GmbH erstellt von **„IT-Management“, dem Fachportal der Business.today Network GmbH**