

Fotokopierer: Die angreifbare Datenstation

Das Gerät steht dort, wo es für möglichst alle bequem erreichbar ist – im Durchgangsflur, im Eingangsbereich, im kleinen, oft unbeobachteten Abstellraum. Es ist mindestens während des gesamten Arbeitstages und häufig auch rund um die Uhr in Betrieb. Und es hängt oft an einer wenig bis gar nicht geschützten Datenleitung. Würden Sie einem solchen Gerät sensible Daten anvertrauen? Nein? – Sie tun es fast täglich: Die Rede ist von Ihrem modernen und mit vielfältigen Funktionen ausgestatteten Fotokopierer, der für clevere Datendiebe eine wahre Fundgrube darstellt. Wussten Sie das?

Die Geräte, die vereinfacht immer noch nur Fotokopierer genannt werden, sind heutzutage ungeheuer praktische Alleskönner: Je nach Ausstattung taugen sie nicht nur für 1:1-Kopien einzelner Dokumente, nein, sie lassen sich als Drucker an einen oder mehrere Computer anschließen, sie versenden Faxe oder sind als Scanner für beliebig dicke Dokumentenstapel einsetzbar – und das alles in einstellbarer Qualität sowie je nach Belieben in Schwarzweiß- oder Farb-Wiedergabe. Kurzum: Kopiergeräte sind mittlerweile zu Multifunktionsgeräten mutiert und dabei meist schnell und einfach zu bedienen. Und weil sie an ihren Einsatzorten und für ihre vielfältigen Zwecke mit den jeweiligen Computern vernetzt sind, haben in Firmen, Behörden, Arztpraxen, Anwaltskanzleien oder Kirchenverwaltungen viele Menschen Zugriff auf diese Geräte, ohne deshalb ständig neben ihnen stehen zu müssen: Große Teile des Tages sind "Kopierer" unbeaufsichtigt.

Und das kann fatale Folgen haben. Denn obwohl ihre Bedienung vergleichsweise einfach ist, müssen innerhalb der Kopierer für deren einzelne Funktionen oft riesige Datenmengen bewegt, sortiert und selbstverständlich auch gespeichert werden. Normale Druckjobs erzeugen ebenso Daten wie komplexe Kopieraufgaben, beides erfordert eine zumindest vorübergehende Speicherung. Die Daten gescannter Dokumente oder Bilder müssen vom

Gerät wenigstens solange aufbewahrt werden, bis sie auf andere Computer oder Datenträger kopiert oder verschoben worden sind. Zeitversetzte Arbeitsfunktionen wie beispielsweise beim Versenden (oder Empfangen) von Faxen erfordern gar eine Datenspeicherung auf lange Sicht und Abruf.

All diese Aufgaben können diese Geräte nur bewältigen, weil sie mit großem internem Speicherplatz ausgestattet sind. Sie besitzen sowohl einen so genannten flüchtigen Arbeitsspeicher, dessen Inhalte beim Ausschalten gelöscht werden, als auch Festplatten oder andere nicht-flüchtige Speicher, die ihre Inhalte selbst dann behalten, wenn der Netzstrom abgeschaltet ist. Auf diesen nicht-flüchtigen Speichern werden beispielsweise Dateien mit den zu druckenden oder zu kopierenden Informationen angelegt – und die existieren solange, bis die Aufgabe erledigt ist. Danach wird zwar der Speicherplatz, den diese Datei innerhalb des Kopierers belegt hat, automatisch wieder freigegeben, aber die enthaltenen Daten sind damit nicht zwingend unumkehrbar gelöscht. Wie bei jeder Computerfestplatte bleiben in der Regel Datenspuren auf den Speichern zurück – und die lassen sich mit geringem technischen Aufwand wieder herstellen. Die notwendigen Informationen hierzu sind im Internet zu finden: Für nahezu jedes Gerät sind dort entsprechende Zugangsdaten aufspürbar: Standard-Passwörter, Administrator-Codes oder Tastenkombinationen, die beim Einschalten des jeweiligen Geräts gedrückt werden müssen, um administrative und somit allumfassende Rechte für den Zugang zum Innersten der Kopiersysteme zu erhalten.

Unbefugte, die direkt am Kopierer stehen, können so alle Möglichkeiten ausschöpfen, die das Gerät bietet: Noch gespeicherte Aufträge sind ebenso leicht auszudrucken wie scheinbar gelöschte, real aber noch vorhandene Daten alter Kopien, Faxe oder Druckaufträge wieder sichtbar gemacht werden können. Dieses Risiko besteht selbstverständlich auch, wenn der Kopierer mit einem lokalen Computer-Netzwerk verbunden ist, um seine Ressourcen mehreren Personen zur Verfügung zu stellen. In der

Regel können die Geräte dann bequem und einfach von einem beliebigen PC dieses Netzes aus konfiguriert werden. Mit den Standardpasswörtern des Herstellers, wenn diese nicht bei Inbetriebnahme des Kopiersystems abgeändert wurden, und einem Browser ist das meist problemlos möglich. Falls das jeweilige Computer-Netzwerk Anschluss hat an das Internet, können sachkundige Hacker sich sogar von außen Zugang zu den gespeicherten Daten der Geräte verschaffen.

