WHITEPAPER

OFFENE TÜREN

EINE UNTERSUCHUNG ZEIGT, DASS DRUCKER NICHT VOR CYBER-ANGRIFFEN GESCHÜTZT WERDEN

Während die IT-Teams sich auf andere Endgeräte konzentrieren, wird die Sicherheit der Unternehmensdrucker vernachlässigt

Drucker sind leichte Ziele: Der Zugriff auf zu viele Netzwerkdrucker ist uneingeschränkt und ohne Sicherheitsmaßnahmen möglich.

Die Bedrohungen sind jedoch real und sollten nicht ignoriert werden. Drucker der Enterprise-Klasse haben sich zu leistungsfähigen Netzwerkgeräten entwickelt, die dieselben Schwachstellen wie andere Endgeräte in Ihrem Netzwerk aufweisen. Diese in der Regel ungeschützten Einstiegspunkte bieten sehr reale Möglichkeiten für Cyber-Angriffe. Sie können z. B. den Zugriff auf Finanzdaten und vertrauliche Daten Ihres Unternehmens ermöglichen, was sehr reale geschäftliche Konsequenzen nach sich zieht.

Dennoch zeigt eine von Spiceworks durchgeführte Befragung von mehr als 300 IT-Entscheidungsträgern in Unternehmen, dass nur 16 % der Befragten glauben, dass Drucker ein hohes Risiko für Sicherheitsbedrohungen/-verletzungen darstellen – erheblich weniger als bei Desktop-PCs/Laptops und mobilen Geräten.[1] Dieser Irrglaube hat bisher das Konzept der IT-Mitarbeiter für die Netzwerksicherheit geprägt. Fast drei von fünf Unternehmen haben zwar Sicherheitsvorkehrungen für Drucker implementiert; das ist aber ein wesentlich niedrigerer Prozentsatz als bei anderen Endgeräten. So bleiben Drucker ungeschützt, obwohl benutzerfreundliche Lösungen für den Schutz dieses Einstiegspunkts verfügbar sind.

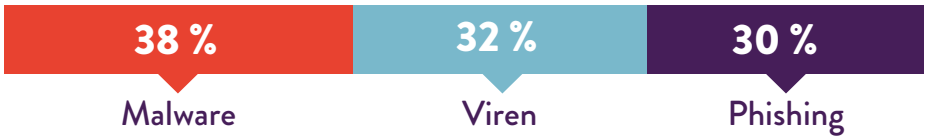
Dieses Whitepaper enthält Fakten zur Druckersicherheit, die auf der Untersuchung von Spiceworks basieren, und beschreibt einige der modernen, integrierten Funktionen für Druckersicherheit zum Schutz vor Cyber-Angriffen.

NUR 16 % DER BEFRAGTEN GLAUBEN, DASS BEI DRUCKERN EIN HOHES RISIKO FÜR SICHERHEITSBEDROHUNGEN/-VERLETZUNGEN BESTEHT.[1]

