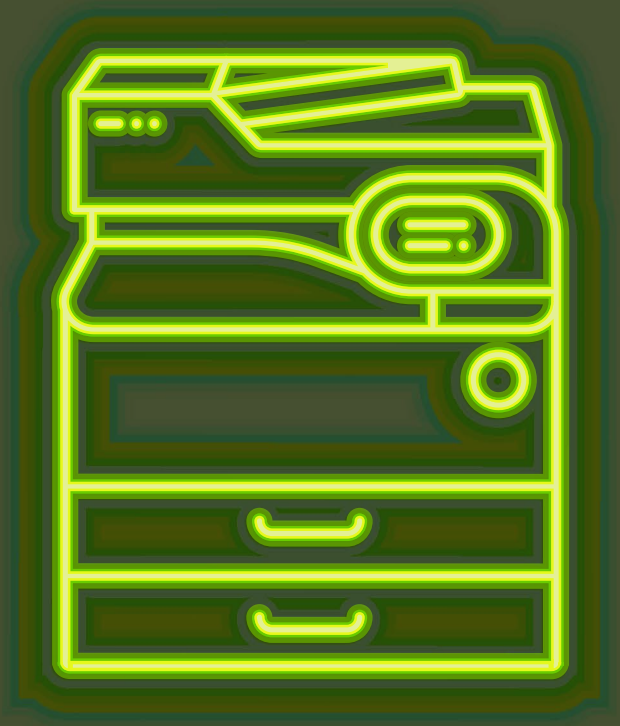
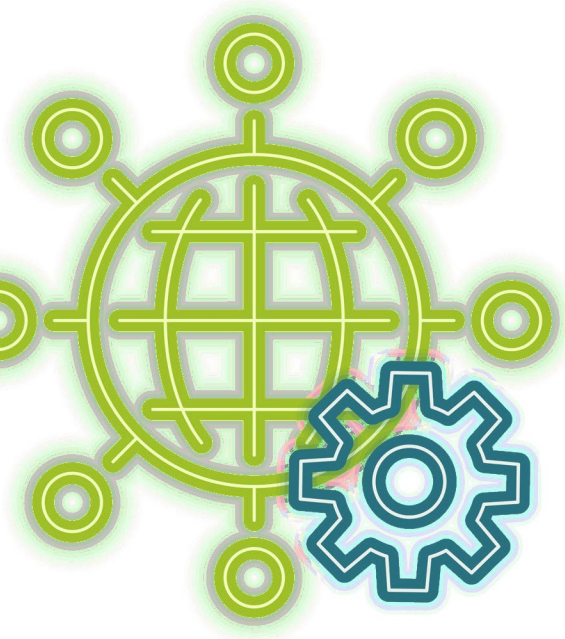
Druckersicherheit: Das neue Muss für Ihre IT

Eine Studie zeigt, dass Sicherheitsgefahren durch Drucker nach wie vor ignoriert werden



Inhaltsverzeichnis



Einführung

Die Bedrohungen der IT-Sicherheit nehmen ständig zu – doch der Schutz der Hardware hält oft nicht mit. Das wird in keinem Bereich so deutlich wie bei den Druckern. Obwohl immer mehr IT-Fachleute die Gefahr erkennen, die durch ungeschützte Drucker im Netzwerk entsteht, bleiben Drucker sicherheitstechnisch ein blinder Fleck: Sie sind in den meisten Fällen zu wenig geschützt.

„Schwachstellen zeigen sich bei allen möglichen Geräten innerhalb eines Netzwerks, auch beim simplen Netzwerkdrucker“, erklärt der Geschäftsführer des Bereichs Drucksysteme bei HP South Pacific, Ben Vivoda. **„Der Drucker ist ein typischer Fall für Geräte, die übersehen werden und dadurch exponiert sind. Aber Unternehmen können es sich nicht mehr leisten, Drucker in ihrer Gesamtstrategie für Cybersicherheit außen vor zu lassen.“**[1]

Tatsächlich sind Drucker laut einer aktuellen Studie von Spiceworks zunehmend Ursache für Sicherheitsbedrohungen. Im Vergleich zu 2016 liegt die heutige Wahrscheinlichkeit, dass Drucker Ziel externer Bedrohungen oder Angriffe werden, um 68 % höher. Bei internen Bedrohungen oder Angriffen ist die Wahrscheinlichkeit sogar um 118 % gestiegen.

