Lauschangriffe auf Drucker verhindern

Datenschleuder Netzwerkdrucker

Achten Sie auf versteckte Details! Ein Beispiel für möglichen Missbrauch sind schlichte, für alle Mitarbeiter zugängliche vertrauliche Ausdrucke. Aber auch unverschlüsselte Datenströme für Netzwerkdrucker bieten sich an. Wir zeigen, welche aktuelle Technik Ihr Unternehmen vor ungebetenen Mitlesern und -lauschern schützt.

Trotz vernetzter Systeme, weltweit agierender Anwendungen, Customer-Relationship-Management-Systeme und E-Mail ist das papierlose Büro weiterhin Fiktion. Millionenfach wird täglich ausgedruckt, das meiste davon in Büros oder auf den Gängen und auf netzwerkfähigen Laserdruckern.

Um die Gefahren der E-Mail-Kommunikation zu umgehen, läuft manches nur auf Papierausdrucken

In einigen Unternehmen sind manche Daten sogar so vertraulich, dass sie ausschließlich gedruckt und nicht etwa per E-Mail weitergegeben werden. Die Gefahren im Mailverkehr sind inzwischen hinlänglich bekannt – und der Feind könnte mithören.

Der Umgang mit „internen“, „vertraulichen“ oder als „streng vertraulich“ gekennzeichneten Dokumenten ist praxiserprobt und üblicherweise in entsprechenden Richtlinien im Unternehmen auf Papier veröffentlicht.

Doch auch Papier ist verräterisch, z.B. der Ausdruck aus der Personalabteilung auf einem zentralen Drucker

Netzwerkfähige Schwarz-Weiß- oder besser Farblaserdrucker sind inzwischen in jedem Unternehmen zu finden. Möglichst zentral aufgestellt, aus jeder Abteilung schnell zu erreichen – optimal vor dem Kaffeeautomaten – bieten sie enorme Druckleistung mit bester Ausgabequalität.

Sofern es sich lediglich um normalen Output wie Korrespondenz oder unkritische Firmeninterna handelt, stellt es kein Problem dar, wenn der Druckauftrag noch einige Zeit in der Ausgabe liegen bleibt, bis der Besitzer ihn bei der nächsten Kaffeepause abholt.

Aber wie sieht es aus bei sensiblen Druckaufträgen, z.B. Urlaubslisten, Reisekostenabrechnungen oder Informationen mit personenbezogenen Inhalten? Bis der Mitarbeiter von der Personalabteilung zum Drucker eilt, hat unter Umständen schon jemand anderer ohne böse Absicht im Vorbeigehen den Papierstapel kontrolliert – es könnte ja etwas aus seiner Abteilung dabei sein.

Eine – unpraktische – Lösung ist das Wachestehen beim Netzwerkdrucker

Alternativ müsste ein Kollege aus der Personalabteilung am Netzwerkprinter stehen, um den Druckjob bei der Ausgabe abzupassen und somit vor neugierigen Blicken zu schützen.

Die „Print-and-Hold“-Funktion ermöglicht auch vertrauliche Ausdrucke

Komfortabler und wesentlich sicherer ist ein PIN-gesicherter „Confidential Print“ (vertraulicher Druck).

Bereits beim Druckauftrag gibt der Anwender über die so genannte „Print-and-Hold“-Funktion seinen persönlichen PIN-Code für den Druckjob ein.

Authentifizierung mit PIN und Loginname direkt am Gerät

Der Druckauftrag wird auf dem Netzwerkdrucker gespeichert und bereitgestellt, jedoch nicht ausgedruckt. Erst durch die Identifizierung mit Loginname und PIN-Code an der Bedienkonsole des Geräts werden die gewünschten Seiten zum Output freigegeben.

Der Druckauftraggeber steht somit unmittelbar vor dem Ausgabefach und kann seine Ausdrucke sofort entgegennehmen. Bei sensiblen Dokumenten eine optimale Lösung!

Schließen Sie mit verschlüsselten drahtlosen Druckströmen weitere Sicherheitslücken

Die „Print-and-Hold“-Funktion schützt zwar vor neugierigen Blicken und kann organisatorische Mängel beseitigen. Der TCP/IP-Datenstrom des Druck-

Sind Sie sicher, dass Ihr Ausdruck wirklich nur auf Ihrem Tisch landet?

auftrags im Unternehmensnetz ist jedoch weiterhin unverschlüsselt.

Eine sichere Art, Daten vom PC zum Drucker zu senden, ist eine verschlüsselte WPA- bzw. WLAN-Verbindung. Profis, die ganz sicher gehen wollen, greifen sogar zu einer SSL-Lösung.