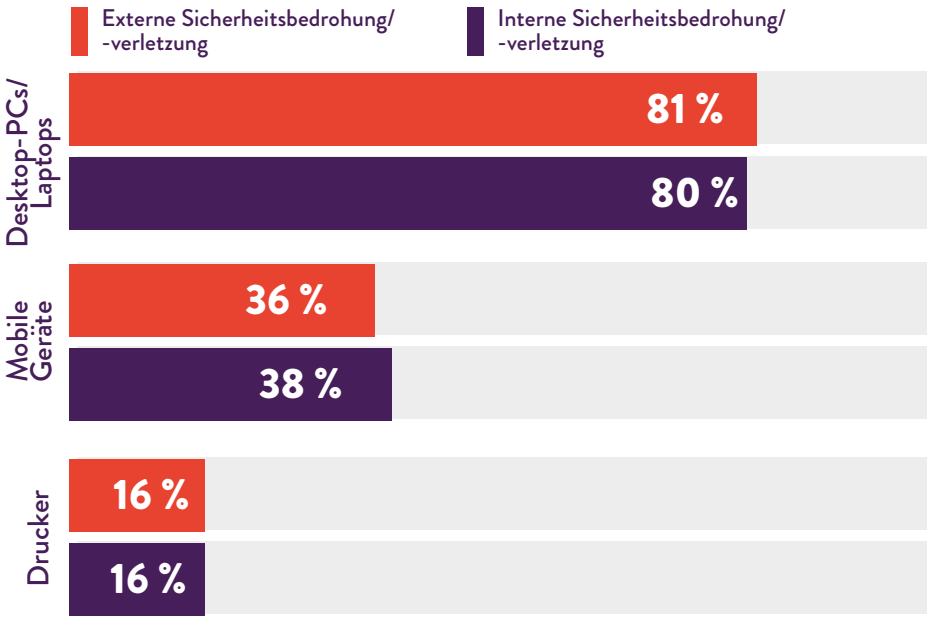
OFFENE TÜREN FÜR ANGRIFFE

In der Untersuchung von Spiceworks gaben 74 % der Befragten (netto) an, dass in ihrem Unternehmen im vergangenen Jahr zumindest ein Typ der externen Angriffe auf die IT-Sicherheit erfolgt ist. 70 % (netto) verzeichneten einen internen Angriff auf die IT-Sicherheit, am häufigsten durch Benutzerfehler oder den Einsatz privater Geräte bzw. die Nutzung von Heimnetzwerken oder öffentlichen Netzwerken für die Arbeit.[1]

WICHTIGSTE AUFGETRETENE EXTERNE BEDROHUNGEN/ VERLETZUNGEN DER IT-SICHERHEIT



Angreifer haben sich hauptsächlich über Desktop-PCs und Laptops und in zweiter Linie über mobile Geräte und Drucker Zugang verschafft.[1] (Die 16 % der über Drucker erfolgten Angriffe sind gegenüber den 4 %, die in einer ähnlichen Untersuchung von Spiceworks im Jahr 2014 ermittelt wurden, deutlich angestiegen.) Es ist auch möglich, dass die Anzahl der Angriffe über Drucker zu niedrig angegeben wurde, da Drucker nicht so engmaschig überwacht werden wie PCs und mobile Geräte.



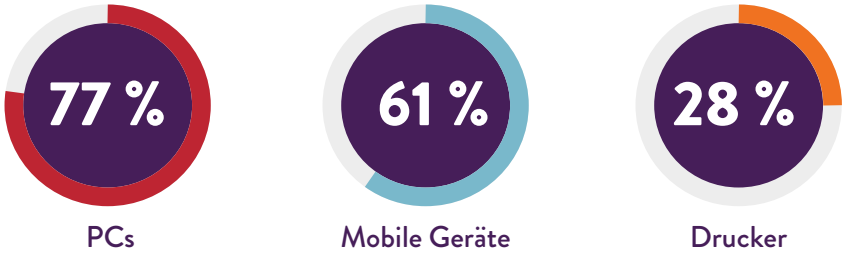
WIR IGNORIEREN UNSERE DRUCKER

Wie auch immer, die Untersuchung von Spiceworks zeigt eindeutig, dass die Druckersicherheit häufig eine untergeordnete Rolle spielt.

Unternehmen sind sich jedoch absolut über die Wichtigkeit der Netzwerk-, Endgeräte- und Datensicherheit im Klaren. Denn mehr als 75 % der Befragten verwenden Lösungen für Netzwerksicherheit, Zugangskontrolle/-management, Datenschutz oder Endgerätesicherheit – oder eine Kombination daraus.[1]

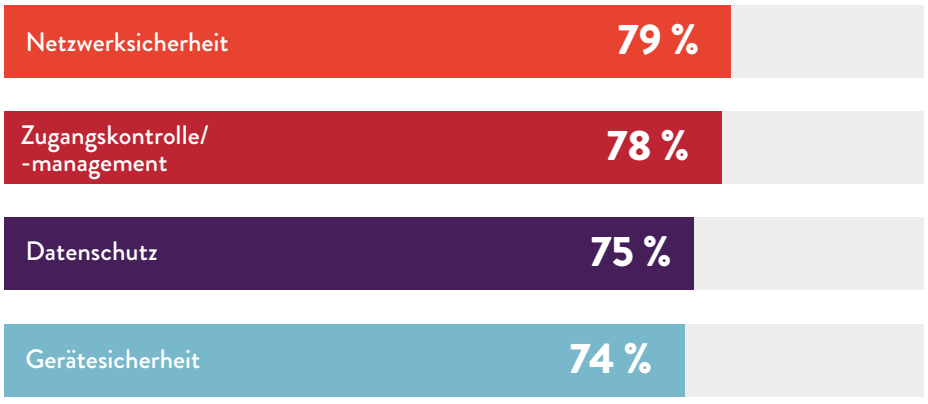
Aber diese Lösungen werden nur sehr selten auf Druckern implementiert. Während Netzwerksicherheitslösungen von 83 % der Befragten auf Desktop-PCs/Laptops und von 55 % auf mobilen Geräten verwendet werden, setzen nur 41 % sie auf Druckern ein.[1]

