ezeep by ThinPrint

eBook

Drucker und Zero Trust – So funktioniert es

Inhalt

Einleitung

Die vermehrten Angriffe auf IT-Systeme erfordern ein Umdenken. Ein vielversprechendes Sicherheitskonzept für zusätzlichen Schutz bietet das Zero-Trust-Prinzip. Innerhalb dieser Struktur kommt es allerdings oft zu Problemen mit Druckern. In diesem Whitepaper erfährst Du, wie Du diese Probleme lösen und wie Du das Drucken in Deiner Firma noch einfacher und sicherer gestalten kannst.

Inhalt des eBooks

- Was ist eine Zero-Trust-Umgebung?
- Warum sollten Sicherheitskonzepte mit einer Zero-Trust-Architektur ergänzt werden?
- Wie integriert man Drucker einfach und unkompliziert in eine Zero-Trust-Umgebung?
- Wie kann man Druckprozesse vereinfachen?
- Was ist Pull Printing und wie wird es implementiert?

Zero Trust – Definition

IT-Systeme werden immer öfter angegriffen. Dies spiegelt sich auch in einer von der Bitkom durchgeführten Studie aus dem August 2021 wider. 59 % der Unternehmen, die ihre Mitarbeiter.innen im Homeoffice arbeiten lassen, waren demnach seit Beginn der Pandemie von solchen Angriffen betroffen. In 52% der Fälle entstand dadurch Schaden. Die interne IT steht also vor der Herausforderung ein sichereres Umfeld zu schaffen.

Bisherige Sicherheitskonzepte basierten größtenteils auf einem VPN (Virtual Private Network). Dieses ist virtuell und in sich abgeschlossen, bietet in der heutigen Welt aber keinen ausreichenden Schutz mehr, da Kriminelle ihren Weg um dieses Hindernis herum kennen.

Diese eigentlich geschützten VPNs haben ein großes Problem. Sobald sich jemand Zugriff verschaffen konnte, hat diese Person Zugriff auf alle dahinterstehenden Ressourcen.

Aus diesem Grund ist es nötig, das vorhandene VPN-System mit einem moderneren Sicherheitskonzept zu ergänzen. So hat das Konzept des Zero Trust in den letzten Jahren zunehmend an Popularität gewonnen, insbesondere bei Behörden und stark regulierten Organisationen im Finanz-, Medizin- und Justizbereich. Kürzlich hat sogar US-Präsident Biden mit der **Executive Order 14028** öffentliche Einrichtungen veranlasst, ein solches Umfeld zu schaffen.

Bild 1: Das Weiße Haus: Hier wird Geräten und Anwender.innen nicht automatisch vertraut.

Was ist Zero Trust?

Zero Trust ist vereinfacht gesagt ein Sicherheitsmodell, welches von dem.der Anwender.in nicht nur das Einloggen in ein Netzwerk, sondern in jede einzelne Anwendung verlangt. Damit gelingt eine regelmäßige Überprüfung der Rechte des jeweils Zugreifenden. Falls es also ein.e Angreifer.in schafft sich in das Netzwerk einzuschleusen, so scheitert er.sie beim Zugreifen auf die entsprechenden Anwendungen. Voraussetzung dafür ist, dass bei der Zuweisung der Rechte jedem.jeder Anwender.in nur genau die Rechte eingeräumt werden, die zum Erfüllen seiner.ihrer Aufgaben nötig sind.

Bild 2: Die drei Eckpfeiler des Zero-Trust-Konzepts

Möchte man ein Netzwerk mithilfe des Zero-Trust-Konzepts optimieren, greift man auf eine Netzwerksegmentierung zurück. In diesem Spezialfall wird auch von Zero-Trust-Segmentierung oder Mikrosegmentierung gesprochen. Hierbei wird das Netzwerk unterteilt, sodass es möglich ist, dem.der Anwender.in den gezielten Zugriff auf Netzwerkressourcen zu erlauben, ohne ihm.ihr das gesamte Netzwerk verfügbar zu machen. Nutzt man dieses Sicherheitskonzept, ist es wichtig, dass sich die Anwenderrechner und die Anwendungsserver in getrennten Segmenten der Zero-Trust-Umgebung befinden.

Bezüglich des Homeoffice gibt es noch eine Besonderheit zu beachten. Da sich kein.e Administrator.in für die Sicherheit von privaten Netzwerken verbürgen sollte, ist es wichtig, die lokalen Heimnetzwerke der Mitarbeiter.innen strikt von den genutzten Unternehmensanwendungen zu trennen. Dafür empfiehlt sich ein VPN in gemeinsamer Nutzung mit einem Remote Desktop An-

satz. Die Fälle, in denen eine Kombination von VPN und Webanwendungen ausreicht, ist steigend. Damit kann der.die Anwender.in seine.ihre Wahl beim Endgerät frei treffen und es könnten zum Beispiel auch Chromebooks genutzt werden.