Kostengünstige Nachrüstung möglich

Die vergleichsweise günstige Nachrüstung besteht aus einer WLAN-Karte für den Client und einem WLAN-Printserver. Selbst günstige WLAN-Printserver können inzwischen verschlüsselte WPA-Druckdaten empfangen und leiten sie decodiert per USB-Kabel an die angeschlossenen Drucker.

In Unternehmen mit besonders sicherheitsrelevanten Daten empfiehlt sich zudem eine Verschlüsselung via SSL mit einer Client-Authentifizierung per Zertifikat. Entsprechende Lösungen mit Druckmanagementsoftware finden Sie z.B. bei SEH *(www.seh.de)*.

Eine weitere Lösung bietet die Verschlüsselung nach AES

Eine andere, jedoch aufwändigere Methode bietet IBM mit einer Verschlüsselungslösung nach Advanced Encryption Standard (AES) für die Druckausgabedaten. Die gesicherte Übertragung über ein TCP/IP-Netzwerk an den Drucker wird durch entsprechende Hardwarekomponenten garantiert.

Neben einer Entschlüsselungskarte in den Endgeräten muss die IT-Abteilung auf den Clients bzw. Workstations eine passende Verschlüsselungssoftware installieren.

Verschlüsselte Daten garantieren Ausgabesicherheit auf mehreren Ebenen

Verschlüsselte Ausgabedaten können nicht über einen ungesicherten oder falschen Drucker ausgegeben werden. Unverschlüsselte Daten werden hingegen wie gewohnt gedruckt.

Besser kein Kabelsalat – Datenströme zwischen Rechner und Drucker sind am sichersten, wenn sie kabellos und verschlüsselt versendet werden.

- Die Verschlüsselungslösung ist so konzipiert, dass verschlüsselte Daten nur dann gedruckt werden, wenn eine Entschlüsselungskarte auf dem Drucker installiert ist.
- Wenn zudem ein eindeutiger, persistenter Schlüssel (Algorithmus) verwendet wird, gibt die Verschlüsselungslösung keine Daten über einen anderen Drucker aus, selbst dann nicht, wenn dieser über eine Entschlüsselungskarte verfügt.

Diese Maßnahmen müssen auch vor internen Lauschern schützen

Die Datenschnüffler in den eigenen Reihen machen inzwischen nicht einmal mehr vor vermeintlich harmlosen Druckdaten halt. Mit einfachen Mitteln fangen sie den Druckjob zwischen Rechner und Netzwerkdrucker ab.

Lauschangriffe auf die Datenströme lassen sich mit legalen Netzwerkanalysatoren starten

Für das Mitschneiden des unverschlüsselten Datenstroms dienen weithin bekannte und völlig legale Netzwerkanalysatoren. Wegen ihrer wirkungsvollen Funktionen auf Freeware-Basis werden die Tools von Millionen Netzwerkadministratoren zur Fehlersuche im lokalen Netzwerk eingesetzt.

Nachdem die Suche nach Druckjobs mit dem entsprechendem Netzanalysator erfolgreich verlaufen ist, ist es einfach, mit weiteren Programmen aus der Freeware-Ecke aus dem TCP/IP-Datenwust ein erneutes Druckerfile zu erzeugen.

Anleitungen und Beispiele für den genauen Ablauf und die zu verwendenden Programme gibt es inzwischen in jeder Computer-Fachzeitschrift.

Analysieren Sie die Druckabläufe, um den Absicherungsbedarf zu ermitteln

Haben Sie eine interne Verfahrensübersicht zur Verfügung und die Abläufe genau analysiert, sollte Ihnen die Beurteilung, in welchen Fällen eine Absicherung der Druckdaten notwendig ist, nicht sonderlich schwer fallen.

Hermann Keck

Herrmann Keck ist externer Datenschutzbeauftragter (www.keck-dsb.de).

Kleines IT-Glossar

Persistenter Schlüssel (hier vereinfacht): Der verwendete Schlüssel wird mit charakteristischen Merkmalen des Druckers abgeglichen. Erst dann erfolgt die Druckfreigabe.

SSL – Secure Socket Layer: Ein von Netscape entwickeltes Sicherheitsprotokoll, das die Datenkommunikation über das Internet schützen soll.

WLAN – Wireless LAN: Allgemein für vollständig oder teilweise drahtlos aufgebautes LAN-System (Local Area Network), das anstelle eines Kabels elektromagnetische oder optische Funkübertragungen einsetzt.

WPA – WiFi protected architecture: Verschlüsselungsmethode für ein Wireless LAN.

Weitere Fachbegriffe finden Sie leicht verständlich auch für „Nicht-ITler“ erklärt im Lexikon „IT von A – Z“ *(www.interest.de/produkte/8180.html)*.