Trotzdem sind sich nur 30 % der IT-Profis bewusst, dass Drucker ein Sicherheitsrisiko darstellen. Der Prozentsatz hat sich seit 2016 zwar ungefähr verdoppelt, ist aber immer noch zu niedrig und spiegelt eine gefährliche Wirklichkeit wider. Viele IT-Profis haben offenbar noch immer veraltete Ansichten zur Druckersicherheit. Vielleicht weil sie denken, dass Drucker innerhalb eines Netzwerks geschützt sind.

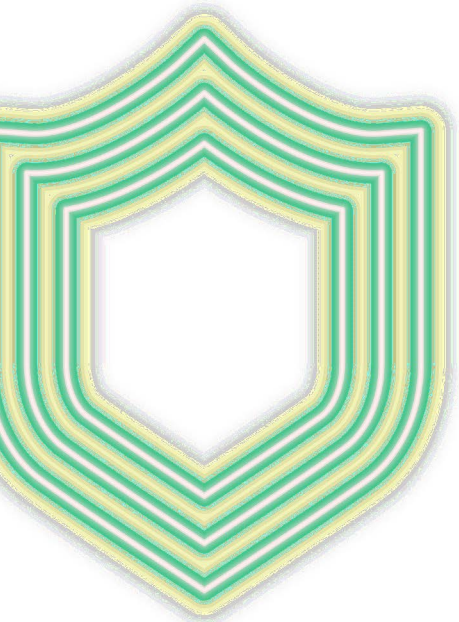
Und selbst Spezialisten, die das Risiko kennen, richten ihren Fokus meist auf andere Geräte; um Drucker kümmern sich die wenigsten – das heißt, die Netzwerke bleiben verwundbar.[2] Obwohl es verständlich ist, dass die Druckersicherheit in der Vergangenheit verglichen mit anderen Endpunkten eine untergeordnete Rolle spielte, müssen IT-Abteilungen heute unbedingt damit anfangen, das Risiko ungeschützter Drucker für die IT-Infrastruktur und die Risikobeherrschung im Unternehmen anzugehen.

Die Risiken für das Geschäft

Sind Drucker wirklich ein Problem? Kurz gesagt: Ja. In einer Zeit, in der stündlich neue Sicherheitsbedrohungen auftauchen, ist der Drucker ein leichtes Ziel. „Genau genommen sind moderne Drucker äußerst fortschrittliche, spezialisierte Netzwerk-Hosts, die die gleiche Aufmerksamkeit in puncto Sicherheit verdienen wie herkömmliche Computer“, führt Kevin Pickhardt in *Entrepreneur* aus.[2] „Bürodrucker sind nicht nur potenzielle Quellen für Datenverluste und Vertraulichkeitsprobleme, sondern auch Angriffsvektoren, die Hacker ausnutzen können.“</6 Nur ein Beispiel: 2017 gab es Berichte über einen Hacker, der ein automatisiertes Script nutzte, um auf 150.000 öffentlich zugängliche Drucker – einschließlich zahlreicher Belegdrucker – zuzugreifen und Fake-Druckaufträge zu erteilen.[3]

Branchenkenner sind derselben Meinung. Laut IDC verfügen die meisten Drucker über „umfassenden Zugriff auf das interne Netzwerk. **Ein Angreifer, der einen Drucker kapert, kann ungehindert ins Netzwerk, in Anwendungen und in sensible Datenbestände von Unternehmen eindringen.“** [4]

Aber woran erkennt man einen Netzwerkdrucker, der nicht ausreichend geschützt ist? Ohne Absicherung ist er weit offen für zahllose Netzwerkprotokolle. Er arbeitet ohne Zugriffskontrolle (selbst das Anlegen eines Admin-Passworts wird oft vergessen). Er ermöglicht das Drucken sensibler Dokumente ohne Authentifizierung, sodass die Dokumente den ganzen Tag für jedermann zugänglich im Ausgabefach liegen bleiben können. Er versendet unverschlüsselte Daten im Netzwerk. Seine Firmware ist veraltet. Und er wird nicht in Bezug auf Sicherheitsbedrohungen überwacht.

