ARTIKEL

Runden Sie Ihre Datenschutzstrategie mit sicherem Drucken ab

Cyberkriminelle sind meist einen Schritt voraus – von Angriffen auf die Supply Chain über Social Engineering bis hin zu durch künstliche Intelligenz unterstützte Attacken.[1] Laufend werden neue Angriffsmöglichkeiten gefunden und wunde Punkte im Netzwerkschutz von Unternehmen gesucht – wunde Punkte wie der Netzwerkdrucker im Büro.

Als führender Technologiepartner treibt HP die Entwicklungen im Bereich Drucksicherheit für Unternehmen weltweit voran. Obwohl Netzwerkgeräte, Server und Computer nach wie vor die meistattackierten Ziele sind, gehören auch Drucker zu den Netzwerkendpunkten. Und für Cyberkriminelle ist jeder ungesicherte Endpunkt ein potenzielles Einfallstor.

Über

30%

der Befragten meldeten einen oder mehrere Vorfälle mit Datenverlust im Zusammenhang mit Drucken.[3]

Drucker werden regelmäßig angegriffen

Im Gegensatz zum vorherrschenden Glauben werden Netzwerkdrucker recht häufig von Cyberkriminellen attackiert. Laut dem Global Print Security Report berichteten fast zwei Drittel der Unternehmen von einem Datenverlust im Zusammenhang mit Drucken.
Dieser Verlust kostet amerikanische Unternehmen über 1 Mio. $.[2]
Eine andere, von der Consultingfirma Booz Allen Hamilton zitierte Studie kam zu dem Ergebnis, dass 2016 61 % der Befragten einen Datenverlust verzeichneten – mindestens 50 % davon meldeten einen oder mehrere dieser Vorfälle im Zusammenhang mit einem Drucker.[3]

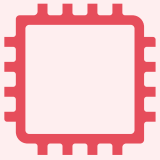
Cybersecurity Ventures prognostiziert, dass Cyberkriminalität die Weltwirtschaft bis 2021 6 Bio. $ kosten wird.[4] Unternehmen können es sich also nicht länger leisten, Drucksicherheit zu ignorieren.

Die Sicherheitsrisiken, die mit Druckern in Verbindung gebracht werden

Bevor ein Unternehmen eine Cybersicherheitsstrategie für seine Netzwerkdrucker entwickeln kann, muss es erst die Sicherheitsrisiken verstehen, die entschärft werden müssen. Diese rangieren von gezielten externen Cyberattacken über potenzielle Malware-Einschleusung durch Verwendung ungesicherter Tonerimitate bis hin zu sensiblen Dokumenten, die im Drucker liegen gelassen werden. Netzwerkdrucker haben eine Reihe von Schwachstellen. Dazu gehören:[5]

Unautorisierte Zugriffe auf Druckdaten

Obwohl Datensicherheit oft als digitales Problem gesehen wird, kann eine Datenpanne auch einfach dadurch entstehen, dass Personen Zugang zu im Drucker liegen gebliebenen Dokumenten erhalten.

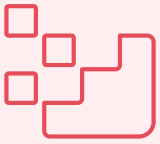


Risiken durch Malware

Im Gegensatz zu Original HP Tonerkartuschen, die gegen Manipulationen abgesichert sind, nutzen viele Tonerimitate Chips, die umprogrammiert werden können, um Malware einzuschleusen.

Umleiten von Druckaufträgen

Mit ein paar Konfigurationsänderungen können Cyberkriminelle Druckaufträge auf ihren eigenen Drucker umleiten.



Datenmanipulation

Ein kompromittierter Drucker kann Angreifern erlauben, Inhalte von Druckaufträgen zu ersetzen oder zu entfernen.

Offenlegung von Daten

Druckdaten können offengelegt werden, wenn ein Angreifer Zugriff auf das Speicher- oder Dateisystem eines Druckers oder auf die physischen Festplatten von stillgelegten Druckern hat.

Risiken beim kabellosen Drucken

Drucker, die über WiFi drucken können, sind weiters anfällig für Angriffe aus dem näheren Umfeld. Angreifer können den Drucker dazu bringen, sich mit einem bösartigen Netzwerk zu verbinden, und schädliche Codes ausführen.

