e-dox
2023

WHITEPAPER

7 SCHRITTE ZUM SCHUTZ IHRER SCAN- & DRUCKDATEN

www.e-dox.de

Sicherheitsrisiko Drucker

Ihr Unternehmen ist schon einmal Opfer eines Cyberangriffs geworden? Dann sind Sie damit nicht allein.
Jedes Jahr werden zahlreiche Unternehmen in Deutschland gehackt, beliebtes Einfallstor: der Drucker. Denn trotz der offensichtlichen Einbindung ins Netzwerk werden diese Geräte in den IT-Sicherheitsarchitekturen oft vernachlässigt, mit teils erheblichen Auswirkungen auf die strukturelle Daten- und Dokumentensicherheit.

Mit welchen einfachen Schritten Sie dies verhindern und Ihre Datenschutz- und Compliance-Richtlinien sicherstellen, erfahren Sie hier.

Alles auf einen Blick...

Zentrale Administration 1

Eine hohe Anzahl an Druck- und Scanhardware bedeutet einen enormen manuellen Aufwand, wenn es darum geht, Konfigurationsänderungen oder Sicherheitsupdates geräteübergreifend vorzunehmen. Es ist daher gerade bei größeren Druckerflotten sinnvoll, alle Geräte zentral zu managen.

Dank dieser Vereinheitlichung lassen sich neben Sicherheits- oder Funktionsupdates auch Verbrauchsmaterialbestellungen einfacher organisieren. Gleichzeitig werden Schwachstellen im System besser überwacht und Sicherheitsberichte zuverlässiger bereitgestellt.

Ihr Vorteil...

Ein zentrales Management gewährleistet, dass kein Drucker innerhalb der Sicherheitsarchitektur vergessen wird. Gleichfalls werden Fehlerquellen durch eine gezieltere Verwaltung - beispielsweise von Sicherheitsupdates - reduziert.

2 Zugriffsrechte im Druckprozess

Wie bei anderen Netzwerkkomponenten sollten auch bei Druckern und Multifunktionsdruckern (MFPs) die Zugriffsrechte verwaltet und kontrolliert werden, da sonst sensible Netzwerkeinstellungen unbemerkt verändert werden können.

So können IT-Administratoren beispielsweise den Zugriff auf die Netzwerkeinstellungen per Passwort beschränken. Gleichzeitig verfügen die meisten Netzwerkdrucker oder MFPs heute über eine individuell konfigurierbare Bedienfeldsperre, die verhindert, dass wichtige Einstellungen am Gerät verändert werden.

Ihr Vorteil...

Durch das Definieren von Zugriffsrechten auf Netzwerkeinstellungen erhöhen Sie die gesamte Netzwerksicherheit bei gleichbleibender Funktionalität für alle Mitarbeiter.

Druck- & Scandaten verschlüsseln 3

In den meisten Fällen werden die Druck- und Scandaten zwischen Client und Computer unverschlüsselt versendet. Das bedeutet, dass diese Datenströme von anderen Rechnern abgefangen, eingesehen oder sogar verändert werden können - ein Albtraum für die Sicherheit Ihrer vertraulichen Informationen!

Verschlüsselungen und Überwachungstools schützen diese Daten und Dokumente vor dem unbefugten Zugriff Dritter. Zusätzlich lassen sich auch spezielle Netzwerksniffer verwenden. Dabei handelt es sich um Programme, welche den Datenaustausch im Netzwerk analysieren und frühzeitig verdächtige Aktivitäten erkennen.

Ihr Vorteil...

Mittels Verschlüsselung Ihrer Druck- und Scandaten erschweren Sie unbefugten Dritten das Auslesen von Dokumenten, beugen Datendiebstahl vor und sichern Ihre unternehmerischen Compliance-Standards.

4 Sichere Authentifizierung

Für einen zuverlässigen Schutz Ihrer Daten vor unautorisiertem Zugriff sind sichere Nutzer-authentifizierungen bei Ihren Netzwerkdruckern unerlässlich. Egal ob über PIN, Chipkarte oder Fingerabdruck-Sensor - die individuellen Authentifizierungsverfahren stellen sicher, dass nur berechtigte Personen Zugriff auf sensible Daten haben.

Damit lässt sich vor allem der unternehmensinterne Umgang mit schützenswerten Informationen absichern. Gleichzeitig hilft die Zuordnung des Druckvolumens zu den verschiedenen Kostenstellen dabei, versteckte Optimierungspotenziale im Dokumentenmanagement oder beim Ressourcenverbrauch offen zu legen.

Ihr Vorteil...

