Drucken – mit Sicherheit!

Vertrauliche Informationen umfassend schützen

Aktuelle Studien belegen, dass Angriffe auf die IT von Unternehmen in Deutschland und weltweit steigen und immer komplexere Formen annehmen. Vertrauliche Daten sind somit einer ständigen Gefahr ausgesetzt. Um sie zu schützen, muss die IT-Sicherheit von Unternehmen insgesamt betrachtet werden. Drucker und Multi-funktionssysteme (MFPs) als potenzielle Sicherheitslücken in der Unternehmens-IT dürfen hierbei nicht vernachlässigt werden.

Laut der aktuellen IDC-Studie „Vor dem Sturm: IT-Security in Deutschland 2013“, in der 305 deutsche Unternehmen mit mehr als 1.000 Mitarbeitern befragt wurden, zielen IT-Angriffe hauptsächlich auf Datendiebstahl, das Unterbrechen bzw. Stören von Betriebsabläufen in den IT-Systemen oder in Produktionssystemen, auf Imageschäden und auf den Missbrauch der unternehmenseigenen IT-Systeme für kriminelle Zwecke ab. Im schlimmsten Fall kann das für die betroffenen Unternehmen das Einstellen der Geschäftstätigkeit zur Folge haben. Dennoch wird diese Gefahr von vielen Unternehmen immer noch unterschätzt. Das Analysezentrum von InfoWatch weist zudem in seiner jährlichen Studie über weltweite Vorfälle von Datenverlusten, die 2012 in den Medien veröffentlicht wurden, auf, dass der Verlust von Daten über Papierdokumente 22,3 Prozent betrug.

„Wenn es darum geht, vertrauliche Daten im Unternehmen oder im autorisierten Personenkreis zu halten, dürfen Drucker und Multifunktionssysteme in keinem Fall unberücksichtigt bleiben“, erklärt Helge Dolgener, Team Manager Office Products bei Konica Minolta Business Solutions Deutschland. „Nicht selten bilden sie einen der letzten Schwachpunkte in einem ansonsten hoch entwickelten Sicherheitssystem. Doch die besten Vorkehrungen in Teilbereichen helfen nichts, wenn anderswo Daten offen zugänglich sind.“

Drucksysteme als Sicherheitsrisiko berücksichtigen

Die meisten Unternehmen haben bereits umfangreiche Sicherheitsvorkehrungen im Hinblick auf die Netzwerksicherheit realisiert. So ist der Zugang auf autorisierte Nutzer beschränkt, Firewalls und Antivirensoftware schützen vor Gefahr von außen und Dateiserver sind mit Verschlüsselungsmechanismen gegen Datenraub und unbefugte Einsichtnahme gesichert. Drucksysteme bleiben in Sicherheitskonzepten jedoch häufig unberücksichtigt oder werden nur am Rande erwähnt.

Dabei sind moderne MFPs ebenso integraler Bestandteil des Firmennetzwerks wie jeder Fileserver – und ihre interne Festplatte kann Zugriff auf nicht weniger brisante Inhalte bieten. Schon längst sind Multifunktionssysteme keine passiven Peripheriegeräte mehr, sondern zentrale Schnittstellen in der Unternehmens-kommunikation. Über Funktionen zum Drucken oder Kopieren hinaus können sie beispielsweise auch E-Mails und Fax-nachrichten senden und empfangen. Mit nur wenigen Handgriffen lassen sich gescannte Daten weiterleiten – auch an unberechtigte Adressaten innerhalb und außerhalb des Unternehmens.

„Obwohl mit dem Funktionsumfang und der immer stärkeren Integration der Systeme in die Arbeitsabläufe nicht nur Effizienz und Geschwindigkeit der Prozesse erheblich ansteigen, sondern auch das Missbrauchspotenzial, fehlt vielfach das Bewusstsein, dass Benutzer und Administratoren unfreiwillig selbst zum Sicherheitsrisiko werden. Hier sehen wir uns als Druckerhersteller in der Pflicht, weiterhin verstärkt Aufklärungsarbeit zu leisten“, ergänzt Dolgener.

Sicherheitsgefahr Nummer eins: Das Ausgabefach

Bereits an der offensichtlichsten Stelle – dem Ausgabefach von Abteilungs- und Arbeitsgruppendruckern – müssen Sicherheitsvorkehrungen ansetzen. Häufig werden Ausdrucke nicht sofort abgeholt oder sogar vergessen. Um in solchen Fällen wichtige Dokumente vor dem Zugriff Unbefugter zu schützen, sollte eine Funktion für vertrauliches Drucken genutzt werden. Die Ausgabe des Druckjobs erfolgt hierbei erst, nachdem sich der Benutzer am System angemeldet hat – so lange bleiben die Druckjobs in der Warteschlange. Dabei kann die Authentifizierung beispielsweise per Passworteingabe, kontaktloser IC-Karte oder mittels biometrischer Daten anhand eines Fingervenenscans erfolgen.

Sichere Netzwerkeinbindung

Die unkomplizierte Einbindung von Druckern und MFPs in bestehende Sicherheitsarchitekturen ist vor allem in größeren Unternehmen besonders wichtig. So lässt sich der administrative Aufwand erheblich reduzieren, da die Benutzerdaten und -rechte nicht mehr für jedes System einzeln angelegt werden müssen. Die

Verwaltung erfolgt dann zentral, etwa über die Active Directory bei Windows-Servern. Anwender profitieren hiervon, indem sie beispielsweise mit demselben Passwort oder mit der gleichen Chipkarte Zugang zu allen Diensten des Unternehmens erhalten.

