ZERO-TRUST-NETZWERKE SIND AUF SIEGESZUG

Druck- und Scaninfrastrukturen wird in Zero-Trust-Security-Modellen oft zu wenig Beachtung geschenkt und entsprechende Serviceprovider werden viel zu spät involviert. Das kann ein risikoreiches Versäumnis sein.



Beat Zingg, Product Business Developer OutputManagement, Canon(Schweiz) AG

Der massive Aufschwung hybrider Arbeitsmodelle hat uns sowohl die Verheissungen als auch die Fallstricke unserer digitalen, konnektiven Welt aufgezeigt. So führt der zunehmende Anteil an Beschäftigten, die von zuhause aus arbeiten, zu einer exponentiellen Zunahme der Angriffsfläche, da sich immer mehr Geräte von verschiedenen Standorten sowie über öffentliche Cloud-Dienste mit dem Unternehmensnetzwerk verbinden.

«Never trust, always verify»

Vor diesem Hintergrund gewinnen Zero-Trust-Netzwerkarchitekturen immer mehr an Bedeutung. Während ein herkömmliches Netzwerk auf die Idee des inhärenten Vertrauens setzt, erfordert das Zero-Trust-Modell, dass alle Nutzer:innen, Geräte und Anwendungen gemäss dem Prinzip «never trust, always verify» kontinuierlich authentifiziert, autorisiert und überwacht werden, bevor ihnen der Zugriff auf Netzwerke und Daten gewährt wird – unabhängig davon, ob sie sich inner- oder ausserhalb des Unternehmensnetzwerks befinden.

Multifunktionsdrucker: der blinde Fleck in Zero-Trust-Umgebungen

Drucker, Multifunktionsdrucker (MFP) sowie die dazugehörigen Softwarelösungen stehen bei der Entwicklung einer Zero-Trust-Netzwerkstrategie nicht an erster Stelle. Dies kann fatale Folgen haben, denn MFP verfügen heutzutage über unzählige Funktionen, Dienste und Sicherheitseinstellungen – viele davon sind entweder unbekannt oder werden nicht, respektive falsch genutzt, was zu einem unnötigen Risiko führt. Für Hacker stellen MFP damit einen praktikablen Angriffsweg dar: Über sie kann Malware im gesamten Netzwerk verbreitet und geschützte Informationen können gestohlen werden oder aber sie dienen gar als Entry Point, um das Netzwerk auszukundschaften und Informationen für einen grösseren Angriff zu sammeln. Unternehmen müssen daher die Netzwerksicherheit mit der Daten- und Endpunktsicherheit für die Scan- und Druckumgebung kombinieren: Das ist der Schlüssel zu einer Zero-Trust-Architektur.

Den richtigen Servicepartner ins Boot holen

Unternehmen, die ihren Mitarbeitenden einen modernen Arbeitsplatz bieten und zugleich das Risikomanagement mit Zero-Trust optimieren möchten, müssen die Servicepartner der In- und Outputinfrastruktur frühzeitig einbeziehen. Es bedarf cloudbasierter Lösungen sowie eines kohärenten Ansatzes, der Geräte, Software, Prozesse sowie Nutzer:innen einschliesst. Dabei müssen insbesondere folgende Faktoren beachtet werden:

- **Identifikation und Schutz der Identitäten:** Zero-Trust beginnt mit der Identifizierung der Identitäten und dem Schutz der Endpunkte. Insbesondere unpersönliche Endgeräte wie MFP oder Drucker müssen ebenfalls authentifiziert und mit Zertifikaten ausgerüstet werden. Zudem sollten ungenutzte Ports und Protokolle, über die sie angesprochen werden können, deaktiviert werden.
- **Schutz von Netzwerken:** Eine Mikrosegmentierung des Netzwerks sorgt dafür, dass User lediglich Zugriff auf die Netzwerkressourcen erhalten, die sie unbedingt benötigen. In Bezug auf standortunabhängiges Arbeiten ist es notwendig, die eingesetzten Unternehmensanwendungen hermetisch von den lokalen und privaten Heimnetzwerken der Mitarbeitenden zu trennen, weil deren Sicherheit schlicht nicht gewährleistet werden kann.
- **Kontinuierliche Überwachung und Optimierung:** Alle Identitäten müssen kontinuierlich überwacht und optimiert werden, um die Sicherheitsrichtlinien des Unternehmens zu erfüllen und gegen aktuelle Bedrohungen resilient zu bleiben. Unbeabsichtigte oder unbefugte Änderungen müssen sofort erkannt werden. Zudem müssen Firm- und Software sowie Applikationen regelmässig aktualisiert werden, um bekannte Lücken zu schliessen und bestmöglich gegen Zero-Day-Angriffe geschützt zu sein.