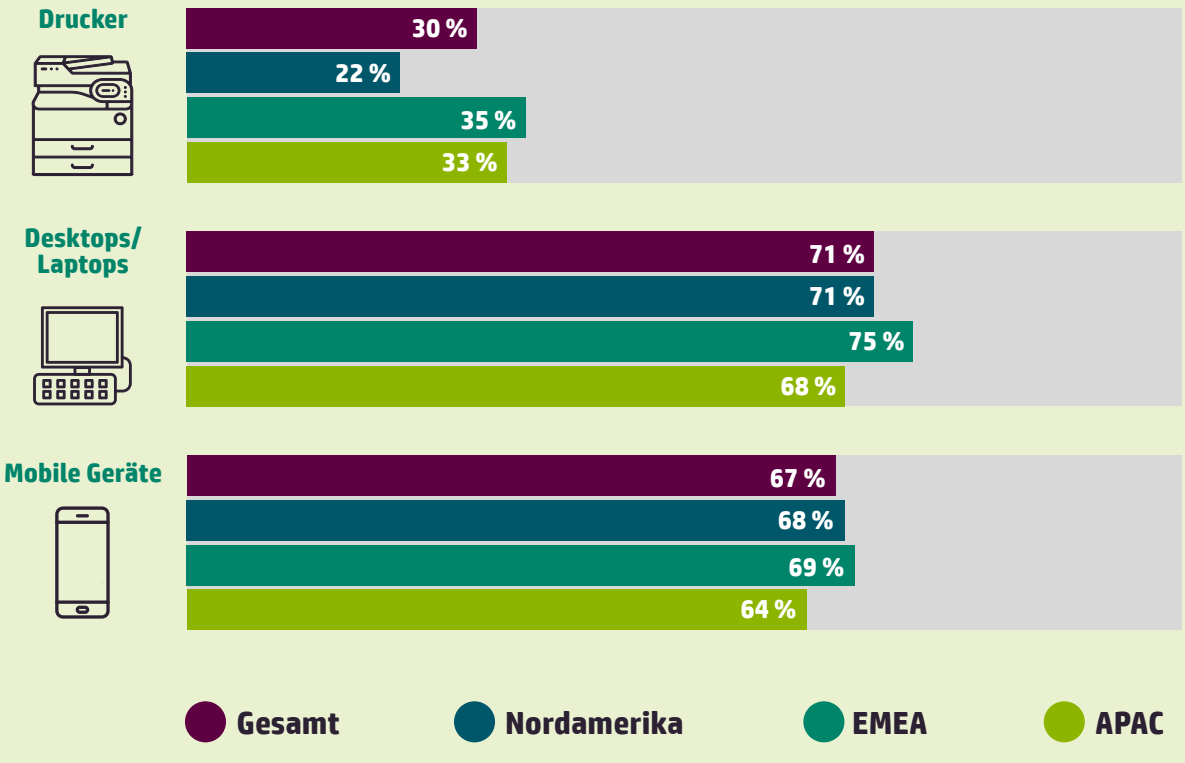


All diese Sicherheitsmängel haben Folgen. Gartner sagt voraus, dass bis 2020 mehr als die Hälfte aller Projekte im Internet der Dinge (IoT) sensible Informationen dadurch preisgeben werden, dass die Sicherheitsfunktionen der Hardware nicht zum Einsatz kommen. Heute sind es weniger als 5 %.[4]

Fehlendes Problembewusstsein

Trotz der Forschungsergebnisse tun sich IT-Profis nach wie vor schwer damit, wahrzunehmen, wie gefährdet Drucker sind. In Nordamerika betrachten nicht einmal ein Viertel aller IT-Profis (22 %) Drucker als Sicherheitsrisiko. In Europa, im Mittleren Osten und in Afrika (EMEA) ist diese Zahl mit gut einem Drittel (35 %) nur unwesentlich höher.

