IT IM SICHERHEITSCHECK:
WIE GUT IST IHR UNTERNEHMEN GERÜSTET?

Neumaier

ALLES FÜRS BÜRO

INHALTSVERZEICHNIS

DAS BEDROHUNGSSZENARIO

Seit Jahren steht bei deutschen Unternehmen eine Erhöhung der IT-Sicherheit auf der Agenda. Längst ist klar, dass im Zentrum der Cyberkriminalität nicht mehr einzelne Hacktivisten in stickigen Kellern, sondern gut organisierte und arbeitsteilig vorgehende kriminelle Vereinigungen mit einer hervorragenden Infrastruktur stecken.

Doch nicht nur die Methoden der Angreifer haben sich verbessert, sondern auch deren Angriffswege sind vielseitiger geworden und lassen sich schwerer eindämmen.

Einen fruchtbaren Nährboden für Kriminelle bieten beispielsweise schon simple MFP (Multifunction Printer) bzw. Multifunktionsgeräte. Multifunktionsdrucker, die über eine Festplatte verfügen – was bei der überwiegenden Mehrzahl moderner Geräte der Fall ist –, speichern tausende kopierter Daten, die mit einfachsten technischen Mitteln von Dritten ausgelesen werden können. Ein sicherheitstechnisches Pulverfass, dessen explosive Bedeutung noch längst nicht jedem Unternehmen ins Bewusstsein gerückt ist.

Datensicherheit bei MFP: die Achillesferse der IT-Sicherheit?

Über die immense Bedeutung, die ungesicherten MFP mit Festplatte im Kontext der IT-Sicherheit zukommt, hat unlängst das Magazin plusminus berichtet. Der Clou: Moderne Multifunktionsdrucker verfügen oftmals über eine Festplatte, auf der die Daten sämtlicher Kopien gespeichert werden. Werden diese nicht konsequent gesichert bzw. vor dem Verkauf/Ausrangieren des Geräts vollständig gelöscht, ist es für kriminelle Dritte ein Leichtes, entsprechende Daten auszulesen. Mit einem einfachen Programm können auf diese Weise auch sehr empfindliche Daten von Anwaltskanzleien, Steuerberatern, Krankenhäusern, Behörden oder Versicherungen ausgelesen werden – ein GAU für jedes Unternehmen.

Das Erschreckende: Wie der Beitrag von plusminus offenbart, landen ausrangierte MFP mit empfindlichen Daten infolge mangelnder Kenntnisse oder zu laxer Sicherheitsbestimmungen mitunter sogar als Gebrauchtgeräte bei eBay, wo sie von jedem x-beliebigen Bieter ersteigert – und letztlich auch missbraucht – werden können.

Welche Handlungsmöglichkeiten Unternehmen speziell im Bereich der Datensicherheit bei MFP mit Fest-

platte haben, soll später in diesem E-Book beleuchtet werden (siehe Abschnitt 4.4, Datensicherheit von MFP mit Festplatte).

IT-Sicherheit: Wie hoch ist das Gefährdungspotenzial?

Zwar investieren deutsche Unternehmen verstärkt in die IT-Sicherheitsinfrastruktur, doch der Sicherheitsvorsprung gegenüber den Methoden der Cyberkriminellen ist gering, das Gefährdungspotenzial nach wie vor hoch. Das belegt eine Studie der techconsult GmbH. Hinzu kommt nicht selten die generelle Unwissenheit bezüglich mancher Sicherheitslecks, speziell was die Sicherheit von Multifunktionsgeräten mit Festplatte angeht. Auch von behördlicher Seite ist in diesem Zusammenhang wenig Hilfe zu erwarten. Zwar müsste durch Landesdatenschutzbeauftragte eine regelmäßige, stichprobenartige Kontrolle von Unternehmen mit Kopierern erfolgen, doch für eine ausreichende Kontrolle des Datenschutzes beim Kopieren sind die Kapazitäten der Behörden viel zu gering. So ist das Missverhältnis von Datenschutzmitarbeitern und Unternehmen so groß, dass ein Datenschützer theoretisch viele tausend Unternehmen kontrollieren müsste – eine Herkulesaufgabe, die schlicht nicht zu bewältigen ist. Wie so oft hinkt die Entwicklung des Datenschutzes auch in diesem Fall der digitalen Entwicklung meilenweit hinterher.

HACKERANGRIFFE, DATENKLAU UND CO.: WELCHE SPEZIFISCHEN BEDROHUNGEN BESTEHEN FÜR UNTERNEHMEN?

Angreifer sind in der Lage, sich auf vielfältige Weise Zugang zu Unternehmensdaten zu verschaffen oder Unternehmen auf andere Weise zu schaden.

Doch wie ist es um das Gefährdungsbewusstsein bei IT-Verantwortlichen und den eigenen Mitarbeitern bestellt? Welche Möglichkeiten gibt es, das Gefährdungspotenzial zu verringern?

Unternehmen im Kreuzfeuer: typische Angriffswege

Die Anfälligkeit für Angriffe hängt maßgeblich von den getroffenen Sicherheitsmaßnahmen ab. Prinzipiell ist es Cyberkriminellen durch die folgenden Methoden möglich, Unternehmen zu schaden:

- Spam: Spam-Mails sind nicht nur ärgerlich, sie stellen auch ein Sicherheitsrisiko dar, da sie in einigen Fällen genutzt werden, um Schadsoftware zu verbreiten. Moderne Spamfilter arbeiten mittlerweile glücklicherweise so gut, dass sich die Bedrohung durch Spam weitestgehend eindämmen lässt.

