Sicherheitslücke Drucker

Auch Großformatdrucker werden zur Zielscheibe

Da stehen Sie nun also vor dem Großformatdrucker und wollen Ihre Pläne abholen. Stattdessen steht auf der Anzeige eine kryptische Fehlermeldung und, zum Glück, gleich auch die Telefonnummer der Hotline. Der hilfsbereite Mitarbeiter dort kümmert sich um Ihr Problem.

Er fragt, um den Fehler nachvollziehen zu können, nach Ihrem Login und Ihrem Passwort, und ja, er sieht schon, wo das Problem liegt: „Einen Augenblick bitte, so, fertig!“ Und jetzt brauchen Sie nur noch den Drucker neu zu starten, und alles läuft wieder, Ihre Deadlines sind gesichert.

Der freundliche Service-Mitarbeiter kann sich jetzt auch über Ihre Anmeldedaten in das Firmennetzwerk einwählen.

Sicherheit beim Drucken? Ist doch kein Thema. Da waren sich jedenfalls rund vier Fünftel der befragten IT-Manager sicher. Dieselben IT-Manager, von denen 90 % überzeugt sind, dass PCs ein Si-

cherheitsrisiko darstellen. Und drei Viertel sehen für Mobilgeräte und Server die Gefahr eines nicht autorisierten Zugriffs.* Es ist dringend Zeit, das Risiko bei den Druckern zu überdenken.

Drucker sind heutzutage leistungsfähige Computer, deren Zweck es eben ist, zu drucken. Sie haben Prozessoren, sie haben eine Firmware, sie haben ein BIOS und sie haben eine Festplatte, auf der die Druckdaten gespeichert werden. All dies sind potenzielle Einfallstore für Hacker. Und damit nicht genug, denn wenn man sich der Sicherheit beim Drucken einigermaßen ernsthaft nähert, wird klar: Wir sprechen eigentlich über drei Themenbereiche: den Drucker, die Daten und die gedruckten Dokumente.

1. Sicherer Drucker

Um den Drucker zu schützen, hat HP zahlreiche Technologien entwickelt, unter anderem HP SureStart und HP Whitelisting. Beide überwachen das „zentrale Nervensystem“ des Gerätes, die Firm-ware und das BIOS. Sollte die Software des Druckers feststellen, dass BIOS oder Firmware nicht vom Hersteller kommen, greifen sie entweder auf eine ältere Firmware zurück oder auf ein BIOS, das auf einem zweiten Chip im Drucker in-stalliert ist. So ist sichergestellt, dass von außen die beiden Systeme nicht manipuliert werden können.

2. Sichere Daten

Daten werden unter anderem durch die sich selbst verschlüsselnde Festplatte geschützt. Selbst wenn die Festplatte aus einem Drucker entwendet wird, hilft das einem „Hacker“ nicht viel, denn durch die Verschlüsselung ist sichergestellt, dass nur der zur Festplatte gehörige Drucker die Daten auslesen kann.

3. Sichere Dokumente

Und auch die Dokumente verdienen Beachtung, schließlich ist es angebracht, dass nur der „rechtmäßige Besitzer“ der gedruckten Seiten diese auch bekommt. So kann – im einfachsten Fall – eine PIN mit dem Druckauftrag mitgeschickt werden; der Drucker verlangt nach deren Eingabe am Bedienfeld und fängt erst dann mit dem Druck an. Eine höhere Sicherheit versprechen Lösungen, die Druckaufträge freigeben, wenn der Mitarbeiter beispielsweise seinen Firmenausweis an ein Lesegerät hält, das am Drucker angebracht ist.

Selbstverständlich beschränkt sich das Risiko nicht auf die Bürodrucker; auch Großformatdrucker sind ein potenzielles Einfallstor für Böswillige. HP DesignJets sind die sichersten Großformatdrucker auf dem Markt.

Partner First Platinum

Ihr Ansprechpartner
Hermann Hinsen
Vertrieb
T +49 228 9080-519
F +49 228 9080-710
hermann.hinsen@hug.de

* *Quelle: Umfrage unter 107 IT-Verantwortlichen in Firmen mit mehr als 250 Mitarbeitern in Nordamerika, Europa, dem Mittleren Osten, Afrika, der Asien-Pazifik-Region und China, im Auftrag von HP durchgeführt von Spiceworks, Januar 2015.*