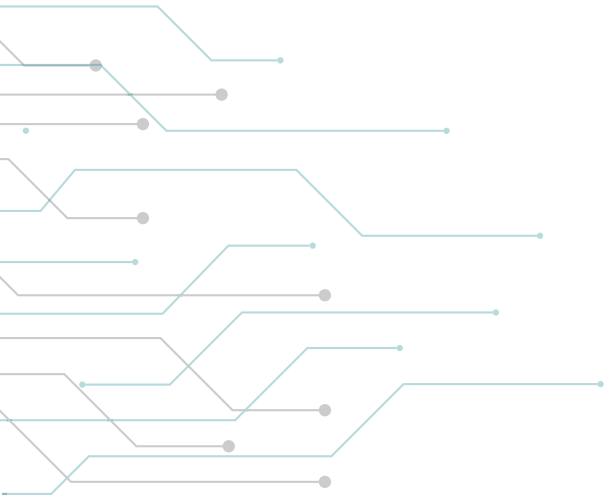
Als Sicherheitsrisiko erkannt



Im Gegensatz dazu erkennen 71 % der IT-Profis das Risiko, das durch Desktop-PCs und Laptops entsteht; in Bezug auf Mobilgeräte sind es 67 %.

Die Recherchen von Spiceworks decken zudem auf, dass viele IT-Profis, die vorbeugende Maßnahmen ergriffen haben, keinen stringenten Ansatz verfolgen. Das ist angesichts der vielen unterschiedlichen Sicherheitsanforderungen auch kein Wunder. Eine einfache Lösung reicht nicht aus. Zum Beispiel ist es lediglich mit einer Firewall noch nicht getan. Wie bei allen Netzwerkgeräten muss die Druckersicherheit von vielen Seiten aus angegangen werden. Und wie bei jeder Sicherheitsstrategie sind die effektivsten Lösungen integriert, automatisiert, benutzerfreundlich und einfach zu verwalten.

Groß wird die Herausforderung auch dadurch, dass jeder Druckerhersteller seine eigene Software und sein eigenes Betriebssystem nutzt. Viele IT-Profis besitzen wahrscheinlich nicht genügend Know-how, um die Druckersoftware so zu konfigurieren, dass die Sicherheitsrichtlinien erfüllt werden.



Gängige Praxis

IT-Profis verfolgen verschiedene Ansätze in Richtung Druckersicherheit, was zu einem Sammelsurium an Sicherheitsverfahren und -funktionen führt – abhängig von den Tools, die man im konkreten Fall verfügbar hat und technisch beherrscht. Im Großen und Ganzen lassen sich die Ansätze aber in sechs Kategorien einordnen.

Anteil der Umfrageteilnehmer, die zurzeit folgende Sicherheitspraktiken für Drucker anwenden

42 % Dokumentensicherheit

31 % Gerätesicherheit

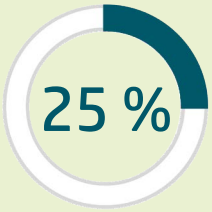
40 % Netzwerksicherheit

30 % Sicherheitsüberwachung

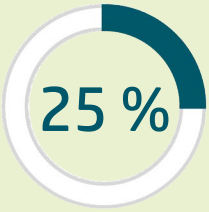
39 % Zugriffskontrolle

28 % Datenschutz

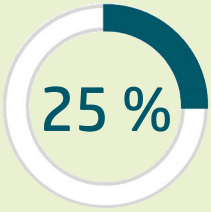
Die Studie zeigt, dass es IT-Profis gibt, die diverse grundlegende Sicherheitsschritte aus diesen Kategorien durchführen – sie machen aber nur einen relativ geringen Prozentsatz aus.