- Phishing-Attacken und Social Engineering: Wesentlich gefährlicher sind Versuche des Social Engineerings (etwa Phishing-Attacken). Im Rahmen des Social Engineerings versuchen Angreifer gezielt, Mitarbeiter zu täuschen. Gefälschte, angeblich von der Personalabteilung stammende E-Mails können beispielsweise dazu auffordern, empfindliche Daten preiszugeben. Auch die empfindlichen Daten, die sich auf MFP mit Festplatte befinden, können durchaus Ziel eines solches Social Engineerings sein.

- Trojaner, Viren und Co.: Trojaner, Viren und sonstige Schadprogramme können Unternehmensnetze ausspähen und sind in der Lage, erheblichen Schaden anzurichten. Besonders häufig sind in diesem Zusammenhang sogenannte Drive-by-Exploits, die beim Surfen im Netz Browser-Schwachstellen oder Sicherheitslücken des Betriebssystems ausnutzen, um Schadsoftware auf dem entsprechenden Gerät zu installieren.

- DoS-Angriffe: DoS-Angriffe (Denial-of-Service-Angriffe) bzw. DDoS-Attacken (Distributed-Denial-of-Service-Attacken) sind in der

Lage, Websites und Unternehmenssysteme komplett lahmzulegen, was enorme Kosten verursachen kann.

- Cyberangriffe durch Nachrichtendienste: Speziell ausländischen Nachrichtendiensten, die Wirtschaftsspionage betreiben, steht eine Vielzahl an Methoden (beispielsweise der Versuch einer umfassenden Abhörung der Unternehmenskommunikation) zur Verfügung.

Gefährdungsbewusstsein bei Mitarbeitern und IT-Verantwortlichen

Einer Studie der techconsult GmbH zufolge ist die aktuelle Sicherheitslage mittelständischer Unternehmen in den meisten Branchen nur als befriedigend bis ausreichend einzustufen. Zwar sehen sich die Unternehmen möglichen Angreifern zumindest einen Schritt voraus, das Sicherheitspolster ist aber denkbar gering. Zumindest teilweise scheinen Sicherheitsrisiken durch Vorstand und Geschäftsleitung noch immer unterschätzt zu werden. Gerade bei den eigenen Mitarbeitern lässt die Sensibilisierung für potenzielle IT-Sicherheitsrisiken noch zu wünschen übrig. Ein zu laxer Umgang beispielsweise mit auf dem Smartphone abgerufenen Daten stellt ein erhebliches Sicherheitsrisiko dar.

Gefährdungsbewusstsein bezüglich MFP mit Festplatte

Von besonderer Brisanz ist das mangelnde Gefährdungsbewusstsein bei Unternehmen, die empfindliche Daten kopieren. Ein nicht unbeträchtlicher Teil trifft nur unzureichende Vorkehrungen zum Schutz der Daten auf Multifunktionsgeräten mit Festplatte – oftmals infolge schlichter Unkenntnis des Gefahrenpotenzials.
Die Umfrage, die das Magazin plusminus hinsichtlich des Gefährdungsbewusstseins bei MFP mit Festplatte unter 200 Ärzten, Rechtsanwälten und Steuerberatern durchgeführt hat, fördert Erschreckendes zu Tage: Die Hälfte der Befragten weiß nicht, ob ihr Kopiergerät eine Festplatte besitzt und in der Lage ist, Daten zu speichern, während ein Viertel glaubt, ihr MFP besitzt überhaupt keine Festplatte. Lediglich ein Viertel der Befragten weiß über die Festplatte ihres MFP Bescheid und besitzt ein entsprechendes Gefahrenbewusstsein.

Lösungsansätze im Überblick

Zur Verringerung des Gefährdungspotenzials im IT-Bereich bedarf es umfassender Sicherheitskonzepte, die auch neue Technologien wie die Nutzung von Smartphones berücksichtigen. Eine allgemeine Verbesserung der Sicherheitslage lässt sich unter anderem durch die Umsetzung folgender Punkte erreichen.

- Patches und Aktualisierungen: Ständige Patches und Updates von Betriebssystem, Browsern, Antivirenprogrammen und Co. verringern die Gefahr, Opfer einer Attacke zu werden, die bestehende Sicherheitslücken in entsprechenden Programmen und Systemen ausnutzt.

- Multifaktor-Authentifizierung: Eine Erhöhung der Datensicherheit lässt sich durch eine Multifaktor-Authentifizierung erreichen, in deren Rahmen der Datenzugriff erst beim Zusammenkommen mehrerer Faktoren möglich ist. So kann neben einem klassischen Passwort das Smartphone des Anwenders zur Authentifizierung (via SMS, Anruf oder App) genutzt werden.

- Mitarbeiterschulung: Eine Sensibilisierung der Mitarbeiter für das Gefährdungspotenzial der IT-Sicherheit durch entsprechende Schulungen ist ein wichtiger Ansatz zur Verbesserung der IT-Sicherheit. Von Passwortsicherheit über die Nutzung ungesicherter Internetverbindungen bis hin zum Umgang mit Smartphones lässt sich das Bewusstsein der Mitarbeiter schärfen.