Bei der Endgerätesicherheit sind die Unterschiede noch größer:



Zudem implementiert nicht einmal ein Drittel (28 %) der Befragten Sicherheitszertifikate für Drucker, im Unterschied zu 79 % für PCs und 54 % für mobile Geräte.[1]

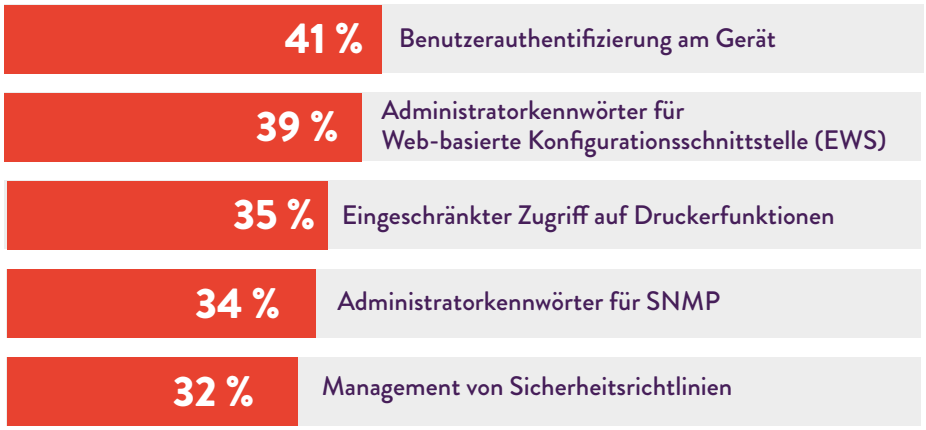
WICHTIGSTE SICHERHEITSVERFAHREN FÜR ENDGERÄTE



Von den auf allgemeinen Endgeräten verwendeten Schutzmaßnahmen werden auf Druckern am häufigsten Lösungen für Dokumentsicherheit, Netzwerksicherheit und Zugangskontrolle genutzt. Jedoch gab weniger als die Hälfte der Befragten an, dass ihr Unternehmen solche Lösungen für seine Drucker einsetzt.[1]

Einige Unternehmen verwenden druckerspezifische Sicherheitsmaßnahmen, aber auch hier bestehen enorme Unterschiede. Knapp über 40 % der Unternehmen haben eine Benutzerauthentifizierung implementiert. Weniger als 40 % verwenden Administratorkennwörter für die Web-basierte Konfigurationsschnittstelle.[1] Für einen wirksamen Schutz müsste jedes Unternehmen eine Kombination dieser Verfahren einsetzen – aber das alleine reicht nicht aus.

WICHTIGSTE DRUCKERSPEZIFISCHE SICHERHEITSVERFAHREN



Wenn es um Verfahrensweisen für Endgeräte-Compliance und -überprüfung geht, hinkt die Druckersicherheit fast allen anderen Endgeräten hinterher. In fast 90 % der Unternehmen wurde eine Richtlinie für Informationssicherheit implementiert. Diese Richtlinien schließen jedoch normalerweise nicht die Drucker ein. Ein Beispiel: Während 57 % der Befragten angab, dass auf ihren PCs Schutzsysteme gegen Malware implementiert sind, haben nur 17 % diese Systeme auf Druckern implementiert.[1]

FAST 9 VON 10 IT-EXPERTEN GEBEN AN, DASS IHR UNTERNEHMEN EINE RICHTLINIE FÜR DATENSICHERHEIT IMPLEMENTIERT HAT, UND ZWAR AUS DEN FOLGENDEN GRÜNDEN:

Offensichtlich nehmen Unternehmen die Druckersicherheit nicht ernst genug – das ist definitiv ein Fehler.