Mit sicheren Nutzerauthentifizierungen erhalten nur berechtigte Personen Zugriff auf bestimmte Funktionen. Dies gewährleistet die Sicherheit Ihrer Druck-, Scan- und Kopiervorgänge und ermöglicht eine präzise Kostenkontrolle.

Pull-printing & Follow-me 5

Aufbauend auf Schritt 4 empfiehlt sich die Nutzung von Pull-printing, beziehungsweise Follow-me-printing. Dabei startet der Druck erst dann, wenn der Mitarbeiter sich am Gerät authentifiziert hat. Die übertragenen Druckdaten verbleiben währenddessen sicher auf dem Printserver, bis der Anwender sie an einem beliebigen Endgerät abruft.

Dieses Verfahren ist gerade für Bereiche interessant, in denen viel mit personenspezifischen oder vertraulichen Daten gearbeitet wird. Pull-printing stellt dabei sicher, dass gedruckte Dokumente nur für die im System hinterlegten Personen zugänglich sind, während ganz nebenbei auch unnötige, fehlerhafte Druckaufträge und Warteschlangen reduziert werden.

Ihr Vorteil...

Dank Pull-printing verbleiben vertrauliche Dokumente geschützt auf dem Printserver, bis die autorisierte Person das jeweilige Dokument freigibt. Dies sichert den Datenschutz und hilft dabei, die Druckkosten umfassend zu reduzieren.

6 Strategische Tools

Moderne Druck- und Outputmanagement-Systeme sorgen nicht nur für eine sichere Dokumentenausgabe, sondern erleichtern auch die unternehmensweite Kostenkontrolle bei Druck-, Kopier- und Scan-Diensten. Mit diesen Tools lassen sich schnell detaillierte Berichte über die Druckernutzung erstellen.

So können Auslastung, die am häufigsten genutzten Anwendungen und der Farbverbrauch einfach erfasst und analysiert werden. Dies hilft konkret dabei, einfacher strategische Entscheidungen hinsichtlich der Workflow-Organisation vordefinierter Gruppen oder der intelligenten Auslastung der vorhandenen Druckressourcen zu treffen.

Ihr Vorteil...

Management-Tools helfen bei der effizienteren Ressourcennutzung im Unternehmen und unterstützen Sie bei der sicheren Ausgabe vertrauenswürdiger oder datenschutzrelevanter Dokumente.

Fälschungssichere Technologien 7

Mittels einer Authentifizierung durch maschinenlesbare Codes, einer automatischen Kennzeichnung von Kopien oder dem Druck mit Sicherheitstoner können Sie sicherstellen, dass Ihre Dokumente vor Manipulation geschützt sind.

Dieser Schritt empfiehlt sich vor allem dann, wenn nicht nur die Daten schützenswert sind, sondern die Integrität des Dokumentes an sich gewährleistet werden muss. Gerade in solchen Fällen sollte auch ein besonderer Wert auf die reibungslose Absicherung des gesamten Netzwerks gelegt werden, um die Sicherheitsansprüche im Dokumentenprozess vollumfänglich zu gewährleisten.

Ihr Vorteil...

Die Einführung mehrstufiger Sicherheitsverfahren und fälschungssicherer Technologien bietet ihnen höchste Dokumentenintegrität und umfassenden Schutz vor Datendiebstahl und unbefugten Zugriffen auf sensible Informationen.

8 Zusammenfassung

Obwohl der Drucker längst als integraler Bestandteil des Netzwerks gilt, wird seine Rolle bei der Sicherung sensibler Daten oft unterschätzt. Professionelle Hersteller wie Xerox haben längst vorgesorgt und integrieren ab Werk zahlreiche Sicherheitsfeatures. Administratoren sollten diese jedoch auch aktiv nutzen und überwachen, indem sie turnusmäßig Passwörter neu setzen, Zugriffsrechte verwalten und Daten verschlüsseln. Authentifizierungsverfahren und Follow-me-Print sorgen währendessen dafür, dass Dokumente nur für autorisierte Personen zugänglich sind. Eine automatisierte Lösung zur Kontrolle der Druck- und Scanumgebung entlastet IT-Verantwortliche und schützt Unternehmen langfristig vor Datendiebstahl und Datenmissbrauch.

Sie haben Fragen...?

...dann hilft Ihnen unser Team gern weiter!

Profitieren Sie von über 20 Jahren Erfahrung im Bereich Multifunktionsdrucker, digitale Transformation und IT-SIcherheit.

e-dox GmbH
Beckerstraße 13
09120 Chemnitz
+49 371 40084-0