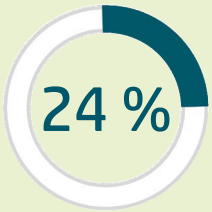
Schließen ungenutzter offener Anschlüsse



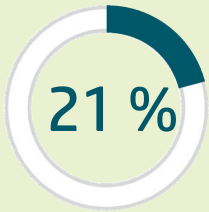
Aktivieren der Funktion „Gesendet von“



Sichere Druckerreparaturen



Einführung von geschütztem Drucken („Pull-Printing“)

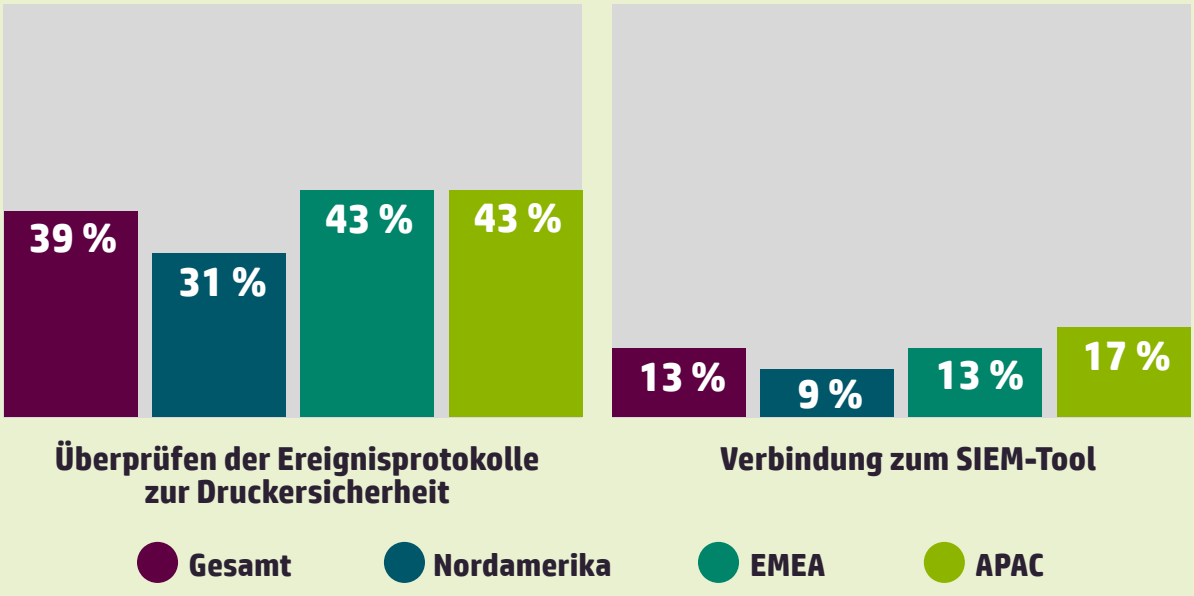


Routinemäßiges Löschen der Druckerfestplatte

Noch geringer ist die Zahl der IT-Profis, die Druckaufträge nach einem festen Zeitplan verfallen lassen bzw. löschen, einen Admin-Zugang für Konfigurationsänderungen anlegen oder die Zertifikatsverwaltung automatisieren.