- Verschlüsselung: Schon die Nutzung einfacherer Verschlüsselungsprogramme in der Unternehmenskommunikation senkt das Sicherheitsrisiko signifikant.

- Druck- und Kopiersicherheit: Durch ausgereifte Tools (etwa das Data Security Kit von KYOCERA) kann die Sicherheit beim Drucken und Kopieren unkompliziert und nachhaltig erhöht werden.

IT-SICHERHEIT: IN DIESEN BEREICHEN SIND UNTERNEHMEN GUT GERÜSTET

Dank der zunehmenden Inanspruchnahme professioneller Security-Lösungen sind deutsche Unternehmen heute zumindest in einigen Bereichen vergleichsweise gut gerüstet.

Das betrifft beispielsweise den Schutz von empfindlichen Daten in Unternehmensnetzwerken sowie die – meist damit verbundene – Cloud-Security.

Datensicherheit: Bewusstsein geschärft wie nie

Der Umgang mit empfindlichen Daten hat sich im Zuge der NSA-Affäre sowie der zunehmenden Datensammelwut von Google, Facebook und Co., die zunehmend auch ins Bewusstsein der Kunden gerückt ist, deutlich gewandelt. So konnten Unternehmen – unter anderem dank Techniken wie der Multifaktor-Authentifizierung – ihre Datensicherheit erhöhen. Das Bewusstsein der Geschäftsführungen für die Notwendigkeit bestmöglicher Datensicherheitslösungen ist, nicht zuletzt infolge des finanziellen und imagetechnischen Gefahrenpotenzials, so geschärft wie nie. Schwachstelle bei vielen Unternehmen bleibt allerdings weiterhin die Mobile Device Security.

Cloud-Security

Lange Zeit war die Cloud – gerade bei IT-Verantwortlichen – als Sicherheitsrisiko verschrien. Die meisten

Anbieter professioneller Cloud-Lösungen (man denke beispielsweise an die für viele Unternehmen so essenziell gewordenen Microsoft-Cloud-Produkte von Office 365 über Exchange Online bis hin zu Skype for Business) verfügen mittlerweile allerdings über eine Sicherheitsinfrastruktur, die die Möglichkeiten mittelständischer Unternehmen bei weitem übersteigen. Die Folge: Die Nutzung entsprechender Cloud-Varianten ist mitunter sicherer als On-Premise-Lösungen. Zudem lässt sich die Cloud-Security durch gezielte Sicherheitsmaßnahmen weiter erhöhen:

- Notfallmanagement: In Abstimmung mit den Unternehmensanforderungen sollte mit dem jeweiligen Provider ein Notfallmanagement erarbeitet und getestet werden, das unter anderem ausgearbeitete Pläne der Datenwiederherstellung beinhaltet. Im Ernstfall steht und fällt der Grad der Cloud-Sicherheit mit der Zusammenarbeit von Unternehmen und Provider.

- Compliance und Rechteverteilung: Selbstverständlich sind beim Umgang mit Kundendaten in der Cloud sämtliche Compliance-Anforderungen einzuhalten. Es gilt sicherzustellen, dass der Personenkreis, der Zugriff auf empfindliche Daten hat, so eingeschränkt wie möglich bleibt, um die Gefahr von Sicherheitslücken möglichst gering zu halten – das gilt sowohl für die Unternehmens- als auch für die Kundenseite. Zugriffsrechte auf gemeinsam genutzte Daten in der Cloud gilt es stets in enger Zusammenarbeit mit dem Kunden zu erarbeiten und entsprechende Prozesse zu dokumentieren.

- Technische Innovationen nutzen: Die Nutzung neuster Technologien im Bereich Verschlüsselung und Authentifizierung ist gerade für Cloud-Lösungen unabdingbar.

Unternehmen, die auf State-of-the-Art-Technologien setzen und eng mit Provider und Kunden zusammenarbeiten, sind in der Lage, ein sehr hohes Maß der Cloud-Security zu erreichen. Ein gutes Zeichen, denn das Cloud-Computing ist unaufhaltsam auf dem Vormarsch und schon heute nicht mehr aus dem Unternehmensalltag wegzudenken.

HIER BESTEHT HANDLUNGSBEDARF: KRITISCHE BEREICHE DER IT-SICHERHEIT

Während einige Bereiche der IT-Security von den meisten Unternehmen bereits gut gemanagt werden, besteht in anderen Punkten noch akuter Handlungsbedarf.

Das betrifft neben der Mobile Device Security, der Verschlüsselung der Unternehmenskommunikation und der zum Teil noch immer unzureichenden Sensibilisierung der Angestellten auch die viel unterschätzte Sicherheit beim Drucken und die ungenügende Datensicherheit im Zusammenhang mit MFP mit Festplatte.

Sensibilisierung der Angestellten

Noch immer sind viele Angestellte nicht ausreichend für die Gefahren der IT-Sicherheit sensibilisiert. In regelmäßig stattfindenden Schulungsprogrammen gilt es, Mitarbeitern daher Risiken und entsprechende Maßnahmen zur Erhöhung der Sicherheit zu vermitteln. Das betrifft nicht nur das leidige Thema „Passwortsicherheit“, sondern bezieht sich insbesondere auch auf die Nutzung von Cloud-Diensten durch private Mobilgeräte.