Es ist also unbedingt darauf zu achten, dass für die ach, so alltäglichen und einfach anmutenden "Fotokopierer" mindestens so scharfe Sicherheitsstandards entwickelt und beachtet werden wie für herkömmliche Computer (und Netzwerke). Und diese Sorgfaltspflicht reicht weit: Denn auch der Verkauf eines nicht mehr benötigten Geräts, seine Rückgabe (falls es gemietet war) oder seine Entsorgung bringen Datenschutzrisiken mit sich. Bei jedem dieser Vorgänge muss sichergestellt werden, dass die auf den Datenträgern des Kopierers noch verbliebenen Daten nicht in unbefugte Hände gelangen.

Auf den hier beschriebenen multifunktionalen Fotokopiergeräten werden alle nur denkbaren Arten personenbezogener, aber auch sonstiger schützenswerter Daten verarbeitet: Bewerbungen, Gehaltsbescheinigungen, Fotos, Kontoauszüge, medizinische Berichte und Gutachten, Führungszeugnisse oder Strafbefehle, Asylanträge, Ausschreibungs- oder Buchhaltungsunterlagen, Rechenschaftsberichte, Entwicklungskonzepte, Patentunterlagen – die Aufzählung könnte nahezu endlos weitergeführt werden. Die meisten Nutzer achten zwar darauf, dass weder papierne Originale noch Kopien im Gerät verbleiben. Die Daten aber, die in den Speichern des Kopierers verbleiben, können in der Regel nicht einfach und problemlos entfernt werden. Für den normalen Nutzer sind diese Daten unsichtbar, vielen ist nicht einmal bewusst, dass sie existieren. Es liegt also nahe, dass sie im Umgang mit solchen Geräten eigentlich notwendige Sorgfalt vermissen lassen.

"Was man nicht sieht, ist auch nicht da"? – Dieser Schein trügt.

Eckpunkte: Datenschutzgerechter Einsatz digitaler Kopiersysteme

1. Nutzung nur durch berechtigte Personen ermöglichen

Die Kopiersysteme sollten gegen eine unbefugte Nutzung gesichert werden, insbesondere sollten sie nicht in Bereichen mit Publikumsverkehr oder an unbeaufsichtigten Orten aufgestellt werden. Durch die notwendige Eingabe von Codes vor jeder Benutzung oder durch den Einsatz elektronischer Schlüssel wie beispielsweise Kopierkarten kann erreicht werden, dass nur berechtigte Personen den Kopierer nutzen können. Eine Weitergabe von Schlüsseln oder Freigabecodes an Dritte darf selbstverständlich nicht erfolgen.

2. Ändern der Standardpasswörter

Wie viele andere Geräte der EDV werden auch Fotokopierer vom Hersteller mit Standardpasswörtern ausgeliefert. Da diese nicht nur in den offiziellen Handbüchern nachzulesen, sondern mit hoher Wahrscheinlichkeit auch im Internet recherchierbar sind, eignen sie sich überhaupt nicht, um das Kopiersystem vor unbefugter Nutzung oder Konfiguration zu schützen. Deshalb sind die Standardpasswörter bei Inbetriebnahme unbedingt in geeigneter Weise abzuändern.

3. Umgang mit Kopiergut

Originale und Kopien sind immer sofort nach Ende der Nutzung aus dem Gerät zu entfernen.

4. Fehlkopien datenschutzgerecht vernichten

In unmittelbarer Nähe zum Kopiersystem sollte ein Schredder möglichst in so genannter Crosscut-Qualität platziert werden, mit dem Fehlkopien mit personenbezogenem oder anderweitig sensiblem Inhalt umgehend und wirksam vernichtet werden können.

5. Rückstellung

Alle Nutzer müssen angehalten sein, das System nach Gebrauch manuell in seinen ursprünglichen Zustand zurück zu versetzen, beispielsweise durch Drücken der <C>-Taste oder einer Tastenkombination, mit der das System in den Stand-by-Modus geschaltet wird. Ist die Nutzung nur durch bestimmte Schlüssel (Zahlen, Token, Kopierkarte) möglich, ist das Gerät so zu konfigurieren, dass es nach Entfernen des Schlüssels automatisch in den ursprünglichen Zustand versetzt wird. Die Schlüssel sind aus dem Gerät zu entfernen, sobald die Nutzung abgeschlossen ist; ein Schlüssel, der aus Gründen der einfacheren Nutzbarkeit über längere Zeit (etwa für einen kompletten Arbeitstag) im Kopierer aktiv bleibt, ist nutzlos.