Wie wir aus dieser ersten Skizze ersehen können, ist die Umsetzung von Zero Trust durchaus mit etwas Aufwand verbunden. Es gibt eine Menge zu bedenken, und ein besonderer Aspekt, auf den wir uns im nächsten Kapitel konzentrieren werden, sind Drucker.

Drucker in einer Zero-Trust-Umgebung einrichten?

Personen, die eine Zero-Trust-Umgebung einrichten, können Drucker schon frühzeitig als Probleme identifizieren. Das liegt daran, dass Drucker über eine Vielzahl von Protokollen angesprochen werden können und diese meistens alle im Auslieferungszustand aktiviert sind. Aus diesem Grund sollte nach dem Einschalten des Gerätes direkt die Deaktivierung aller nicht benötigten Druck- bzw. Netzwerkprotokolle vorgenommen werden.

Drucker, die Hindernisse in der Zero-Trust-Umgebung

Hier sind übliche Probleme, die entstehen, wenn Drucker in einer Zero-Trust-Umgebung verwendet werden:

1. Bei einer sauberen Netzwerksegmentierung befinden sich die Drucker und Anwendungsrechner in getrennten Segmenten. Damit ist die Einrichtung einer direkten Verbindung zum Drucken komplexer und nicht blindlings möglich.

2. Es ist oft nicht möglich, Drucker direkt mit dem Heimnetzwerk, externen Ports oder lokalen Schnittstellen zu verbinden, da diese an sicheren Homeoffice-Arbeitsplätzen keinen Zugriff auf die Zero-Trust-Umgebung haben.

3. Durch den untersagten Zugriff auf die lokale Festplatte ist es auch nicht möglich, aus einer Webanwendung heraus zu drucken, ohne dass dafür zunächst ein PDF erstellt werden muss.

Dabei müssen andere Zero-Trust-Prinzipen berücksichtigt werden:

- Eine ständige Autorisierung und Authentifizierung für Zugriffe auf Drucker sollte gewährleistet werden
- Vollumfängliche Verschlüsslung der Kommunikationswege

Wie kann man Drucker in Zero-Trust-Umgebungen sicher integrieren?

Empfehlenswert ist eine unternehmensweite Drucklösung, die mit allen Anwendungen, Geräten und Druckern verbunden werden kann, ohne die Sicherheitsmaßnahmen zu gefährden, die zum Schutz des Unternehmens und seiner Daten eingerichtet wurden. Am Beispiel der Cloud-Drucklösung ezeep Blue lässt sich zeigen, wie jedes der oben genannten Hindernisse beseitigt werden kann.

Direkte Verbindung mit Druckern in segmentierten Netzwerken herstellen

Zuerst muss eine sichere Verbindung zwischen der Cloud und dem Drucker hergestellt werden. Um auch andere eingehende Verbindungen blockieren zu können, muss sichergestellt werden, dass der Drucker nicht direkt aus dem Internet adressierbar ist.

Cloud-Printing-Lösungen bieten hierfür Connector Software oder Hardware an. Dazu nutzt ezeep Blue den ezeep Hub, welcher selbstständig die Verbindung zwischen Cloud und Drucker aufbaut und somit den einzigen Kontaktpunkt für den Drucker darstellt.

Der Hub, der so klein ist, dass er in jede Tasche passt, wird einfach an das gleiche Netzwerk, in dem sich der Drucker befindet, angeschlossen. Anschließend wird der Hub im ezeep Admin Portal über seine Mac-Adresse registriert und verbindet den Drucker automatisch mit der ezeep Cloud.

Bild 3: Große, teure Druckserver können mit Appliances wie dem ezeep Hub vollständig eliminiert werden. Alle Druckdaten werden mit ezeep Blue verschlüsselt übertragen.

Lokales Drucken aus einem gesicherten Homeoffice

Der ezeep Hub ist auch ideal fürs Homeoffice, da er keine Wartung erfordert, klein ist und nur gering zum Stromverbrauch beiträgt. Klein und unkompliziert ermöglicht er das Zero-Trust-Drucken, ohne dass PC und Drucker aufeinander zugreifen müssen.

Diese Lösung ist eine sichere und einfache Möglichkeit für Unternehmen, das schwierige Druckerszenario im Homeoffice zu bewältigen, ohne sich mit VPN-Einstellungen herumschlagen zu müssen oder Drucker über USB anzuschließen. Da der ezeep Hub über die Cloud konfiguriert werden kann und nur in das Netzwerk eingesteckt werden muss, können IT-Administrator.innen ihn auch direkt an jede.n im Homeoffice schicken. Lokale Drucker können also problemlos genutzt werden. Auch wenn eine Remote-Desktop-Lösung wie Azure Virtual Desktop verwendet wird, ist natives Drucken möglich. Sobald ein ezeep-Konto auf dem Azure Marketplace erstellt wurde, muss lediglich ein zusätzlicher Agent auf dem Rechner installiert werden.