Mobile Device Security

Die Verbreitung der Cloud lässt auch die Nutzung von mobilen Endgeräten immer selbstverständlicher werden. Entsprechend ist die Mobile Device Security sehr rasch zu einem kritischen Sicherheitsaspekt geworden, den noch längst nicht alle Unternehmen zufriedenstellend gelöst haben. Mobile Endgeräte müssen nicht nur in bestehende Sicherheitskonzepte eingebaut werden, auch der Trend zu „Bring Your Own Device“ („Bring dein eigenes Gerät“) muss im Rahmen des Mobile Device Managements (MDM) berücksichtigt werden. Wie können die privaten Geräte von Mitarbeitern in die Sicherheitsarchitektur des Unternehmens integriert werden? Wie lassen sich Sicherheitslücken beim Verlust eines Mobilgeräts vermeiden?

Möglichkeiten des Sicherheitsmanagements

Unternehmen stehen im Rahmen der Mobile Device Security verschiedene Möglichkeiten zum Schutz von Daten zur Verfügung. Zu nennen sind etwa die folgenden:

- MDM-Programme: Moderne Mobile-Device-Management-Programme sind in der Lage, die privat genutzten Geräte der Mitarbeiter in die bestehende Sicherheitsarchitektur einzubauen. Eine zentrale Verwaltung der Mobilgeräte erlaubt beispielsweise die Einrichtung von Webfiltern und granularen Kontrollen, die die normale private Nutzung (Surfen im Web, Nutzung von Facebook, Download von Apps) weitestgehend unberührt lässt, bestimmte, potenziell schädli-

che Interaktionen der Nutzer mit Programmen jedoch unterbindet. Entsprechende Richtlinien können von Unternehmen mittels MDM-Programmen individuell erstellt und umgesetzt werden.

- Container-Lösungen: Sogenannte Container-Lösungen erlauben die Einrichtung eines durch Verschlüsselungsprogramme abgeschotteten Bereichs innerhalb eines Mobilgeräts, der einzig zur geschäftlichen Nutzung bestimmt ist. Nutzer eines Smartphones können so jederzeit entscheiden, ob sie ihr Gerät privat oder geschäftlich nutzen wollen. Auf geschäftliche Inhalte und Applikationen innerhalb eines solchen Containers kann von der IT-Abteilung – etwa im Rahmen von MDM-Programmen – zugegriffen werden. Wird der Privatbereich eines solchen Mobilgeräts beispielsweise von Malware infiziert, bleibt der geschützte Geschäftsbereich unbeeinflusst. Beim Verlust des Mobilgeräts ist es möglich, empfindliche Daten innerhalb des Containers aus der Ferne zu löschen.

- Synchronisation: Damit der Verlust eines Mobilgeräts nicht mit einem Datenverlust einhergeht, sind regelmäßige Backups und Datensynchronisationen bei der Nutzung von Cloud-Lösungen von Vorteil.

- Biometrische Verfahren: Der Verlust eines Mobilgeräts mit empfindlichen Unternehmens- bzw. Kundendaten kann nicht ausgeschlossen werden. Es gilt daher, von vornherein sicherzustellen, dass entsprechende Daten nicht in die falschen Hände geraten können. Mobilgeräte können (und sollten) nicht nur durch einfache PINs, sondern durch weitere Faktoren geschützt werden. Immerhin rund 40 Prozent der deutschen Unternehmen sichern laut einer Studie der IDC Central Europe GmbH die Smartphones ihrer Mitarbeiter daher bereits durch biometrische Verfahren der Authentifizierung (Fingerabdruck, Gesichtserkennung, Spracherkennung, Irisabgleich) ab.

Verschlüsselung von Kommunikation/ Daten

Eine Verschlüsselung der Unternehmenskommunikation, gerade bei vertraulichen Geschäfts-E-Mails, wird von vielen Unternehmen vorgeschrieben, konsequent umgesetzt wird sie damit jedoch noch lange nicht. Gerade die zunehmende Nutzung von Mobilgeräten und das damit verbundene Verschwimmen der Grenzen zwischen geschäftlich und privat haben mit dazu beigetragen, dass Kommunikation wieder verstärkt unverschlüsselt stattfindet. Ein Trend, dem durch Mitarbeiteraufklärung und die Implementation von Verschlüsselungstechniken unbedingt entgegengewirkt werden muss.

Welche Möglichkeiten der Verschlüsselung gibt es?

Es gibt vier Kommunikationsbereiche, für die eine Verschlüsselung naheliegt, um zu verhindern, dass Daten in die falschen Hände gelangen: E-Mail, Textnachrichten, Anrufe und Druckvorgänge.

- E-Mail-Verschlüsselung: Eine Verschlüsselung von E-Mails findet in der Regel durch eine digitale Signatur statt, die eine Manipulation durch Dritte auf dem Transportweg verhindern soll. En détail stehen hierfür je nach individuellen Unternehmensbedürfnissen verschiedene Möglichkeiten zur Verfügung – von der klassischen Ende-zu-Ende-Verschlüsselung (Client-zu-Client-Verschlüsselung) über eine serverbasierte Verschlüsselung, die sich speziell für Unternehmen anbietet, bis hin zur passwortbasierten Verschlüsselung.

