# Hackers Liebling

**Drucker und Scanner sind in Unternehmen Einfallstore für Angriffe. Das geht problemlos und schnell. Die Abhilfe ist ebenso schlicht. Doch dafür müssen einige wenige Vorkehrungen getroffen werden**

Bei uns ist alles sicher. Eine Antwort, die Hendrik Herberger zur Genüge kennt. Der Experte für IT-Sicherheit bei der Modox – Modern Documents hört sie immer wieder, nur entspricht sie selten der Realität. Drucker, Scanner, Fax, meist vereint in einem Multifunktionsgerät bieten eine große Angriffsfläche für Daten-Klau. „Die wenigsten kennen die Gefahr", so der Fachmann. Der große Bundestags-Hack vor Kurzem – „dabei spielten diese Geräte eine große Rolle".

Die Cyber-Attacke erfolgte über Netzwerkdrucker, mit der Folge, dass das politische Leben in Berlin zum Stillstand kam. Einfallstore bieten insbesondere Multifunktionsgeräte zuhauf. Via Drucker ins firmeneigene Netzwerk – kein Problem. Das dauert maximal eine halbe Minute, live und anschaulich demonstriert von Herberger. Die dafür erforderliche Vorgehensweise liefert das Internet kostenlos und frei zugänglich. Auch IP-Telefone lassen sich so in Abhörwanzen verwandeln.

Damit Daten in falsche Hände gelangen, bedarf es nicht einmal krimineller Energie. Meist reichen Unwissenheit und Schlampigkeit. „Vergessene Dokumente im Ausgabefach ist einer der häufigsten Gründe, wie Informationen an Unbefugte gelangen." Ständige Schulungen und eine klare Nutzerregelung versprechen hier Linderung.

Ein anderes Problem ist die Festplatte. Welche Festplatte? Das bekommt Herberger ebenfalls häufig zu hören. Ausdruck der Unkenntnis dessen, dass die Multifunktionsgeräte eine solche besitzen. „Alles, was gescannt wird, wird auf der Festplatte gespeichert", betont der Experte. Und das meist für immer. Geht das Gerät zurück an den Hersteller oder wird verkauft, denken die wenigsten daran, die Daten der Festplatte vorher zu löschen. Ein ebenso häufig begangener Fehler ist der laxe Umgang mit den Passwörtern der Geräte. „Kaum einer ändert die Standardpasswörter der Werkseinstellung."

Die wiederum sind jedermann zugänglich. Wer nun Böses im Schilde führt, kann sich folglich einfach im Service-Menü des Geräts einloggen: „Also unbedingt selbst Passwörter setzen." Weiterhin rät der Fachmann, alle unnützen Protokolle ebenso abzuschalten wie die USB-Funktion sowie eigene und klare Richtlinien zum Umgang mit Multifunktionsgeräten zu entwickeln. Schutz verspricht zudem eine Software, die im Hintergrund prüft, ob alle Parameter in Ordnung sind. ***Michael Hölle***


Nach der Ka-It-Si-Veranstaltung sahen viele Teilnehmer Drucker mit anderen Augen

Foto: KaITSi

KA IT-Si
Karlsruher IT-Sicherheitsinitiative

## Psychologie der Sicherheit

Ist der DAU wirklich dumm? Der Faktor Mensch spielt eine wichtige Rolle in der IT-Sicherheit. Deshalb orientiert sich diese gerne am „dümmsten anzunehmenden User" (DAU). Wie solche Fehler bei der Entscheidungsfindung entstehen und wie man daraus lernen kann, das zeigt die Veranstaltung auf.

**Wo** Fraunhofer IOSB, Fraunhoferstraße 1, Karlsruhe
**Wann** 21. April, 18 Uhr