Null Vertrauen in den **Drucker?**

Zero-Trust-Architekturen lassen sich aus der heutigen IT nicht mehr wegdenken. Allerdings können immer wieder äußere Elemente wie Multifunktionsgeräte die geschlossene Struktur stören … | VON MYRKO RUDOLPH

Vorsicht ist besser als Nachsicht. Nach dem Prinzip dieses uralten Sprichworts arbeitet auch das Zero-Trust-Modell. In dieser immer mehr an Beliebtheit gewinnenden IT-Struktur können Einwirkungen von außen, meist in Form von nicht angebundener Hardware, schnell zu Problemen führen – so auch Multifunktionsgeräte (MFP). Hier beginnt ein Konflikt zwischen Druck- und Scansystemen und der favorisierten Zero-Trust-Umgebung schon damit, daß sich die Geräte über viele verschiedene Protokolle ansprechen lassen – ein Störfaktor für die Sicherheit des erstellten Gesamtsystems. Diese gleich nach dem Aufstellen zu deaktivieren, sollte immer die erste Amtshandlung sein. In einem sauber segmentierten Netzwerk befinden sich die MFPs in einem anderen Netzbereich als beispielsweise die Anwendungsrechner, wodurch sich direkte Verbindungen zu diesen Systemen allerdings schwierig gestalten. Da bei einer derart auf Vorsicht basierenden IT-Struktur die Mitarbeiter von ihren Remote-Arbeitsplätzen keinen direkten Zugriff

auf lokale Schnittstellen, externe Ports oder das Firmennetzwerk haben, läßt sich auch kein Drucker einbinden. Erweisen sich Zero-Trust-Architekturen und die Nutzung intelligenter Multifunktionsgeräten also als unvereinbar? Absolut nicht!

Vertrauen ist gut, Kontrolle ist besser

Wer neue Bausteine in eine komplexe Struktur integrieren möchte, muß letztere zunächst verstehen – also: Was genau versteckt sich hinter Zero Trust? Einfach ausgedrückt existieren in einem solchen Modell für jede einzelne Applikation klar definierte Zugangsrechte, die eine stetige Befugnisüberprüfung erfordern. Anwender loggen sich nicht einmalig in das vorhandene Netzwerk ein, sondern separat in jedes einzelne Programm. Diese Berechtigungen sollten nur so verteilt werden, wie die Mitarbeiter sie für die Erledigung ihrer Aufgaben benötigen. All dies dient dem Schutz vor Cyberkriminellen, die so, selbst wenn sie sich Zugang zum Netzwerk verschaffen, nicht beliebig auf Anwendungen zugreifen können. Um auch den Zugriff auf sensible Informationen und Daten unter Kontrolle zu behalten und Prozesse innerhalb des Unternehmens zu optimieren, empfiehlt sich eine Netzwerksegmentierung. Bei der Arbeit aus dem Homeoffice müssen IT-Verantwortliche eine hermetische Trennung zwischen Unternehmens- und Heimnetzwerken gewährleisten. Hier kann bereits ein einfaches VPN kombiniert mit einem Remote-Desktop-Ansatz genügen, um das Zero-Trust-Konzept zufriedenstellend umzusetzen.

Auf Wolke sieben in die Struktur

Um ein Multifunktionsgerät erfolgreich in das beschriebene System einzubauen, sollten Anwender es exakt genauso behandeln wie jeden anderen Baustein der Zero-Trust-Infrastruktur. Das heißt: Zugriff erst nach Autorisierung. Für eine reibungslose Umsetzung dieser Prämisse bieten sich Cloud-Printing-Lösungen an. Sie ermöglichen ein differenziertes Rechtemanagement und stellen, in Kombination mit einer klassischen Zwei-Faktor-Authentifizierung, gleichzeitig sicher, daß zu keinem Zeitpunkt ein direkter Zugriff auf das MFP möglich ist. Da Zero-Trust jedoch nicht ausschließlich die Druckausgabe betrifft, gilt es neben den Cloud-Systemen auch Pull-Printing-Lösungen zu etablieren. Dieses Konzept bietet zusätzlichen Schutz durch den Nachweis physischer Anwesenheit – beispielsweise durch QR-Code-Authentifizierungen direkt am Endgerät. So läßt sich zu 100 Prozent sicherstellen, daß gedruckte Informationen nicht in falsche Hände geraten. Jede Ergänzung einer Zero-Trust-Architektur birgt Risiken – die Integration von Multifunktionsgeräten kann jedoch durch Cloud-Printing sehr gut funktionieren, ohne auch nur einen Teil von der hart erarbeiteten Sicherheit zu opfern. So wird aus dem Störfaktor eine enorme Bereicherung für die IT- und die gesamte Arbeitsstruktur.“ <<

Bild: exapure GmbH