- Textnachrichten: Zwischen Mitarbeitern versendete Textnachrichten lassen sich durch Apps wie TextSecure schnell und unkompliziert verschlüsseln.

- Anrufverschlüsselung: Auch eine Verschlüsselung der Sprachkommunikation ist dank entsprechender Programme heute weitestgehend unkompliziert möglich. Die App „Red Phone“ beispielsweise ermöglicht die Verschlüsselung von Anrufen. Sowohl TextSecure als auch Red Phone wurden von keinem Geringeren als dem Whistleblower Edward Snowden empfohlen.

- Verschlüsselung von Drucksendungen: Vielfach unterschätzt wird die Gefahr, die beim unverschlüsselten Versenden von Drucksendungen besteht. Glücklicherweise stehen Unternehmen auch hier eine Reihe von Verschlüsselungsmaßnahmen zur Verfügung.

Datensicherheit von MFP mit Festplatte

Darauf, dass die Datensicherheit von Multifunktionsgeräten mit Festplatte bei nicht wenigen Unternehmen noch in den Kinderschuhen steckt, haben wir bereits mehrfach hingewiesen. Für Unternehmen ist dies ein nicht tragbarer Zustand. Neben den beträchtlichen wirtschaftlichen Schäden, die Datendiebstahl durch den folgenden Imageverlust nach sich ziehen dürfte, besteht bei Geheimnisträgern wie Anwälten zudem die Gefahr rechtlicher Konsequenzen. Umso wichtiger ist es, kopierte Daten umfassend zu schützen.

Kopierte Daten schützen: Funktionen des Data Security Kits von Kyocera

Weitreichende Möglichkeiten, die Datensicherheit von Multifunktionsgeräten mit Festplatte zu erhöhen, bietet das Data Security Kit von KYOCERA. Das Sicherheitskonzept des Data Security Kits beruht dabei im Wesentlichen auf zwei Säulen:

1. Sicherheit während der Nutzung: Die HDD-Verschlüsselung mit 256-Bit-AES-Algorithmus sorgt für den Fall vor, dass die Festplatte eines MFP von unbefugten Dritten mit dem Ziel des Datenklaus entfernt wird. Empfindliche Daten können dank Verschlüsselung in diesem Fall nicht ausgelesen werden. Dank der Sicherheitsfunktion HDD-Überschreiben-Löschen werden Daten auf der Festplatte, die nicht mehr benötigt werden, zudem physikalisch überschrieben und sind somit nicht oder kaum noch für Dritte zugänglich. Ge-

wählt werden kann zwischen einem einmaligen oder einem noch sichereren dreimaligen Überschreiben.

2. Sicherheit nach der Nutzung: Wird die Festplatte eines MFP nicht mehr benötigt, müssen sämtliche darauf befindlichen Daten gelöscht werden, um Sicherheitslecks zu vermeiden. Die Funktion „System initialisieren“ des Data Security Kits ermöglicht es auch, die Daten endgültig zu löschen, die während der Nutzung nicht im Rahmen der Sicherheitsfunktion HDD-Überschreiben-Löschen gelöscht worden sind. Hierzu gehört auch das Löschen von Benutzern und Systeminformationen.

EXPERTENINTERVIEW ZUR IT-SICHERHEIT

Was meinen IT-Experten zur IT-Sicherheit in Unternehmen? Wir haben Marc Fliehe, Bereichsleiter für IT-Sicherheit bei Bitkom befragt.

Welche Anforderungen an die IT-Sicherheit gibt es speziell in Unternehmen, d. h., wo gehen diese über die Sicherheitsanforderungen an private Computersysteme hinaus?

IT-Systeme sind in den meisten Unternehmen heute notwendig, um den Geschäftsbetrieb zu gewährleisten. Bei Störungen oder Ausfällen kommt es schnell zu hohen finanziellen Verlusten. Daher braucht es zusätzliche Sicherheitsmaßnahmen, die über den üblichen Basisschutz mit Virenscannern und Firewalls hinausgehen. Der reicht heute nicht mehr aus. Daneben sind spezielle Angriffserkennungssysteme und Maßnahmen gegen Datenabfluss von innen notwendig. Weitere Themen sind Verschlüsselung oder erweiterte Zugriffskontrollen.

Welche Schwachstellen in der Sicherheitsarchitektur von Unternehmen fallen Ihnen am häufigsten auf?

Schwache Passwörter und alte Softwareversionen sind noch sehr weit verbreitet. Die größte Schwachstelle ist und bleibt aber der Mitarbeiter selbst. Hier ist wichtig, dass der Anwender von IT-Systemen die Risiken kennt und sich entsprechend sensibel verhält. Angreifer nutzen manchmal auch das Telefon oder die offene Tür im Hinterhof des Firmengebäudes, um sich unbefugten Zugriff auf die Unternehmensdaten zu verschaffen. Der unwissende Mitarbeiter wird dabei manchmal unfreiwillig zum Komplizen.

Haben Unternehmen seit der NSA-Affäre ein höheres Sicherheitsbewusstsein?

Das lässt sich zwar schwer messen, aber nach unserer Beobachtung hat sich das Sicherheitsbewusstsein tatsächlich erhöht. Dazu tragen aber auch die immer neuen Fälle schwerer Cyberattacken auf Unternehmen bei. Die Investitionen in IT-Sicherheit steigen jedenfalls kräftig an.