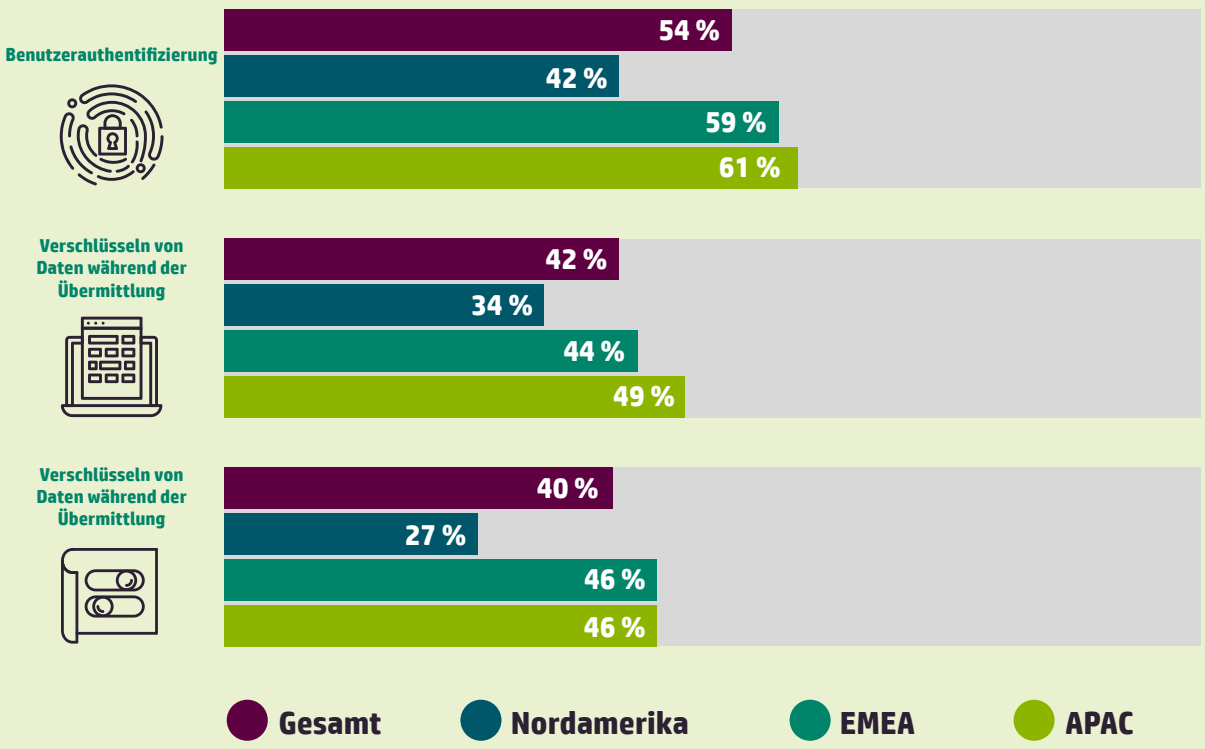
Zwar überwacht man inzwischen häufiger die Druckersicherheit – doch es bleibt ein Minderheitenphänomen: Nur 39 % der Verantwortlichen geben an, die Druckerprotokolle routinemäßig zu prüfen. In Nordamerika sind es nur 31 %. Was den Anschluss von Druckern an SIEM-Tools betrifft, geben nur 13 % an, entsprechend aktiv geworden zu sein. Dadurch, dass Druckerprotokolle nicht überwacht werden und Drucker nicht mit SIEM-Tools verbunden sind, tappt die IT im Dunkeln; Cyberkriminelle, die unbewachte Infrastruktur als Versteck im Netzwerk nutzen, um Daten herauszufiltern, werden einfach übersehen.

