Sicheres Drucken

JEDER NUTZT SIE, ZU WENIGE SCHÜTZEN SIE: DRUCKER UND MULTIFUNKTIONSGERÄTE

Wenn es um die Sicherheit und den Datenschutz ihrer Arbeitsplatzrechner geht, überlassen viele Unternehmen nichts mehr dem Zufall und sorgen für eine hinreichende Absicherung. Anders hingegen sieht es oftmals bei den eingesetzten Druckern und Multifunktionsgeräten aus. Sie bleiben häufig unter dem Radar, viele Funktionen sind unbemerkt im Hintergrund aktiv. Die Datenschutz-Grundverordnung (DSGVO) fordert jedoch technische und organisatorische Maßnahmen zum Schutz der Daten auch beim Scannen, Kopieren und Drucken. Ein Leitfaden hilft bei der Umsetzung.

Montag Morgen, ab 06:30 Uhr. In vielen Büros spielt sich das gleiche Szenario ab: Kolleginnen und Kollegen treffen ein, fahren ihre PCs hoch und holen sich ihren Kaffee oder Tee in der Küche, um dann mit der Arbeit zu starten. Etwa eine halbe Stunde später laufen die Drucker und Multifunktionsgeräte (MFP) auf den Fluren heiß. Ein Kollege geht zum Drucker, möchte sich seinen Druckauftrag abholen und findet weitere Dokumente im Ausgabefach – datiert von Freitagmittag – wohin sollen die Unterlagen, wenn kein Name darauf steht? Meist bleiben sie im Ausgabefach, landen direkt im Papierkorb oder im „Kopierer-Ablagefach für vergessene Dokumente“, für alle zugänglich, direkt neben dem Drucker. Ein Szenario, das sich nicht nur zum Start einer neuen Woche wiederholen kann, sondern täglich. Wussten Sie, dass die beschriebene Situation gleich zwei Gefahren birgt? Neben der Gefahr eines visuellen Hacks verstößt man je nach Inhalt der Dokumente womöglich auch gegen den Datenschutz: Unterlagen, die unnötig lange im Ausgabefach liegen, sind für Dritte einsehbar. Die Folge können enorme Kosten durch Strafen und Rechtsstreitigkeiten sein. Es droht Imageverlust, und die Kunden verlieren das Vertrauen. Und dies sind nicht die einzigen Gefahren, die von MFP und Drucker ausgehen – welche lauern noch?

Unterschätztes Risiko: Sicherheitslücken beim Drucken, Scannen und Kopieren

Da viele Funktionen wenig offensichtlich und einige Einstellungsmöglichkeiten nicht bekannt sind, sehen die meisten Unternehmen in Druckern und Multifunktionsgeräten kein Sicherheitsrisiko. Dies kann zu verheerenden Sicherheitslücken führen, denn bei jeder Benutzung verarbeiten und speichern die Geräte Daten – darunter auch personenbezogene. Die Geräte senden und empfangen laufend solche Daten über das Unternehmensnetzwerk. Damit sind Drucker und MFP unterschätzte Einfallstore für Hackerangriffe. Um dies zu verhindern, müssen Geschäftsführung, IT-Sicherheitsbeauftragte sowie Chief Information Security Officers gemeinsam ein unternehmensweites IT-Sicherheitskonzept erarbeiten und erfolgreich integrieren.

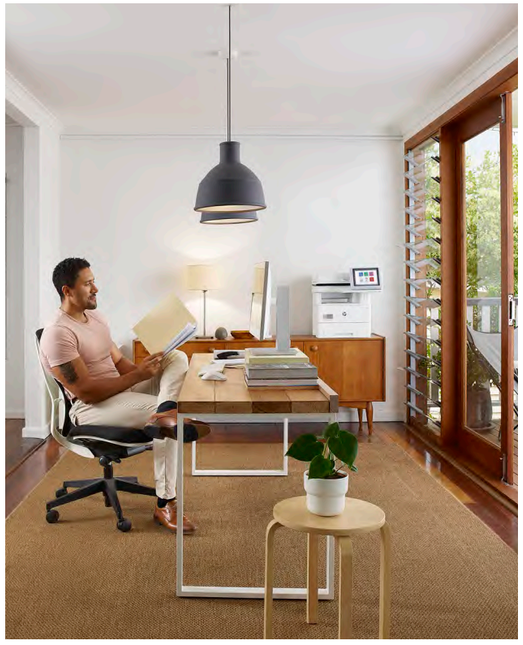
Diese Risiken sollten Sie kennen:

- **Das verwundbare Firmennetz**
  Drucker und MFP sind als netzwerkfähige Geräte besonders gefährdet, wenn sie ohne entsprechende Sicherungen vom Internet aus zu erreichen sind. Hacker können in der Geräte-Software schadhaften Code unterbringen und damit tiefer ins Firmennetzwerk eindringen.