Welche einfachen Maßnahmen würden Sie Unternehmen und Privatleuten empfehlen, die sich vor wie auch immer motivierten unerwünschten Zugriffen auf ihr System (z. B. Wirtschaftsspionage) schützen möchten?

Privatleute sollten vor allem ihren Virenschutz und die Firewall auf dem neuesten Stand halten. Daneben können sie über Verschlüsselung von E-Mails und Dateien nachdenken, um ihre Daten besser zu schützen. Bei Unternehmen ist die Sache komplexer und hängt von vielen Faktoren wie Größe oder Branche ab. Am Anfang steht aber immer die Frage: Welche Daten in meinem Unternehmen sind besonders wertvoll? Danach kann man dann die Sicherheitsstrategie ausrichten.

SICHERHEIT BEIM DRUCKEN

Da viele sensible Dokumente auch gedruckt, gescannt oder kopiert werden, ist das Potenzial für Missbrauch entsprechend hoch. Prinzipiell sollten für den Prozess des Druckens die gleichen Sicherheitsstandards wie bei der Nutzung anderer Geräte gelten.

So gilt es, Passwörter für Netzwerkdrucker einzuführen, etwaige Sicherheitslücken durch schnelle Firmware-Updates zu schließen, die ausgedruckten Daten vor dem Zugriff durch unbefugte Dritte zu schützen und die Übermittlung der Druckaufträge zu verschlüsseln.

Sicherheitslücke Ausgabefach

Gerade das Ausgabefach stellt eine nicht zu unterschätzende Sicherheitslücke dar. Drucker und Multifunktionsgeräte werden nur in den seltensten Fällen von einer einzigen Person genutzt, vielmehr stehen die Geräte oftmals pro Abteilung oder Flur für alle zugänglich zur Nutzung bereit. Hierbei ist es egal, ob gerade ein vertrauliches Dokument oder der Speiseplan der Kantine gedruckt wird – jeder kann auf diese Dokumente im Ausgabefach zugreifen.

Was passiert also, wenn ein Druck gestartet wird, das Dokument sich aber nicht im Ausgabefach befindet, wenn man es abholen will? Kaum ein Mitarbeiter würde hier an die Möglichkeit des Datendiebstahls denken – hat nicht eher die Maschine mal wieder eine Macke, und der ganze Druckvorgang wird erneut gestartet? Oder aber ein eiliger Druckauftrag geht an einen Drucker, an dem bereits ein langwieriger Auftrag bearbeitet wird. Ein erneuter Auftrag wird an den gerade nicht beanspruchten Drucker der Nachbarabteilung gesendet – der Ursprungsauftrag wird vergessen, die Dokumente bleiben für alle zugänglich liegen. Je nachdem, um welche Dokumente es sich in diesen Szenarien gehandelt hat, können sich hier riesige Sicherheitslücken auftun; die so abhandengekommenen Dokumente können einem Unternehmen im schlimmsten Fall ernsthaften Schaden zufügen.

Die Lösung: authentifiziertes Drucken

Damit der Datendiebstahl aus dem Ausgabefach gar nicht erst zustande kommt, ist es sinnvoll, eine quasi personalisierte Form des Druckens einzuführen, die sogenannte Pull-Printing- oder Print-&-Follow-Lösung. Print & Follow erlaubt den Druck aus der Warteschlange des Servers erst dann, wenn sich der Mitarbeiter, der den Druckvorgang in Auftrag gegeben hat, am Ausgabegerät authentifiziert hat.

Die Freigabe erfolgt über eine PIN, ein Kennwort oder eine RFID-Card. So lassen sich Dokumente sicher und ausschließlich von autorisierten Personen ausgeben. Das funktioniert auf verschiedenen Druckern, zu beliebigen Zeiten und zusätzlich auch über mobile Geräte. Dokumente in der Warteschlange werden automatisch gelöscht, werden sie innerhalb einer bestimmten Zeit nicht abgearbeitet. Zudem lassen sich Sicherheitsroutinen einrichten, die überwachen und dokumentieren, wer wann was auf welchem Gerät gedruckt hat.

Erfolg spricht für sich – Beispiele für eingeführte Print-&-Follow-Konzepte

Das international erfolgreiche Modelabel BASLER FASHION führte für eine verbesserte Kostenkontrolle und eine zentrale administrative Überwachung der Druckerflotte die Print-&-Follow-Lösung SequiMe von Kyocera ein. Seither authentifizieren sich Mitarbeiter über ihren Dienstausweis zunächst am jeweiligen Endgerät, bevor sie den Druck-, Scan- oder Kopiervorgang auslösen können. Fehldrucke und im Ausgabefach vergessene Dokumente, die ein Sicherheitsrisiko darstellen, gehören somit der Vergangenheit an. Für die gleiche Lösung entschied sich auch der SC Freiburg, der dank SequiMe unnötige oder unbefugte Ausdrucke verhindert.

Auch die mit zahlreichen vertraulichen Daten arbeitende Versicherungsbranche setzt auf Print & Follow: So wurde bei der MÜNCHNER VEREIN Versicherung die Lösung SequiMe installiert. Auch hier folgt der Druckauftrag dem Anwender quasi, bis dieser sich an einem Multifunktionsgerät authentifiziert. Sollte das ursprünglich angesteuerte Gerät schon besetzt sein, kann man den Druck ganz einfach und ohne Mehraufwand von einem anderen, freien Gerät aus starten. Sensible Dokumente können so nicht mehr in die falschen Hände geraten.