Ein weit verbreitetes Authentifizierungssystem, das MFPs unterstützen sollten, ist etwa der Standard IEEE 802.1x. Hierbei müssen sich alle Clients, die Zugang zum Netzwerk erhalten wollen, zuerst via Radius-Server authentifizieren. Dies ist vor allem in Unternehmen mit viel Publikumsverkehr sinnvoll, da so verhindert wird, dass sich Besucher mit mobilen Endgeräten über WLAN oder freie Netzwerkbuchsen unberechtigt in den Datenverkehr einklinken.

Doch auch wenn nur berechtigte Nutzer an die Ausgabesysteme gelangen, bleibt eine Sicherheitslücke bestehen: Mit entsprechenden Softwaretools können diese untereinander Daten abgreifen, wie zum Beispiel Druckjobs umleiten, manipulieren oder mitlesen. Dem beugt zum Beispiel Kerberos, der ticketbasierte Authentifizierungsdienst, vor und unterbindet Eingriffe von Dritten. Mit dem Sicherheitsprotokoll IPsec lässt sich zudem der gesamte Datenverkehr zwischen Arbeitsplatzrechner und Drucksystem verschlüsseln. IPsec sollte bei neuen Systemen daher ein fester Bestandteil sein.

Sicherheit für die E-Mail- und Faxkommunikation

Damit Informationen vom Multifunktionssystem aus nicht beliebig per E-Mail weitergeleitet werden können, sollte die manuelle Eingabe von Zieladressen am Multifunktionssystem blockierbar sein. Mit Aktivierung dieser Funktion lassen sich Nachrichten nur an die im internen Adressbuch angelegten Empfänger senden. Die

Auswahl autorisierter Adressaten kann auch über die lokale E-Maildatenbank per LDAP-Suche erfolgen. Für ein maximales Sicherheitsniveau sollte zudem S/MIME unterstützt werden. Hiermit lässt sich der Inhalt einzelner vom MFP aus gesendeter E-Mails verschlüsseln. So kann eine Nachricht vom Empfänger nur dann geöffnet werden, wenn dieser über den entsprechenden Dekodierungsschlüssel verfügt. Um einen sicheren Datenaustausch mit dem Mailserver zu gewährleisten, sollte neben den Standardprotokollen auch ESMTP und APOP unterstützt werden.

Der Administrator kann die Verfügbarkeit dieser Funktion auf spezifische Nutzer einschränken, um Sicherheitslücken in der Faxkommunikation zu schließen.
Im Rahmen des Faxverkehrs sollte auch ausschließlich das Faxprotokoll genutzt werden. Bei dem Versuch, ein anderes Protokoll zu nutzen oder Daten zu senden, die nicht als Faxdaten dekomprimiert werden können, müssen sichere Systeme Fehlermeldungen abgeben und die Datenübertragung verhindern. Somit ist ein Einbruch von außen mit Hilfe von anderen Protokollen über die Faxleitung ausgeschlossen.

Schutz des internen Datenträgers

Auch nach der formalen Löschung können Daten auf der Festplatte der MFPs noch lange erhalten bleiben, wenn sie nicht überschrieben werden. Dies ist vor allem dann problematisch, wenn die Systeme den Standort wechseln – etwa in andere Firmen oder Abteilungen – oder entsorgt werden sollen. Eine endgültige und zuverlässige Beseitigung der Daten stellt die bis zu 7-fache Überschreibung nach VSITR-Standard sicher. Zusätzlich können

bei Inaktivität des Systems nicht genutzte Speicherbereiche der Festplatte mit Zufallsdaten überschrieben werden, um keine verwertbaren Daten zurück zu lassen.
Auch für den Fall, dass die interne Festplatte entwendet wird, sollte vorgesorgt werden. Aktuelle Systeme sollten bereits im Standard über eine bis zu 256 Bit Datenverschlüsselung der Festplatte verfügen. So lassen sich die Daten außerhalb des MFPs nicht mehr verwerten.

Knappe Budgets sind kein Argument

Laut der aktuellen Studie von EY (vormals Ernst & Young) stellen mangelnde finanzielle Mittel derzeit immer noch ein Hindernis auf dem Weg zu einer verbesserten IT-Sicherheit dar. Die Unternehmen haben weiterhin Mühe, den steigenden Sicherheitsbedrohungen adäquat zu begegnen. Konica Minolta bietet in diesem Dilemma eine klare Lösung: „Für uns steht der Schutz von Kundendaten im Vordergrund, daher ist unser fester Standpunkt, dass unsere Kunden nicht für Sicherheitsfunktionen bezahlen sollen“, führt Helge Dolgener aus. „Die allermeisten dieser Funktionen sind somit in der neuesten Generation der bizhub-Reihe bereits standardmäßig integriert. Viele davon, wie etwa die Festplattenverschlüsselung, sind bei anderen Fabrikaten nur gegen Aufpreis verfügbar.“ Kostendruck muss also – zumindest im Druckerbereich – kein Grund dafür sein, die IT-Sicherheit zu vernachlässigen.

Zusätzliche Sicherheit

Mit der neuen Dienstleistung bizhub SECURE leistet das Unternehmen einen weiteren Beitrag zur Sicherheit. Basierend auf

den speziellen Kundenbedürfnissen konfiguriert Konica Minolta diverse Sicherheitsmerkmale des Multifunktionssystems vor, um Daten, Dokumente und Informationen sicher zu halten. Der besondere Schutz der so vorkonfigurierten Systeme wurde durch die Syss GmbH, einem erfahrenen Dienstleister im Bereich der IT-Security, in einem zweiwöchigen Penetrationstest bestätigt. Auch Kunden erhalten mit dem bizhub SECURE-Zertifikat eine offizielle Bestätigung über die zusätzliche Sicherheit ihres MFPs.