Sichern Sie Ihren Drucker und Ihre Druckdaten

Um diesen sensiblen Endpunkt zu schützen, empfiehlt HP ein paar grundlegende Sicherheitsmaßnahmen. Zunächst sollten Sie Drucker oder Managed Print Services von einem Anbieter mit bewährten Sicherheitsfunktionen wählen. Vermeiden Sie Tonerimitate, um eine sichere Basis für Drucksicherheit zu schaffen. Runden Sie Ihre Maßnahmen ab, indem Sie das Betriebssystem des Druckers rechtzeitig patchen, regelmäßig PIN und Passwort ändern, ungenutzte Services abschalten, Multi-Faktor-Authentifizierung implementieren und Ihre Mitarbeiter:innen in Best Practices für Datensicherheit schulen. So stärken Sie den Sicherheitsstatus Ihres Unternehmens.

Mit der Durchführung dieser Maßnahmen können Sie versteckte Schwachstellen in Ihrer Sicherheitsstrategie schließen und das Risiko von Datenverlusten durch schlecht geschützte Netzwerkdrucker reduzieren.

Das HP Druckersortiment verfolgt einen mehrschichtigen Sicherheitsansatz, um Unternehmen sicheres Drucken zu ermöglichen: von automatischer Malware-Erkennung und Selbstheilungsfähigkeiten[6] bis hin zu aktualisierbarer Firmware[7] und Sicherheitstools für das Druckerflottenmanagement.[8] Zusätzlich enthalten die Chips in Original HP Tonerkartuschen manipulationsresistente Firmware.[9] Sie werden mit Sicherheitsmaßnahmen entlang der gesamten Lieferkette entwickelt und produziert, um die Produktintegrität zu gewährleisten.[8]

Schützen Sie Ihre Daten mit Drucklösungen, die für Sicherheit entwickelt wurden.
Erfahren Sie mehr unter **hp.com/go/SuppliesThatProtect**.

Referenzen:

[1] ZDNet, Artificial intelligence will be used to power cyberattacks, warn security experts, April 2020.
[2] Quocirca, The Print Security Landscape, 2020, Louella Fernandes, Dezember 2020.
[3] DarkReading.com, How Hackers Hit Printers, 2018.
[4] Cision, Cyberattacks are the fastest growing crime and predicted to cost the world $6 trillion annually by 2021, Dezember 2018.
[5] Business News Daily, Is Your Printer Your Weak Security Link?, April 2020.
[6] Die modernsten eingebetteten Sicherheitsfunktionen von HP sind auf HP Enterprise und HP Managed Geräten mit HP FutureSmart Firmware 4.5 oder höher verfügbar. Aussage basiert auf einer von HP durchgeführten Überprüfung von veröffentlichten Funktionen von Wettbewerbsdruckern in der Klasse in 2019. Nur HP bietet eine Kombination von Sicherheitsfunktionen zur automatischen Erkennung, Beendigung und Wiederherstellung nach Angriffen mit einem selbstheilenden Neustart in Übereinstimmung mit den NIST SP 800-193 Richtlinien für Geräte-Cyber-Resilienz. Eine Liste der kompatiblen Produkte finden Sie unter: hp.com/go/PrintersThatProtect. Für weitere Informationen besuchen Sie: hp.com/go/PrinterSecurityClaims.
[7] Einige Druckersicherheitsfunktionen, die durch zukünftige HP FutureSmart-Firmware-Upgrades aktiviert werden, sind möglicherweise auf älteren Geräten nicht verfügbar, falls z. B. physische Produkteigenschaften die Funktionalität von neuen Features einschränken.
[8] HP JetAdvantage Security Manager muss separat erworben werden. Mehr Info unter: hp.com/go/securitymanager.
[9] HP Office-Drucksysteme umfassen Geräte der Enterprise- und Managed Klasse mit FutureSmart Firmware 4.5 oder höher, Geräte der Pro-Klasse, LaserJet 200 oder höher und die jeweiligen Original HP Tonerkartuschen bzw. PageWide- und Tintenpatronen. Umfasst keine HP Druckerpatronen mit integriertem Druckkopf. Die digitale Lieferkettenverfolgung und die Sicherheitsmerkmale der Verpackung variieren lokal je nach SKU. Siehe hp.com/go/SuppliesThatProtect und hp.com/go/SuppliesSecurityClaims.