Die EMG Automation GmbH entschied sich hingegen für den Einsatz der Softwarelösung KYOcontrol, ebenfalls aus dem Hause Kyocera. Auch hier werden die Druckaufträge zentral verwaltet und können nach Authentifizierung des jeweiligen Mitarbeiters bequem am verfügbaren System abgerufen werden. Gleiches gilt für die Sparkasse Hamm, die sich ebenfalls für KYOcontrol entschied, um die Dokumentensicherheit innerhalb des Hauses zu gewährleisten.

Verschlüsselung auch beim Drucken

Was für Mails und Telefonate gilt, sollte auch für Druckdaten gelten: Verschlüsselung. Denn moderne Druckersysteme mit CPU, Festplatte, Arbeitsspeicher und Netzwerkanbindung bieten ungeschützt eine große Angriffsfläche. Sensible Daten, die über ein Netzwerk an einen Drucker geschickt werden, sind ohne Schutz im Klartext sichtbar und somit manipulierbar bzw. können mit entsprechenden Tools mitgeschnitten werden. Dies kann mit einer Verschlüsselung über Protokolle wie Secure Sockets Layer (SSL) oder Internet Protocol Security (IPsec) verhindert werden. Der Zugriff während der Übertragung etwa über ungesicherte Schnittstellen lässt sich so wirkungsvoll vermeiden, ebenso wie das Nachdrucken von Dokumenten anhand von vorhandenen Joblisten, Netzwerkprotokollen oder Re-Printing-Funktionen.

Risiko mobiles Drucken

Dank der zunehmenden Nutzung von Cloud-Services und dem Datenzugriff auch von unterwegs aus wird auch

das Drucken immer mobiler. Mitarbeiter drucken von unterwegs oder von externen Standorten über Geräte außerhalb ihrer Abteilung. Informationen sollen dabei über jedes beliebige Gerät innerhalb eines Unternehmens bzw. an verschiedenen Unternehmensstandorten auf möglichst sichere Weise abrufbar sein. Das Drucken über Tablet oder Smartphone wird immer beliebter und immer häufiger eingefordert. Datensicherheit muss also nicht nur in der Cloud, sondern auch auf den genutzten Endgeräten und besonders auf den Druckern gewährleistet sein.

Gefährlich wird es, wenn Multifunktionssysteme jetzt eine offene und damit ungeschützte Schnittstelle außerhalb des Firmennetzwerks haben. Mittels Near Field Communication (NFC) kann man sich über Smartphones an den Geräten authentifizieren und so Druckaufträge starten – wichtig ist jetzt, dass die verschiedenen Mobilgeräte von den entsprechenden Druckern nicht nur identifiziert werden, sondern ihnen gleichzeitig auch die zum betreffenden Mitarbeiter gehörigen Rechte und Unternehmensrichtlinien zugewiesen werden. Nur so lassen sich die Gefahren, die durch eine Nutzung der Drucker über das Unternehmensnetzwerk hinaus entstehen können, wirkungsvoll abwenden.

Sensibilisierung im Druckbereich

Die Sensibilisierung der Mitarbeiter in Bezug auf Sicherheitslücken und Fragen der Datensicherheit sollte in allen Unternehmen vorangetrieben werden. Gerade im Bereich „Drucker“ gilt es aber, besondere Sorgfalt walten zu lassen. 87 Prozent der Befragten in einer Studie der Bitkom zum Thema Datenschutz gaben an, eher pragmatisch mit diesem Thema umzugehen. Aus Gründen der Bequemlichkeit wird oftmals auf Sicherheitsbedenken verzichtet. Wer aus Gründen der Bequemlichkeit schon bei den klassischen Bedrohungsszenarien für PC, Smartphone und Co. Sicherheitsbedenken über Bord wirft, wird dem eher unbekannten Risiko „Drucker“ wohl noch eine Spur gleichgültiger gegenüberstehen. Die Wichtigkeit des Themas Sensibilisierung wird auch durch die Umfrage zum 16. Datenschutzkongress in Berlin bestätigt: 84 Prozent der Befragten gaben an, Aufklärung im Bereich Datensicherheit sei die wichtigste Maßnahme, die in Zukunft umgesetzt werden müsse.

Lösungen für sicheres Drucken und Kopieren von Kyocera im Überblick

Kyocera stellt Unternehmen eine Vielzahl an kosteneffizienten Lösungen für sicheres Drucken und Kopieren zur Verfügung. Das Produktportfolio umfasst unter anderen die folgenden Lösungen:

- KYOcontrol: KYOcontrol ermöglicht dank zentraler Verwaltung und der Definition individueller Druckregeln eine optimale Prozesseffizienz und Kostenkontrolle. Die Sicherheit wird durch einen authentifizierten Dokumentenabruf gewährleistet.

- SequiMe und SequiMe Access: SequiMe sorgt für eine hohe Datensicherheit, indem jedem Druckvorgang eine Identitäts- bzw. Berechtigungsüberprüfung vorangestellt wird. Über SequiMe Access können des Weiteren Zugangsberechtigungen gesetzt und die Drucksicherheit weiter erhöht werden. Die Lösungen eignen sich ideal für kleine und mittelständische Unternehmen.