Druckerüberwachung



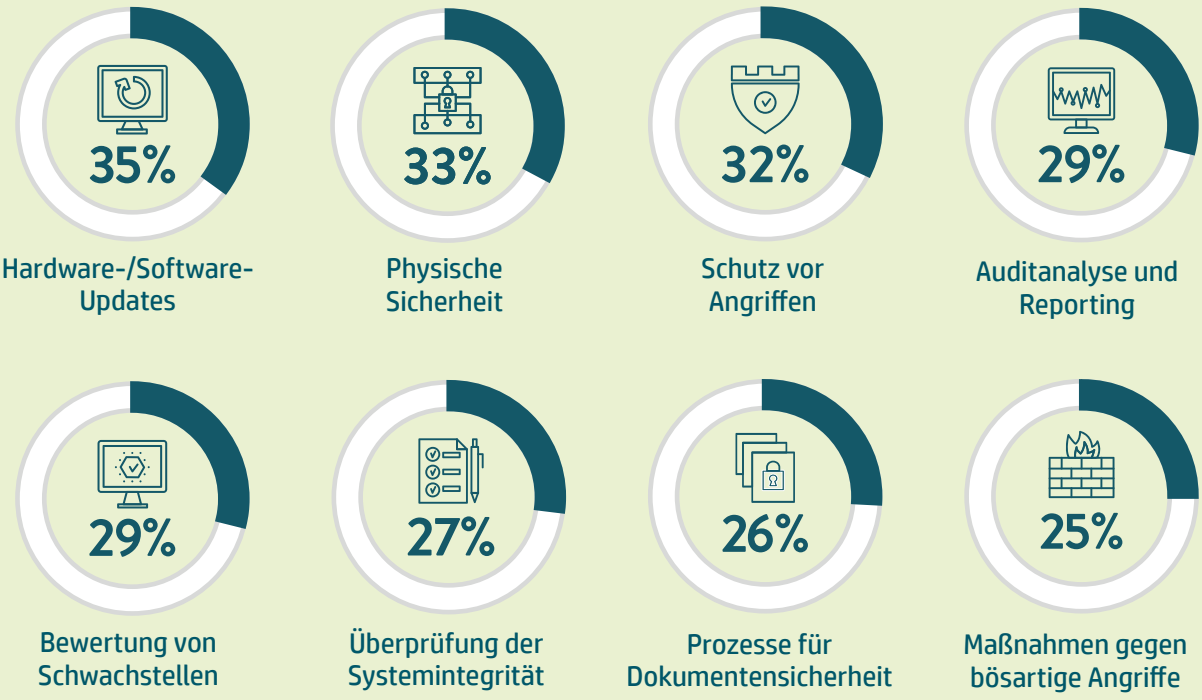
Die Studie deckt noch weitere Unterschiede zwischen den Regionen auf – und wieder liegt Nordamerika in puncto Druckersicherheit hinten. Dies gilt besonders für die Bereiche Zugriffskontrolle und Verschlüsselung. Gegenüber Nordamerika verschlüsseln IT-Profis in APAC mit deutlich höherer Wahrscheinlichkeit ihre Daten bei der Übertragung; sie verlangen häufiger eine Authentifizierung auf Geräteebene; und sie vergeben häufiger Zugriffsrechte basierend auf der Rolle des Nutzers im Unternehmen.

Eingesetzte Verfahren zur Druckersicherheit



Auch wenn es um die Einhaltung von Datenschutzbestimmungen geht, kommen unterschiedlichste individuelle Strategien zum Einsatz; in einigen Fällen ist die Druckerkontrolle in die Gesamtstrategie zur IT-Compliance integriert. In der Spiceworks Studie wurden IT-Profis gefragt, welche Compliance-Kontrollen sie auf Basis von „CIS Controls V7“ des Center for Internet Security umgesetzt haben.[5]

Eingesetzte Compliance-Kontrollen



Die Daten zeigen, dass IT-Profis oft die grundlegendsten Vorsichtsmaßnahmen für Drucker übersehen, z. B. die Aktualisierung der Firmware. Nur ein Drittel erklärt, diese Aufgabe im Rahmen der Compliance-Routine auszuführen. Branchenstudien zeigen dieselben Ergebnisse. Laut IDC wird die Firmware bei Druckern häufig nicht aktualisiert, weil die Unternehmen das Risiko sehr oft unterschätzen.4 Hinzu kommt, dass ihnen häufig die Zeit fehlt, um neue Firmware für sämtliche Drucker im Bestand zu prüfen, zu testen und abzunehmen.

Auf dem Weg zu umfassender Druckersicherheit

Von den 84 % der IT-Profis, deren Unternehmen Sicherheitsrichtlinien festgelegt haben, geben nur 64 % an, dass auch die Drucker von diesen Richtlinien abgedeckt sind. In Nordamerika beläuft sich die Quote auf nur 52 %. Das zeigt, wie dringend notwendig es ist, integrierte und automatisierte Kontrollmechanismen in Sachen Druckersicherheit zu entwickeln und tatsächlich umzusetzen. Drucker mit eingebauten Sicherheitsfunktionen minimieren das Risiko und maximieren gleichzeitig die IT-Effizienz.