- **Die verstreuten Daten**
  Relativ häufig kommt es zu sogenannten Man-in-the-Middle-Angriffen, bei denen die zu druckenden Informationen an den Rechner des Angreifers umgeleitet und dann erst an den Drucker geschickt werden – somit fällt das Mitlesen niemandem auf. Zum Beispiel konnten Studierende auf diese Weise Druckaufträge ihres Professors mitlesen, um vorab an die Klausuren zu kommen. Mit MFP lassen sich Dokumente zudem per E-Mail und Fax versenden. Fehlen Beschränkungen, besteht die Gefahr, dass Angreifer unter Angabe eines fremden Absenders Unterlagen intern und extern verbreiten.

- **Das vergessene Gedächtnis**
  Viele Nutzer glauben, dass ein Multifunktionsgerät mit dem Ausdruck einer Seite deren Inhalt vergisst. Das ist jedoch ein Fehler: MFP speichern Daten für Bildbearbeitung und Druck auf ihrer Festplatte – und dort bleiben sie bei älteren Geräten sogar unverschlüsselt. Zudem liegen ausgedruckte Dokumente oft viel zu lange im Ausgabefach des Geräts, das in vielen Unternehmen leicht zugänglich in einem separaten Raum oder im Flur steht. Somit sind die Dokumente für jeden einsehbar, bis sie jemand abholt.

- **Die verräterischen Metadaten**
  Metadaten enthalten besondere Informationen, wie Datum, Uhrzeit, Zugangsdaten für Netzlaufwerke, den Inhalt der Druckaufträge oder den Namen der Person, die den Druck anstößt. Viele Drucker und MFP zeigen diese bereits im Bedienfeld und auf dem Webserver an. Ohne entsprechende Konfiguration vergisst ein Drucker nichts und die Aufträge bleiben einsehbar.



Homogene Druckerflotte erleichtert Konfiguration

Leistungsstarke Drucker und MFP bringen viele Funktionen mit – zur Freude der Anwender, zum Leidwesen der IT-Admins. Denn die zahlreichen Einstellungsmöglichkeiten müssen sicherheits- und datenschutzkonform konfiguriert werden. Hat ein Unternehmen keine homogene Druckerflotte, sondern unterschiedliche Geräte von verschiedenen Anbietern im Einsatz, ist der Aufbau einer Sicherheitsrichtlinie für MFP mit hohen Aufwänden verbunden. Wenn darüber hinaus Management-Tools fehlen, die einen Remote-Zugriff ermöglichen, sind viele IT-Abteilungen komplett überlastet. Doch neben diesen Herausforderungen sind auch gesetzliche Auflagen zu beachten.

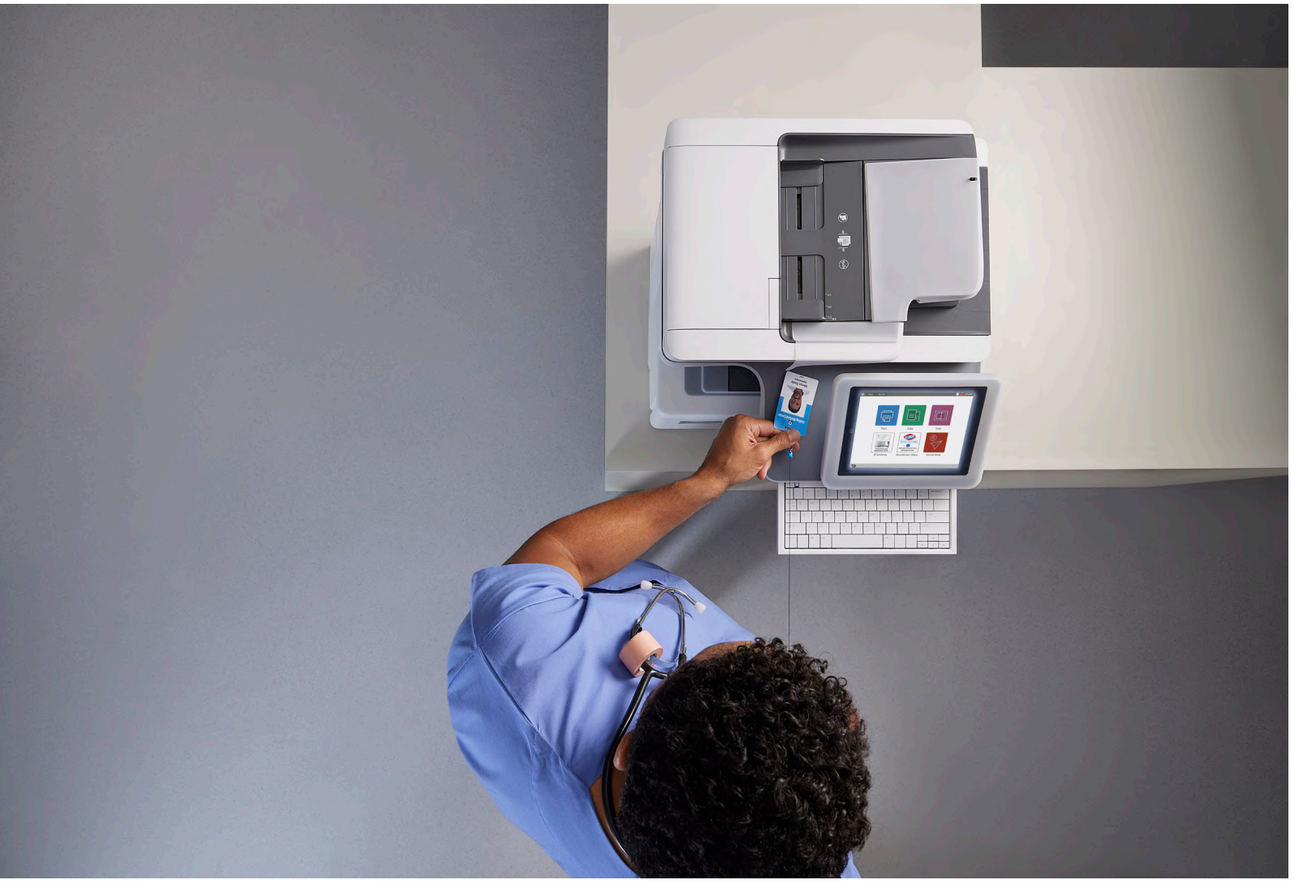
Unsichere Wege zur sicheren Druckumgebung

