BLOSS EIN DRUCKER?

DAS UNERKANNTE SICHERHEITSRISIKO.

Schliessen Sie Ihre Sicherheitslücke!

Cyber-Kriminelle haben Bürodrucker und Multifunktionssysteme als leichtes Ziel für Attacken identifiziert. Viele dieser Systeme sind mit dem Internet verbunden und unzureichend gesichert. Daher können sie – genau wie Computer und Server – von ausserhalb Ihres Netzwerks gehackt werden. Wir möchten Sie für dieses Thema sensibilisieren und darüber informieren, wie Sie sich bestmöglich gegen Cyber-Angriffe schützen können.

Warum hacken Cyber-Kriminelle sich in Druckinfrastrukturen ein?

Antwort: Ungesicherte Drucker stellen eine offene Hintertür zu Ihrem Netzwerk dar. Cyber-Kriminelle tarnen beispielsweise Malware in Form eines Treiber-Updates und können – sobald dieses installiert wird – auf sensible Daten und Passwörter zugreifen.

Drei potenzielle Sicherheitslücken an Drucksystemen

1. Ungesicherte Festplatten

Wenn Sie eine Datei an einen Drucker oder ein Multifunktionsgerät (MFD) senden, wird sie in vielen Fällen auf der Festplatte des Druckers gespeichert. Wenn diese nicht verschlüsselt ist, kann die Datei gefährdet sein.

2. Ungesicherte Drucker-Ports

Über offene Drucker-Ports können Hacker die Endgeräteerkennung umgehen und Ihr Netzwerk dahingehend manipulieren, dass sie Administratorrechte erhalten – was eine massive Bedrohung darstellt.

3. Unbefugter Zugriff

Ohne Authentifizierung am Gerät selbst, könnte ein unbefugter Benutzer Malware installieren oder indirekt in ein bestehendes Netzwerk eindringen.

Canon

JA, DRUCKER KÖNNEN GEHACKT WERDEN.

Im Jahr 2022 hat das CyberNews-Sicherheitsteam im Rahmen einer spektakulären Aktion 27'944 ungesicherte Drucker auf der ganzen Welt gekapert und erzwungen, dass ein Leitfaden zur Druckersicherheit ausgedruckt wird*. Aktuell sind allein in der Schweiz über 500 Multifunktionsgeräte komplett frei zugänglich.

* www.cybernews.com

DRUCKEREMPFEHLUNG FÜR IHRE SICHERHEIT

CANON imageRUNNER ADVANCE DX SERIES

- Encryption Key Management (Schlüsselverwaltung)
- Encrypted PDF (Schutz vor falschem Zugriff)
- SSD/HDD Encryption and Erase (Verhinderung von kritischem Datenverlust)
- Secure Network Communication
- Embedded Device Management Trellix/ McAfee Embedded Control (Verhinderung nicht-autorisierter Programm-Codes)
- Security Controls (Manipulationsschutz)
- Forced Hold Printing/Secure Printing (Authenifikation verhindert Datenverlust)
- Security Information and Event Management Integration (Sicherer Datenaustausch)
- Multifunction Authentication (Schutz vor unbefugtem Zugriff)
- Automated Certificate Update (Automatische Integritätsprüfung)

Benötigen Sie Unterstützung in Bezug auf Ihre Drucksicherheit?

Die Experten von Canon beraten Sie gerne zu allen Fragen rund um den Themenkreis «Sicherheit der Dokumenten- & Printinfrastruktur». Nehmen Sie hier Kontakt mit uns auf.

Canon (Schweiz) AG
Richtistrasse 9
8304 Wallisellen
canon.ch

Canon Schweiz B2B
Canon Europa
Canon EMEA

Canon