Denn IDC-Analysten haben auch das herausgefunden: „Drucker sind deutlich schwieriger zu sichern, wenn sie bereits im Unternehmen stehen; das zeigt nochmals, wie wichtig es ist, sich von vornherein für Geräte zu entscheiden, die bereits über umfangreiche moderne Sicherheitsfeatures verfügen.“ [4] Und Gartner führt aus: „Um die entstehende Marktdynamik für Drucker zu nutzen, müssen die technologiestrategischen Planer ein umfassendes Portfolio an Sicherheitslösungen für Drucker aufbauen, das die Best Practices der Sicherheitsbranche sogar noch übertrifft. Diese Lösungen müssen in das Gesamtsystem für Sicherheitslösungen integriert werden.“[6]

Auch Anbieter von Druckermanagementdiensten passen sich an eine neue Nachfrage an: Sie weiten ihren Service aus, um IT-Abteilungen zu unterstützen, die personell nicht so breit aufgestellt sind, dass sie die Challenge Druckersicherheit allein bewältigen können. IDC schreibt: „Der Markt bietet zahlreiche Services für den Schutz auf Geräte- und Datenebene, die sich problemlos in bestehende Systeme für das Dokumenten- und Enterprise Content Management (ECM) integrieren lassen, um den Schutz zu erweitern, die Verwaltung zu erleichtern und optimale Compliance zu gewährleisten.“[7]

Ebenfalls zum Glück für IT-Profis bieten moderne Drucker dutzende integrierter Sicherheitsfunktionen: Gefahrenerkennung, Schutzmaßnahmen, Benachrichtigungen, eigenständige Fehlerbehebung – all das macht es so einfach wie nie, eine entscheidende Schwachstelle Ihres Netzwerks endlich abzusichern.

Es ist Zeit für echte Druckersicherheit.

Weitere Informationen

Über die Studie

HP beauftragte Spiceworks im Mai 2018 mit der Durchführung der Studie. Sie richtet sich an Entscheidungsträger im IT-Bereich – IT-Bereichsleiter, IT-Manager und andere IT-Mitarbeiter. Ermittelt wurde, welche Sicherheitspraktiken zurzeit genutzt werden und welche Risiken bestehen. Die Studienergebnisse spiegeln die Antworten von ca. 500 Teilnehmern in Nordamerika, EMEA und APAC wider, die in Unternehmen mit mehr als 250 Mitarbeitern beschäftigt sind.

Quellen

1 McLean, Asha, "Unsecured printers a security weak point for many organisations: HP", *ZDNet*, 18. April 2017. https://www.zdnet.com/article/unsecured-printers-a-security-weak-point-for-many-organisations-hp/

2 Pickhardt, Kevin, „Why Your Innocent Office Printer May Be a Target For Hackers", *Entrepreneur*, 31. Januar 2018. https://www.entrepreneur.com/article/308273

3 Peyser, Eve, „Hacker Claims He Hacked 150,000 Printers to 'Raise Awareness' About Hacking", *Gizmodo*, 6. Februar 2017. https://gizmodo.com/hacker-claims-he-hacked-150-000-printers-to-raise-aware-1792067012

4 Brown, Duncan, et al., „IDC Government Procurement Device Security Index 2018", *IDC*, Mai 2018.

5 „CIS Controls", *Center for Internet Security*, März 2018. https://www.cisecurity.org/controls/

6 Von Manowski, Kristin Merry und Deborah Kish, „Market Insight: IoT Security Gaps Highlight Emerging Print Market Opportunities", *Gartner*, 31. Oktober 2017 https://www.gartner.com/doc/reprints?id=1-4OCKFKG&ct=180110&st=sb

7 Palmer, Robert und Allison Correia, „IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment", IDC, 2017.