Unternehmen orientieren sich beim Aufbau einer IT-Sicherheitsrichtlinie an den Empfehlungen von Fachverbänden und Behörden, zum Beispiel am Bundesamt für Sicherheit in der Informationstechnik (BSI) – einer zentralen Instanz mit dem Bestreben, Lücken in der IT-Sicherheit zu schließen. Es hat mit dem IT-Grundschutz eine Richtlinie entwickelt, die als anerkannter Standard für IT-Sicherheit Orientierungshilfen bietet. Sie schafft für Unternehmen eine Grundlage zur Entwicklung eines Managementsystems für Informationssicherheit (ISMS). Das IT-Grundschutz-Kompendium beschäftigt sich explizit mit den Anforderungen an Drucker, Kopierer und MFP. Die Herausforderung für Unternehmen besteht allerdings darin, diese Anforderungen praxisnah, mit geringem Aufwand und auf die eigene Infrastruktur zugeschnitten umzusetzen. Das ist nicht einfach, und viele fragen sich: Was wird wirklich benötigt und wie setzt man es richtig ein?

Praxisleitfaden „Sicherheit und Datenschutz beim Drucken, Scannen und Kopieren“

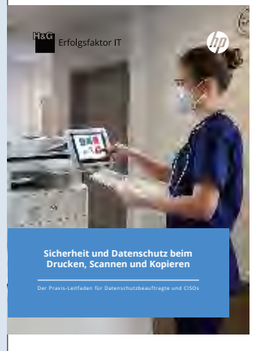
Ein gutes IT-Sicherheitskonzept auf die Beine zu stellen ist zweifellos im Sinne aller Unternehmen, doch um das Dickicht dabei aufkommender Fragen zu überwinden, bedarf es eines guten Konzepts. Der Praxisleitfaden „Sicherheit und Datenschutz beim Drucken, Scannen und Kopieren“ für Datenschutzbeauftragte und CISOs gibt hilfreiche Tipps und Antworten auf unter anderem folgende Fragen:

- Wie werden die Anforderungen an eine Druckerflotte definiert?
- Wie entwickeln Unternehmen die passenden IT-Sicherheitsrichtlinien für ihre Bedürfnisse?
- Wie stellt man die Praxiswirksamkeit der definierten IT-Sicherheitsrichtlinien sicher?
- Wie können Management-Tools die IT-Abteilung entlasten?



DRUCK AUF DRUCKER

Sowohl das IT-Sicherheitsgesetz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) als auch die Datenschutz-Grundverordnung (DSGVO) verlangen technische und organisatorische Sicherheitsmaßnahmen. Artikel 32 der DSGVO legt fest, dass die Sicherheitsmaßnahmen nach dem „Stand der Technik“ gestaltet sein müssen, um „ein dem Risiko angemessenes Schutzniveau zu erreichen“. Jedoch werden bei beiden gesetzlichen Regelungen keine konkreten technischen Maßnahmen genannt, was aufgrund des steten technischen Fortschritts auch kaum Sinn machen würde. Woran können sich Verantwortliche orientieren? Unser Praxisleitfaden gibt Antworten auf diese und viele weitere Fragen.



Ausführliche Informationen über die Drucksicherheit finden Sie in unserem kostenfreien Praxisleitfaden „Sicherheit und Datenschutz beim Drucken, Scannen und Kopieren“

www.hug.de/praxisleitfaden-drucksicherheit-download/

HP AMPLIFY™ Power Services Partner

Ihr Ansprechpartner
Jan Gieraths

MPS Sales Consultant
+49 228 9080-781
jan.gieraths@hug.de