Schwachstelle Drucker

Ingrid Dypa / Carola Wolfgramm

Drucker und Multifunktionsgeräte sind Einfallstore für Cyber-Kriminelle und dürfen bei der Sicherung der IT-Infrastruktur nicht vernachlässigt werden. Dennoch wird dem Thema Print Security in vielen Behörden noch nicht die nötige Aufmerksamkeit geschenkt.

Mit dem Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) scheint die IT-Sicherheit zu einem hochbrisanten Thema geworden zu sein. Oder sind es die angekündigten hohen Strafen für den schlechten Schutz von Daten, die zum Handeln zwingen sowie die Angst, ein Opfer von Cyber-Kriminellen zu werden? Welcher Grund Unternehmen und Behörden auch immer antreibt, die Daten im eigenen Haus besser zu schützen, ist sekundär. Wichtiger ist, dass jedes Gerät in das Sicherheitskonzept eingebunden wird.

Ein häufig vernachlässigtes, obwohl von allen Anwendern regelmäßig genutztes Gerät, ist der Drucker beziehungsweise das Multifunktionsgerät. So gab in einer Umfrage des Unternehmens Spiceworks nicht einmal ein Drittel der Befragten (28 Prozent) an, Sicherheitszertifikate für Drucker implementiert zu haben. Zum Vergleich: Für PCs taten dies 79 Prozent, für mobile Geräte 54 Prozent der Umfrageteilnehmer.

In heutigen Büros sind jedoch alle Geräte vernetzt und ermöglichen somit einen Zugang von außen. Es wird unterschätzt, wie viele sensible Daten ungeschützt in Druckern gespeichert oder ausgedruckt werden. Nicht selten stehen die Geräte in einem zentralen, allen Mitarbeitern zugänglichen Raum und Ausdrucke liegen bis zur Abholung im Ausgabefach bereit. Dabei bieten die Geräte zahlreiche Anwendungen zum Schutz und zur Sicherheit der Daten. Ausgestattet mit einer Benutzerauthentifizierung und integrierten Druckfreigabefunktionen werden Druckaufträge beispielsweise erst dann gedruckt, wenn sich der Mitarbeiter am Gerät verifiziert – durch einen PIN-Code, eine Chipkarte, einen Finger- oder gar Iris-Scan. Dafür ist es nicht notwendig, ein Neugerät anzuschaffen. Bestehende Geräte können durch einfache externe Lösungen nachgerüstet werden.

Print Security nicht außer Acht lassen.

Es reicht heutzutage also nicht mehr aus, die IT-Infrastruktur im Bereich PCs und Notebooks weitläufig zu sichern und die Festplatten zu schützen. Ebensoviel Aufmerksamkeit ist auf die Drucker und Multifunktionsgeräte zu richten. Denn diese sind mit Festplatte, Netzwerkzugang, Betriebssystem, Internet-Zugang und der Möglichkeit des E-Mail-Versands ausgestattet. So können Trojaner beispielsweise über den Ausdruck von Phishingmails in das Netzwerk gelangen und die Steuerung der Daten oder der Geräte übernehmen. Unzureichend gesicherte Drucker sind ein Kinderspiel für Hacker, die Druckaufträge und Daten, wie etwa E-Mail-Adressen, auslesen und sich Zugriff auf weitere Endgeräte im Netzwerk verschaffen. Es ist daher nötig, das Thema Print Security in der eigenen Organisation neu zu definieren und in drei Ansätzen zu betrachten:

Geräte: Welche Sicherheitskriterien erfüllen sie? Ist eine aktuelle Firmware-Version auf der Modellreihe installiert? Sind sicherheitsrelevante Konfigurationen erstellt und per Admin-Passwort geschützt?

Gibt es eine Risikobewertungsmöglichkeit für die aktuelle Druckerflotte, und wie werden notwendige Veränderungen bewertet?

Daten: Wie sicher sind vertrauliche Informationen? Sind Daten beim Drucken oder auf der Festplatte verschlüsselt? Werden diese regelmäßig gelöscht? Sind die Druckjobs verschlüsselt? Wer kann auf die Konfigurationen der Maschine zugreifen und Einstellungen verändern? Werden Faxbuch und Festplatte bei einem Geräteaustausch BSI-konform gelöscht?

Dokumente: Welche Authentifizierungslösungen sind im Einsatz und wie werden ausgedruckte Dokumente vor unbefugtem Zugriff geschützt?

Dass das Thema Print Security von vielen noch stiefmütterlich behandelt wird, liegt am fehlenden Bewusstsein dafür, dass Drucker und Multifunktionsgeräte ein Sicherheitsrisiko darstellen, keine Ressourcen vorhanden sind und ein entsprechendes Budget nicht eingeplant ist. Eine Lösung für Unternehmen sowie Einrichtungen im behördlichen Umfeld bietet hier die Firma druckerfachmann.de mit ihrem Angebot „Print Security as a Service“. Dieses beinhaltet unter anderem eine Ist-Analyse der Output-Umgebung. Dazu gehören die Betrachtung der aktuellen Infrastruktur und vorhandenen Prozesse, eine toolgestützte Risikobewertung, die Erarbeitung einer individuellen Security-Richtlinie, die Implementierung eines Testverfahrens inklusive Inbetriebnahme mit Abgleich des Soll-/Ist-Zustands sowie die Einleitung eventueller Korrekturmaßnahmen.

druckerfachmann.de unterstützt zudem bei der Verabschiedung einer Security-Richtlinie inklusive Dokumentation, der finalen Installation von Softwaretools zur automatisierten Überwachung der Security-Richtlinie sowie der Zertifizierung durch eine neutrale Prüfinstanz gemäß IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI). Zum Leistungsumfang gehören zudem eine permanente Betriebsüberwachung und Betreuung. Diese erfolgt durch einen gemeinsamen Remote-Zugriff, Ticketrouting, falls die installierte Überwachungssoftware Probleme meldet, die Bereitstellung einer dedizierten Hotline von Experten, ein toolgestütztes, quartalsweises Reporting und Update-Management sowie eine permanente Dokumentation.

Das Modell bietet Unternehmen und Behörden verschiedene Vorteile. So werden etwa keine eigenen Fachressourcen benötigt, und Maßnahmen können unmittelbar umgesetzt werden, da sich die Projektvorlaufzeit durch die externe Unterstützung verringert. Zudem entfällt das Verwalten von Software-Lizenzen und die Investitionen in Softwaretools halten sich in Grenzen: Print Security as a Service wird monatlich entsprechend der tatsächlichen Geräteanzahl abgerechnet.

Ingrid Dypa ist Print Service Consultant, Carola Wolfgramm ist Head of Marketing bei der Firma druckerfachmann.de, Berlin.