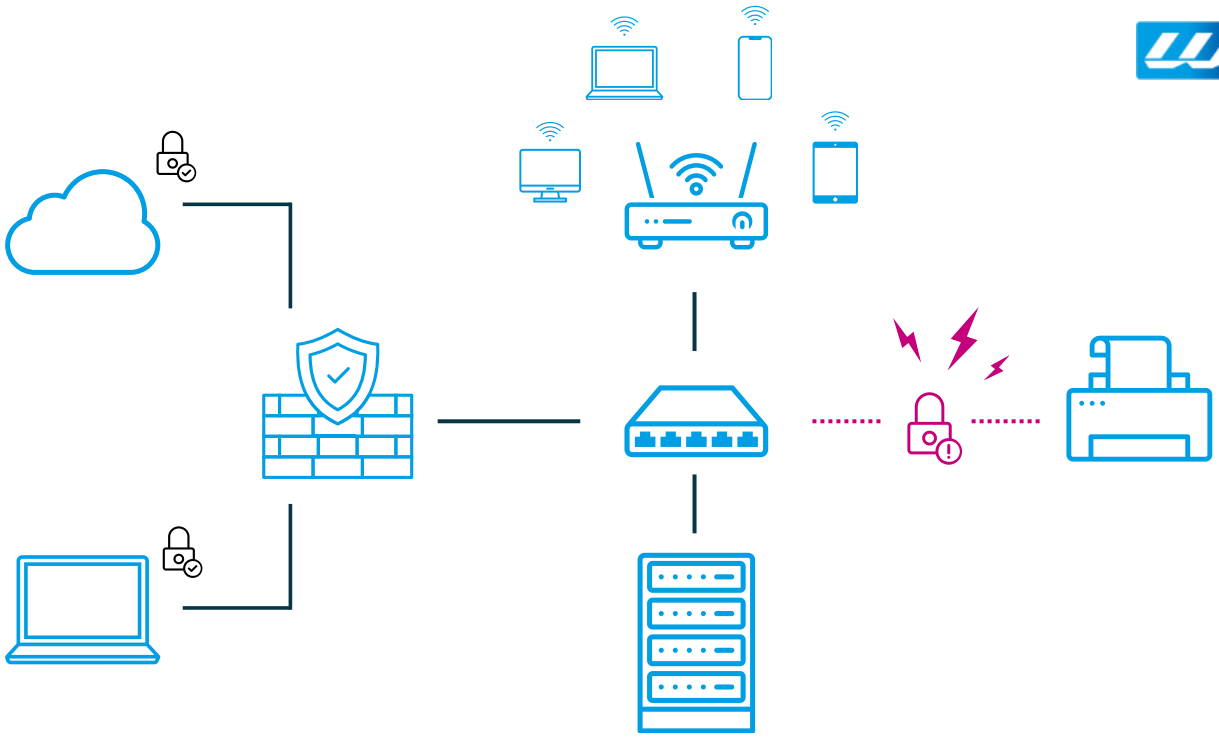
WIETHOLT®
SO GEHT BÜRO

DIE VERSTECKTEN RISIKEN IN IHREM NETZWERK

WARUM DRUCKER OFT ÜBERSEHEN WERDEN.



In einer Zeit, in der Cyberangriffe immer häufiger und ausgeklügelter werden, ist das Bewusstsein für Netzwerksicherheit entscheidend. Während Unternehmen oft in die Sicherung ihrer Computer, Server und Mobilgeräte investieren, bleibt eine potenzielle Schwachstelle oft unbeachtet: die Drucker und Multifunktionsgeräte. Diese Geräte sind heute vollwertige PCs, die in den meisten Unternehmen alltäglich genutzt werden und ein Einfallstor für Cyberkriminelle darstellen können.

WARUM DRUCKER OFT ÜBERSEHEN WERDEN.

HEUTE SIND DRUCKER MEHR ALS EINFACHE AUSGABEGERÄTE

Obwohl Drucker und Multifunktionsgeräte heute weit mehr sind als einfache Ausgabegeräte, werden sie in der IT-Sicherheitsstrategie oft vernachlässigt. Moderne Drucker verfügen über Festplatten, Netzwerkschnittstellen und können Daten senden, empfangen und speichern – all dies macht sie zu potenziellen Zielen für Angriffe.

DIE HÄUFIGSTEN SICHERHEITSRISIKEN BEI DRUCKERN.