6. Einsatz des Kopierers als Abteilungsdrucker

Werden die Kopierer als Arbeitsgruppendrucker von mehreren Personen genutzt, so sollten dort möglichst keine Dokumente mit personenbezogenen oder anderweitig sensiblen Daten ausgedruckt werden. Lässt sich dies indes nicht vermeiden, sollte die Druckfunktion mit einer Sperre versehen werden: Der Druck wird solange nicht ausgeführt, bis der zugehörige Auftraggeber direkt am Gerät einen mehrstelligen Code eingibt. So wird sichergestellt, dass die ausgedruckten Dokumente sofort nach Abschluss des Druckvorgangs entfernt werden können und dass keine unbefugten Personen Kenntnis der ausgedruckten Daten erhalten können.

7. Nicht benötigte Dienste abschalten

Die Kopiersysteme stellen, wenn sie mit einem Computernetzwerk verbunden sind, eine Vielzahl von Netzdiensten zur Verfügung. Vom Hersteller werden die Geräte in der Regel so konfiguriert, dass sie möglichst problemlos in Betrieb genommen werden können. Beispielsweise werden die Geräte mit unterschiedlichsten Netzwerkprotokollen programmiert, damit von verschiedensten Computersystemen aus auf sie zugegriffen

werden kann. Bei der Inbetriebnahme sollten daher die Dienste, die für den konkreten Einsatzzweck nicht benötigt werden, abgeschaltet werden. In reinen Microsoft-Windows-Netzwerken etwa wird das Netzwerkprotokoll "AppleTalk" nicht benötigt; es gehört abgeschaltet.

8. Verschlüsselte Ablage der Daten

Je nachdem, wo das Fotokopiersystem eingesetzt wird (Handelsunternehmen, Forschungseinrichtungen, Ärzte, Steuerverwaltung etc.) und welche Arten von Daten hauptsächlich auf ihm verarbeitet werden, sollte die Datenspeicherung möglichst in geeigneter Weise verschlüsselt erfolgen. Insbesondere bei der Neuanschaffung von Geräten sollte auf diese Option geachtet werden. Die Daten sind dann vor missbräuchlicher Nutzung geschützt, auch wenn das Kopiergerät beispielsweise gestohlen wird. Wichtig dabei ist, dass die verwendeten Zugangscodes und Passwörter wie unter Punkt 2 beschrieben bei Übergabe niemandem mitgeteilt werden. Oft ist Verschlüsselung nur über eine Zusatzfunktion erreichbar, die den Einsatz so genannter "Security-Kits" erfordert (siehe auch Punkt 9: Löschen der Daten).

9. Löschen der Daten

Bei der Neubeschaffung von Kopiergeräten muss auf eine Konfiguration geachtet werden, mit der die Daten unumkehrbar automatisch gelöscht werden, sobald sie nicht mehr benötigt werden. Meist wird diese Funktion über (optional erhältliche) Zusatzmodule mit Namen wie "Security-Kit" oder "Daten-Sicherheits-Kit (DSK)" ermöglicht. Zusätzlich sollte es jederzeit möglich sein, die vollständige Löschung aller Daten manuell anzustoßen. Hintergrundinformationen zur datenschutzgerechten Löschung von Datenträgern sind unter dem folgenden Link zu finden:

http://www.datenschutz-bremen.de/pdf/oh_sicheres_loeschen.pdf

10. Sicherheitsupdates

Sicherheitsupdates, die von den Herstellern zur Verfügung gestellt werden, sollten umgehend installiert werden, um bekannte Sicherheitslücken im Kopiersystem zu schließen. Dies gilt insbesondere dann, wenn der Kopierer als Multifunktionsgerät innerhalb eines Computernetzwerks betrieben wird.

11. Wartungspasswörter

In der Regel existiert zu jedem Gerät ein so genanntes Master-, Wartungs- oder Servicepasswort. Damit ist es den Wartungstechnikern der Hersteller möglich, auch dann administrativ auf das System zuzugreifen, wenn Kunden ihre Passwörter vergessen haben. Es sollten nach Möglichkeit nur solche Systeme angeschafft werden, bei denen es möglich ist, die Daten innerhalb des Systems vor dem Zugriff nach Eingabe des Masterpasswortes zu schützen.

12. Rückgabe, Verkauf und Entsorgung

Bei der Entsorgung ausgemusterter Geräte gilt, dass alle Daten, die noch auf dem System verblieben sind beziehungsweise sein könnten, gelöscht werden müssen. Falls dies nicht durch manuelles Anstoßen eines Löschvorgangs und/oder durch Einsatz von "Security-Kits" (siehe Punkt 9) wirksam erreicht werden kann, müssen die Datenträger physikalisch zerstört werden.