OKTOBER/NOVEMBER 2020 29. JAHRGANG DEUTSCHLAND € 6,00 ÖSTERREICH € 6,20 G6095

FACTS MAG

Test- und Wirtschaftsmagazin

Arbeitswelt im Stresstest

64 **STRESSVOLL**
Vermehrte Cyberangriffe auf Krankenhäuser

86 **STRESSFREI**
Moderne Telefonie ohne Hardwareinstallation

Technik **verbindet …**

… leider nicht nur mit den gewünschten Menschen. Auch Cyberkriminelle machen sich die Verbindungen zunutze. Dass Drucker und Multifunktionssysteme als entscheidende Schnittstelle zwischen analogen und digitalen Prozessen ein Einfallstor bieten können, wird oft sträflich vernachlässigt – hat eine Studie von Sharp herausgefunden.

Denken Sie wirklich, Ihr Drucker fristet ein harmloses Schattendasein? Haben Sie noch nie darüber nachgedacht, was er gerade treibt? Dann sind Sie nicht allein. „Moderne Multifunktionssysteme können weit mehr als drucken und scannen", klärt Jens Müller auf. Der Ethik-Hacker hat sich intensiv mit dieser Schwachstelle in Unternehmen befasst: „Sie sind an das Firmennetzwerk angeschlossen, kommunizieren mit anderen Anwendungen und assistieren damit bei einer Vielzahl von Aufgaben, die am Arbeitsplatz anfallen. Bei unzureichendem Schutz stellen sie damit ein perfektes Ziel für Hacker dar. Diese haben es in der Regel nicht nur auf sensible Daten aus Druck-, Scan- und Faxaufträgen abgesehen – vielmehr nutzen sie den Drucker als Einfallstor, um sich unbemerkt im ganzen Unternehmensnetzwerk auszubreiten. Ein solcher Sicherheitsvorfall kann schwerwiegende rechtliche Konsequenzen und Schäden in Milliardenhöhe nach sich ziehen."

LÜCKEN DRINNEN UND DRAUSSEN

Dass dies keine Lappalie ist, zeigt die jüngste Studie von Sharp. In einer europaweit angelegten Umfrage hat der Hersteller kleine und mittelständische Unternehmen (KMU) zu ihrem Sicherheitsbewusstsein und den entsprechenden Maßnahmen im Umgang mit Multifunktionssystemen befragt. „Was wir gefunden haben, war sehr interessant, hat aber mehr beunruhigende Fragen aufgeworfen als Fragen beantwortet", sagt Torsten Bechler, Manager Product Marketing DACH bei Sharp. Die Umfrage ergab, dass in ganz Europa weniger als 10 Prozent der Büroangestellten ihrem MFP als IT-Sicherheitsrisiko betrachten, ebenso wenige sind sich überhaupt darüber im Klaren, dass netzwerkfähige Drucker ein Einfallstor für Hacker darstellen.

Mit dem internen Datenschutz verhält es sich ganz ähnlich. So gaben 20 Prozent der Befragten an, dass sie überhaupt keinen Sicherheitsprozess haben, der regelt, wie ihr

„Hacker haben es in der Regel nicht nur auf sensible Daten aus Druck-, Scan- und Faxaufträgen abgesehen – vielmehr nutzen sie den Drucker als Einfallstor, um sich unbemerkt im ganzen Unternehmensnetzwerk auszubreiten."

JENS MÜLLER, Ethik-Hacker

MFP verwendet wird, und 68 Prozent der Studienteilnehmer berichten, dass in ihrem Unternehmen kein spezielles Authentifizierungsverfahren für den Zugang zum Drucker zum Einsatz kommt: Auch auswärtige Personen könnten jederzeit auf das Gerät zugreifen. Nicht einmal die Hälfte der Mitarbeiter hat an einer Schulung oder Weiterbildung zum Thema sicheres Drucken und Scannen teilgenommen. Deshalb ist es auch um den Umgang mit den Informationsknotenpunkten schlecht bestellt – allen voran im Personalwesen. Aus diesem Bereich bestätigten 90 Prozent der Befragten, dass in ihrem Unternehmen jeder den MFP frei nutzen kann. Mit einigem Abstand folgen die Kommunikationsbranche (60 Prozent) und – trotz Wissensvorsprung beim Thema IT-Sicherheit – der IT- und Telekommunikationssektor (59 Prozent). Auch das Alter der Büroangestellten spielt eine Rolle: So wissen etwa 52 Prozent der 16- bis 24-Jährigen, dass Scans ohne ausreichende Sicherheitsvorkehrungen von Hackern abgefangen werden können. Bei den 45- bis 54-Jährigen ist dieses Wissen nur noch zu 28 Prozent verbreitet.

VORKEHRUNGEN TREFFEN

Das Problem lässt sich nicht so einfach lösen – schließlich sind MFPs unverzichtbare Helfer im Büro, die man nicht einfach abschaffen oder zumindest vom Netz nehmen kann. Während der hauseigene Datenschutz in erster Linie eine Frage des Verhaltens ist, kann jedes Unternehmen mit Sensibilisierung der Mitarbeiter sowie relativ einfachen technischen Maßnahmen dazu beitragen, das Bewusstsein für Sorgfalt im Umgang mit Dokumenten zu schärfen, damit keine Ausdrucke oder Kopiervorlagen liegen bleiben dürfen beziehungsweise können. Funktionen wie Datenverschlüsselung und Zugriffskontrolle helfen dabei, zu verwalten, wer was drucken darf, und stellen sicher, dass zum Drucken gesendete Daten sicher bleiben. Einige MFPs von Sharp verfügen sogar über eine physische Erinnerung, die Dokumente nach dem Scannen zu entfernen, um zu verhindern, dass Originalausdrucke in die falschen Hände geraten.

Drucker und Multifunktionsgeräte vor Angriffen von außen zu schützen, ist hingegen eine IT-Aufgabe. Doch auch die lässt sich lösen, weiß Bechler: „Hacker nutzen immer das schwächste Glied im System. Die gute Nachricht ist: Mit vergleichsweise geringem technischem Aufwand lässt sich sicherstellen, dass es nicht ausgerechnet ein Schlüsselsystem wie der Drucker ist."

Mit Unterstützung durch Jens Müller hat Sharp einen Leitfaden mit Tipps und Lösungsansätzen zum Thema Datensicherheit bei MFPs erarbeitet, der kostenlos erhältlich ist. „Neben der technischen Komponente ist die Aufklärung und Stärkung des Risikobewusstseins bei den eigenen Mitarbeitern wichtig", ist sich Torsten Bechler sicher. „Verbindliche Richtlinien und Awareness-Trainings zur Nutzung der Multifunktionsgeräte helfen, eine durchgängige Sensibilität für Risiken und sicherheitskonformes Verhalten zu schaffen. Unser ‚Security Guide' hilft insbesondere kleinen und mittelständischen Unternehmen, die grundlegendsten Maßnahmen Schritt für Schritt umzusetzen."

Anja Knies ■

„Die gute Nachricht ist: Mit vergleichsweise geringem technischem Aufwand lässt sich sicherstellen, dass nicht ausgerechnet ein Schlüsselsystem wie der Drucker zur Schwachstelle im Netzwerk wird."

TORSTEN BECHLER, Manager Product Marketing Sharp Business Systems Deutschland