Drucker und Multifunktionsgeräte sind heute oft vollwertige Netzwerkgeräte mit eigenen Betriebssystemen und IP-Adressen. Diese Eigenschaften machen sie anfällig für verschiedene Arten von Sicherheitsrisiken:

Laut des Ponemon Institute hatten 26% aller bedeutenden, von IT-Managern gemeldeten Datensicherheitsverletzungen einen Bezug auf Drucker und Multifunktionsgeräte.

- **UNVERSCHLÜSSELTE DATENÜBERTRAGUNG:**

  Viele Drucker übertragen Druckdaten unverschlüsselt, was das Abfangen sensibler Informationen wie, persönliche Daten, Finanzinformationen oder vertrauliche Geschäftsunterlagen, ermöglicht.

- **SCHWACHE ZUGANGSKONTROLLEN:**

  Oft haben Drucker standardmäßige oder schwache Passwörter, die leicht aufzufinden sind.

- **FEHLENDE AKTUALISIERUNGEN:**

  Firmware ist Software und Software beinhaltet Fehler. Fehler, die zum Sicherheitsrisiko werden können. Firmware-Updates, die Sicherheitslücken schließen, werden oft vernachlässigt oder nicht flächendeckend installiert.

CLOUDBASIERTER ZUGRIFF

PAPIERAUSGABE

BEDIENFELD

NETZWERK

ADMINISTRATION

BIOS UND FIRMWARE

MOBILES DRUCKEN

MASSNAHMEN ZUR SICHERUNG IHRER DRUCKERFLOTTE

Um Drucker als potenzielle Schwachstellen zu eliminieren, müssen Unternehmen proaktive Maßnahmen ergreifen:

- **IMPLEMENTIERUNG VON SICHERHEITSRICHTLINIEN:**

  Klare Regeln für die Nutzung und Wartung von Druckern festlegen. Wie z.B. die Festlegung von Zugriffsrechten und Benutzer Authentifizierungen sowie das ändern von Standardpasswörtern.

- **VERSCHLÜSSELUNG DER DATENÜBERTRAGUNG:**

  Sicherstellen, dass alle Daten, die an und von Druckern gesendet werden, verschlüsselt sind, indem Protokolle wie TLS oder End-to-End-Verschlüsselung verwendet werden.

- **REGELMÄSSIGE UPDATES UND WARTUNG:**

  Firmware-Updates regelmäßig durchführen, um Sicherheitslücken zu schließen, und das Manipulieren der Drucker und Multifunktionsgeräte von Hackern zu vermeiden.

- **NUTZUNG VON SICHERHEITSLÖSUNGEN WIE DEM HP SECURITY MANAGER:**

  Überwachung und Management der Druckersicherheit automatisieren. Sicherheitsrichtlinien zentral definieren und auf alle verbundenen Geräte 24/7 anwenden. Updates und Patches sowie Sicherheitszertifikate völlig automatisch auf Druckern und Multifunktionsgeräten installieren lassen.

DER HP SECURITY MANAGER – IHRE LÖSUNG FÜR UMFASSENDE DRUCKERSICHERHEIT

Mit dem HP Security Manager können Sie Ihre Druckumgebung ganz einfach verwalten und schützen. Verwalten Sie Sicherheitsrichtlinien, überwachen Sie Geräteaktivitäten und schützen Sie vertrauliche Daten vor unbefugtem Zugriff - alles von einer zentralen Plattform aus. Von der Authentifizierung und Autorisierung bis hin zur Verschlüsselung und Compliance-Überwachung bietet der HP Security Manager die Tools, die Sie benötigen, um Ihre Druckerflotte geschützt zu halten.

DER HP SECURITY MANAGER BIETET EINE UMFASSENDE LÖSUNG ZUR SICHERUNG IHRER DRUCKERFLOTTE:

- **AUTOMATISIERTE ÜBERWACHUNG:**

  Der HP Security Manager überwacht jegliche Geräteaktivität Ihrer Drucker rund um die Uhr und prüft sie auf Sicherheitsbedrohungen.