„Auf vielen Druckern werden noch immer die Standardkennwörter oder gar keine Kennwörter oder auf zehn Druckern dieselben Kennwörter verwendet“, so Michael Howard, Chief Security Advisor bei HP gegenüber Computerworld im Juni. „Ein Drucker ohne Kennwortschutz ist eine Goldmine für einen Hacker. Eine häufige Sicherheitsverletzung ist ein Man-in-the-Middle-Angriff. Dabei übernimmt ein Angreifer die Kontrolle über einen Drucker und leitet [eingehende Dokumente] an einen Laptop weiter, bevor sie gedruckt werden. So kann er alles lesen, was der CEO druckt.“[2]

POTENZIELLE AUSWIRKUNGEN EINES ERFOLGREICHEN DRUCKERANGRIFFS

Gemäß Bogdan Botezatu, Senior E-Threat Analyst bei Bitdefender, stellen Drucker eine riesige potenzielle Sicherheitslücke dar. „Wir empfangen ein großes Volumen an Telemetriedaten in unseren Labors für Schwachstellenanalyse. Der Router ist nicht mehr das am stärksten gefährdete Gerät im Internet. Dieses Gerät ist jetzt der Drucker.“[3]

Diese Schwachstelle kann fatale Folgen für ein Unternehmen haben. Durch einen einzigen ungeschützten Drucker kann Ihr gesamtes Netzwerk einem Angriff zum Opfer fallen. So erhalten Hacker die Möglichkeit, Ihre Netzwerkgeräte auszuspähen und die Sicherheit des ganzen Netzwerks zu gefährden.

Wir alle kennen die Auswirkungen von Sicherheitsverletzungen. In der Untersuchung von Spiceworks haben die Befragten die folgenden fünf wichtigsten Auswirkungen einer Sicherheitsverletzung genannt:[1]

1. Mehr Anrufe beim Help Desk und Zeitaufwand für Support

2. Geringere Produktivität/Effizienz

3. Längere Systemausfallzeit

4. Mehr Zeitaufwand für Supportanrufe

5. Durchsetzung von mehr Endbenutzerrichtlinien

Jedoch kann eine Sicherheitsverletzung beim Drucker noch schwerwiegendere Folgen haben, insbesondere wenn es sich um ein Multifunktionsgerät handelt, das gedruckte Daten elektronisch speichern

kann. Über Druckjobs, die im Drucker-Cache gespeichert sind, erhalten Hacker Zugriff auf vertrauliche persönliche oder geschäftliche Informationen.

Was noch besorgniserregender ist: Über einen ungeschützten Drucker können Hacker auf das gesamte Unternehmensnetzwerk zugreifen und vertrauliche Informationen wie Sozialversicherungsnummern, Finanzdaten oder interne Memos und Dokumente stehlen. Diese gestohlenen Informationen schaden nicht nur einzelnen Mitarbeitern, sondern können von Konkurrenten zu ihrem Vorteil genutzt oder eingesetzt werden, um den Ruf eines Unternehmens zu beschädigen.

DIE EINFACHE LÖSUNG: INTEGRIERTE SICHERHEITSFUNKTIONEN

Kein Zweifel, Unternehmen müssen die Sicherheit auch bei ihren Druckern erhöhen. Einige der modernen Drucker der Enterprise-Klasse sind ab Werk mit benutzerfreundlichen integrierten Sicherheitsfunktionen ausgestattet. Dazu gehören:

- Automatische Angriffserkennung, Schutzmaßnahmen und Wiederherstellung
- Nutzungsverfolgung zur Verhinderung der unbefugten Verwendung
- Einfache Anmeldeoptionen wie PIN oder Smartcards
- Lesegerät für Transponderkarten, das Benutzern die schnelle Authentifizierung und den sicheren Druck mit ihrem Ausweis ermöglicht
- Sicheres verschlüsseltes Drucken für vertrauliche Dokumente

Wenn Sie über den Kauf Ihres nächsten Druckers nachdenken, unabhängig davon, ob es um einen Desktop-Drucker oder ein Multifunktionsgerät geht, sollten Sie sich über die integrierten Sicherheitsfunktionen des Geräts informieren - und diese auch nach dem Kauf aktivieren. Mit einfachen, druckerspezifischen Funktionen wie diesen können Sie Schwachstellen durch Ihre Drucker sehr leicht vermeiden. Schließlich gibt es mit dem Internet der Dinge noch genügend Zugangspunkte, über die Sie sich Sorgen machen müssen – **auch ohne Ihre Drucker.**

SIE SUCHEN DRUCKER MIT HÖHERER SICHERHEIT?

ERFAHREN SIE MEHR ›

Quellen:

[1] Spiceworks Befragung von 309 IT-Entscheidungsträgern in Nordamerika, EMEA und APAC im Auftrag von HP, November 2016.

[2] „Printer Security: Is your company's data really safe?" *Computerworld*, 1. Juni 2016. http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

[3] „Printers Now the Least-secure Things on the Internet", *The Register*, 8. September 2016. http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/