- KYOCERA – Data Security Kit: Mit dem Data Security Kit lassen sich Dokumente von Drucker-

oder MFP-Festplatten löschen und so vor unbefugtem Zugriff schützen.

- Drivve Print: Drivve Print sorgt dank Anwenderauthentifizierung auch beim Drucken von verschiedenen Mobilgeräten in der privaten Cloud für die notwendige Sicherheit.

Weitere Informationen und Produkte zur Erhöhung Ihrer Drucksicherheit finden Sie auf der Website www.kyoceradocumentsolutions.de unter der Kategorie „Cost Control & Security“.

FAZIT

Die richtige Balance aus Sicherheitsstandards und Produktivität muss jedes Unternehmen selbst finden. Eine 100-prozentige IT-Sicherheit kann unmöglich erreicht werden.

Wer auf ausgereifte, integrative Sicherheitskonzepte, die auch neueste Entwicklungen wie die zunehmende Nutzung privater Mobilgeräte für Geschäftszwecke berücksichtigen, und State-of-the-Art-Technologien setzt, kann jedoch eine hohe IT-Sicherheit erreichen, ohne dass dies zu Lasten der eigenen Wirtschaftlichkeit geht. Insbesondere im Bereich Druck- und Kopiersicherheit haben Unternehmen hier Nachholbedarf.

Ein Blick in die Zukunft

Auch in naher Zukunft dürfte sich nichts an der drohenden Gefahr durch Sicherheitslücken in der IT ändern. Der Trend zur Digitalisierung setzt sich weiter fort. Die Allgegenwart von zugänglichen Daten – etwa durch die zunehmende Verbreitung von Cloud-Diensten – wird ebenso umfassender wie die Komplexität und Vernetzung sämtlicher Lebensbereiche durch neue Technologien. Das „Internet of Things“ – Smartphones, Smartwatches und vernetzte Autos sind hier nur die Spitze des Eisbergs – bietet Unternehmen in puncto Produktivität zunehmend neue Möglichkeiten, stellt aber die IT-Sicherheit kontinuierlich vor neue Herausforderungen. Ausgereifte Sicherheitskonzepte sind daher auch zukünftig unabdingbar. Entsprechende Investitionen in die IT-Sicherheit zahlen sich heute wie morgen aus.

Über KYOCERA Document Solutions Deutschland GmbH

KYOCERA Document Solutions ist ein weltweit führender Anbieter von Lösungen und Dienstleistungen im Bereich Dokumentenmanagement. Die Produktpalette umfasst neben ressourcenschonenden Druckern und Multifunktionssystemen auch Verbrauchsmaterialien sowie Solutions und Services. Gemeinsam mit seinen Fachhandelspartnern unterstützt KYOCERA Document Solutions Unternehmenskunden dabei, Dokumentenprozesse effizienter und kostengünstiger zu gestalten. Dazu setzt das Unternehmen auf eine sorgfältige Analyse der vorhandenen Dokumenteninfrastruktur und erarbeitet dann – gemeinsam mit regionalen und kompetenten Fachhandelspartnern – ein Optimierungskonzept. Eine Aufgabe, die angesichts der Digitalisierung unserer Arbeitswelt immer wichtiger wird. Dazu engagiert sich das Unternehmen unter anderem im vom Fraunhofer-Institut für Arbeitswirtschaft und Organisation (IAO) initiierten Verbundforschungsprojekt OFFICE 21. Ziel dieses Projekts ist es, die Herausforderungen einer sich verändernden Arbeits- und Bürowelt besser zu verstehen und daraus entsprechende Lösungen abzuleiten.

Nachhaltige Dokumentenprozesse

Als hundertprozentige Tochtergesellschaft der japanischen KYOCERA Corporation spielt insbesondere das Thema Umweltschutz bei KYOCERA Document Solutions eine zentrale Rolle: So legte bereits der Gründer des KYOCERA-Konzerns, Dr. Kazuo Inamori, im Jahre 1959 fest, dass eine harmonische Koexistenz mit Natur und Gesellschaft die Grundlage aller Geschäftsaktivitäten zu sein hat. Daher verbindet man auch in der deutschen Niederlassung von KYOCERA Document Solutions, die im Jahr 2016 ihr 30-jähriges Bestehen feiert, Ökonomie und Ökologie miteinander.

Neben dem Angebot von klimaneutralem Toner gehört hierzu vor allem der „KYOCERA Umweltpreis“. Dieser wird im Jahr 2016 bereits zum fünften Mal verliehen und möchte die Entwicklung von umweltfreundlichen Bürokonzepten fördern. Der „KYOCERA Umweltpreis“ ist aus der seit 1987 bestehenden Partnerschaft mit der Deutschen Umwelthilfe (DUH) hervorgegangen. Für sein Umweltengagement wurde KYOCERA Document Solutions Deutschland 2014 auch mit dem „Blauen Engel-Preis“ ausgezeichnet.

Impressum

KYOCERA Document Solutions Deutschland GmbH
Otto-Hahn-Straße 12 | D-40670 Meerbusch
Telefon: 0800 / 187 187 7 | Fax: +49/2159/918-100