- **EINHALTUNG VON SICHERHEITSRICHTLINIEN:**

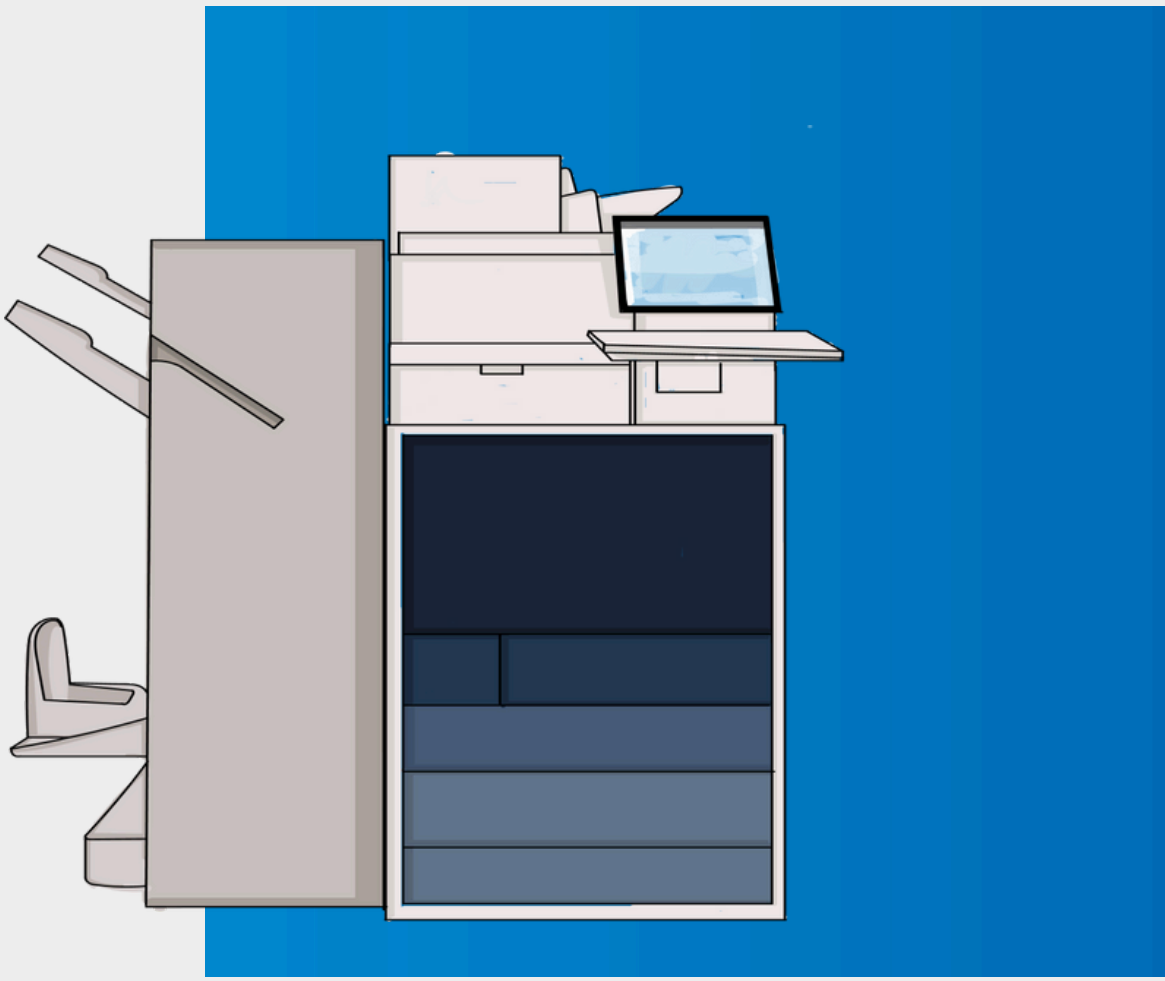
  Er ermöglicht es, Sicherheitsrichtlinien zentral zu definieren und auf alle verbundenen Geräte anzuwenden. Dies umfasst die Konfiguration von Verschlüsselung, Authentifizierung und Zugriffskontrollen.

- **EFFIZIENTES ZERTIFIKATSMANAGEMENT:**

  Er ermöglicht die Erstellung, Verwaltung und automatische Verteilung von Sicherheitszertifikaten für die gesamte Druckerflotte.

- **AUTOMATISIERTE BERICHTERSTATTUNG:**

  Nach jeder Sicherheitsüberprüfung erhalten Sie detaillierte Berichte per Mail, die einen Überblick über den Sicherheitsstatus der Drucker, einschließlich der Einhaltung von Sicherheitsrichtlinien, installierter Updates und erkannter Bedrohungen geben.



FAZIT

Drucker und Multifunktionsgeräte sollten in keiner IT-Sicherheitsstrategie übersehen werden. Mit der richtigen Vorgehensweise und den entsprechenden Tools können Unternehmen ihre Druckerflotte sichern und somit eine weitere potenzielle Schwachstelle im Netzwerk eliminieren. Der HP Security Manager bietet eine umfassende Lösung, um diese Herausforderungen zu bewältigen.

IHR ANSPRECHPARTNER
IHR BÜROMANE

BENJAMIN MIKULLA

+49 2863925227
b.mikulla@wietholt.de