Drucken aus Webanwendungen

Damit Webanwendungen auch ohne lokales Ablegen von Dateien drucken können, ist ezeep Blue mit einer API ausgestattet, die Druckaufträge aus dem Backend der Webanwendung auslösen kann. Weiterhin kann man die Nutzung vereinfachen, indem man ezeep über das Javascript Modul ezeep.js einbindet.

Auch Apps wird das Drucken erleichtert. Durch die Verbindung von ezeep und Zapier ist eine automatische Druckausgabe in unzähligen Apps möglich. Zaps sind automatisierte Workflows. Löst man einen Zap aus, startet dieser die vorgegebenen Aktionsschritte. Integriert man ezeep in einen Zap, so kann man automatisch aus Anwendungen heraus drucken.

Weitere Sicherheitsmaßnahmen für Drucker

Damit die Sicherheit der Zero-Trust-Umgebung bestehen bleibt, ist es wichtig, die Nutzung eines Druckers nur bei autorisiertem Zugriff zu erlauben. Dafür empfehlen sich Cloud-Printing-Lösungen, die es erfordern, dass der.die Anwender.in sich beim Cloud-Printing-Dienst autorisiert. Hierbei ist eine Zwei-Faktor-Authentifizierung besonders sicher. Diese Lösungen erlauben zu keinem Zeitpunkt einen direkten Zugriff auf den Drucker. Ein Beispiel dafür ist ezeep Blue. Als Cloud-Printing-Lösung richtet ezeep eine Zwei-Faktor-Authentifizierung über Active Directory oder Google ein.

Auch die Connector Software / Hardware sorgen dafür, dass eine ständige Autorisierung mit OAuth 2 gewährleistet wird. Beispielsweise scannt der ezeep Hub das Netzwerk selbstständig und ermöglicht die Auswahl des gewünschten Druckers. Dadurch lässt sich der Drucker nur noch von autorisierten Personen ansteuern und schließt damit eine oft vergessene Sicherheitslücke. Denn: Drucker speichern und geben verschiedenste Dokumente aus, darunter auch solche mit sensiblen Daten. Durch die autorisierte Nutzung des Druckers kann sich dort befindliche Malware nicht auf das Unternehmensnetzwerk ausbreiten oder die Rechner der Mitarbeiter.innen befallen.

Pull Printing

Um das Zero-Trust-Konzept auch bei der Druckausgabe aufrecht zu erhalten, nutzen viele Cloud-Printing-Lösungen, wie ezeep Blue, das Pull-Printing-Verfahren. Dieses lässt den.die Anwender.in sicher und ressourcenschonend an einem beliebigen Drucker drucken. Die Pull-Printing-Funktion wird einfach mit einem Mausklick im ezeep Admin Portal für die gewünschten Gruppen und Benutzer.innen aktiviert.

Bild 4 Verschiedene Authentifizierungsmethoden sind möglich, wie NFC oder Card Reader.

Um die ausgewählten Dokumente zu drucken, scannt der.die Anwender.in zum Beispiel einen QR-Code am Drucker, um per Zwei-Faktor-Authentifizierung sicherzustellen, dass die Dokumente nicht von einer unbefugten Person entnommen werden. Somit wird die sichere Zero-Trust-Umgebung auch bei der gemeinsamen Nutzung von Druckern erhalten. Auch Ressourcen wie Tinte und Papier werden dadurch geschont, denn es werden nur noch Dinge gedruckt, die auch wirklich benötigt werden.

Ein weiterer Vorteil von Pull Printing, wie es ezeep Blue bietet, ist, dass eine bequeme „Flex-Desk“-Lösung sofort aktiviert werden kann. Das ist perfekt für Mitarbeiter.innen, die ihren Standort häufig wechseln. Dank einer nicht druckerspezifischen Druckerwarteschlange muss kein bestimmter Drucker ausgewählt werden und sie können zu ihrem bevorzugten Drucker gehen, wann immer sie bereit sind.

Fazit

Das Zero-Trust-Konzept ist in der heutigen Welt unabdingbar. Herkömmliche Lösungen vernachlässigen dabei oft das Drucken. Cloud-Printing-Dienste, wie ezeep Blue, lösen dieses Problem und ermöglichen die sichere Nutzung des Druckers. Auch Administratoren profitieren von ezeep Blue im Vergleich zur klassischen Druckumgebung, da ezeep einfacher und ressourcenschonender zu verwalten ist. Mit ezeep schützt Du Drucker vor Angreifer.innen und vor unautorisierten Zugriffen auf vertrauliche Dokumente. **Eine kostenlose Testphase von ezeep Blue** findest Du auf unserer Webseite.