

Beitrag Multifunktionsgeräte, Jörg Frahm, 21. Juni 2006

Scannen, Faxen, Mailen, Drucken. Multifunktionsgeräte: Eine Herausforderung für den Datenschutzbeauftragten.

Vortrag von Jörg Frahm, Datenschutzbeauftragter Panasonic, anlässlich des Treffens im Ruder-Club Favorite Hammonia am 21. Juni 2006

Als Sie die Einladung bekamen und über den folgenden Vortrag lasen, kam Ihnen sicherlich der Gedanke, was soll das, wir kennen uns mit Faxen aus, Scannen gehört ebenso zum Alltag wie E-Mail-Versendung und das Drucken. Was ändert sich eigentlich durch die angesprochenen Multifunktionsgeräte? Der Datenschutz in diesen Bereichen gehört doch zu unseren täglichen Arbeitsaufgaben.

Natürlich haben Sie Recht und Ihre Aufgaben sind erfolgreich durchgeführt, aber trotzdem gibt es einen erheblichen Wandel in der Technik, der erst einmal verinnerlicht werden muss, und die sich daraus ergebenden Datenschutzaufgaben müssen erkannt und umgesetzt werden.

Lassen Sie mich dieses vorab einmal als Wandel mit Globalisierungsaktionen bezeichnen. In den Organisationsstrukturen vieler Firmen wird heute unter dem Begriff Globalisierung Vieles vereinheitlicht. Auch das Drucken und Kopieren.

A. Peripheriegeräte

Früher wurden Scanner, Drucker und Faxgeräte an vielen Arbeitsplätzen eingesetzt; mit Geräten, die unmittelbar am Arbeitsplatz angeschlossen worden sind. Dies ist teilweise auch heute noch der Fall. An meinem eigenen Arbeitsplatz beispielsweise befinden sich jeweils ein Farbtintenstrahldrucker und ein hochauflösender Scanner. Diese Ausstattung befindet sich in dieser oder ähnlicher Konstellation an mindestens 60 bis 70 % der Arbeitsplätze meines Unternehmens.

B. Multifunktionsgeräte

Bei dem Fortschreiten der Technik ist es eine natürliche Folge, dass hier über Synergieeffekte nachgedacht wird. Das Ergebnis sind so genannte Multifunktionsgeräte, die einen großen Teil der Anforderungen in einem Gerät durchführen können. Sie können Scannen und die Ergebnisse als E-Mails oder Faxe versenden oder direkt drucken. So verhält es sich auch mit den sonstigen Druckaufträgen.

Gerade für diese Multifunktionsgeräte, die auch noch netzwerkfähig sind, bietet sich der Einsatz an räumlich zentralen Positionen im Unternehmen an. Entsprechend der Organisationsstruktur kann dieses flur-, etagen- oder auch abteilungsweise erfolgen. Der Nutzen liegt in der Optimierung von Workflows und kann damit auch eine erhebliche Kostensenkung bringen. Bei zentralen Geräten lassen sich höhere Qualitäten erzielen, weil mehr investiert wird.

In der Vergangenheit wurden Dokumente von jedermann erstellt und dann über ein Verteilungssystem wie die Hauspost an den Bestimmungsort gebracht. Durch den Einsatz der Multifunktionsgeräte hat im Umgang mit der Dokumentenerstellung eine Veränderung

stattgefunden. Sie werden elektronisch verteilt und dann bei Bedarf von den Empfängern gedruckt.

C. Datenschutzfragen

Jetzt stellt sich die Frage nach der Daten- und Zugriffssicherheit, insbesondere nach dem Installationsort. Gibt es sicherheitstechnisch geschützte Druckerräume, welchen Zugriffs- und Zutrittsschutz gibt es, wie werden Zugriffe auf die Festplatte des Multifunktionsgerätes verhindert und welche Lösungsverfahren werden für die dort befindlichen Daten verwendet.

Um die Sicherheiten der PCs und Notebooks haben sich die Geschäftsleitungen in der Vergangenheit viele Gedanken gemacht und diese häufig über Nutzungsvereinbarungen geregelt. Die datenschutzrechtlichen Gedanken über die mögliche Streuung und den damit erleichterten Missbrauch von personenbezogenen Daten bei Multifunktionsgeräten stecken noch in den Kinderschuhen.

Im Datenschutz-Berater, den Ausgaben 5/2005 und 3/2006, wurde auf diese Problematik schon von Dr. Probst (ULD Schleswig-Holstein), Dr. Kramer und mir in ausführlichen Beiträgen hingewiesen.

D. Allgemeine technische Fragen

Noch einmal zurück zur technischen Schutzproblematik. Wenn die Multifunktionsgeräte, eingebunden in die Firmennetzwerke, keine eigenen E-Mail-Adressen haben, so ist ein Virenangriff nicht als problematisch anzusehen, denn Viren setzen fast ausschließlich auf Microsoft-Betriebssysteme auf. Durch eine Firewall lassen sich Attacken von außen sehr leicht in den Griff bekommen. Wird IP-Filterung eingesetzt, so werden dadurch Zugriffsmöglichkeiten eingegrenzt. Nur bestimmten PCs wird der Zugriff auf die Multifunktionsgeräte gewährt. Es gibt also diverse Möglichkeiten des technischen Schutzes.

Trotzdem müssen die Gedanken auf den Datenschutz gerichtet werden. Jedem Anwender muss bewusst sein, dass kopierte, gescannte oder gedruckte Dokumente personenbezogene Daten beinhalten können, die durch das Gerät elektronisch gespeichert werden. In der Regel wird das als Zwischenspeicherung über die Festplatte oder einen anderen internen Speicher durchgeführt. Auf jeden Fall kann die zuletzt erstellte Dokumentenseite noch auf der so genannten Drucktrommel vorhanden sein. Ein Hinweis für die Praxis: erstellen Sie Drucke oder Kopien, sollte das letzte Blatt ein Leerblatt sein. Damit ist die Drucktrommel auf jeden Fall gelöscht.

In der Regel werden die Unternehmen keine eigenen Wartungstechniker einsetzen, das heißt, dass externe Techniker unter Umständen Zugriff auf gespeicherte Daten haben können. Wartungs- oder Reparaturverträge sollten immer die datenschutzrechtlichen Anforderungen gemäß § 11 BDSG (Auftragsdatenverarbeitung) einhalten. In jedem Fall sollten die Wartungstechniker aber auch nach § 5 BDSG zur Geheimhaltung verpflichtet sein.

E. Technische Fragen betreffend Anlage zu § 9 BDSG

Lassen Sie mich jetzt noch andere datenschutzrechtliche Aspekte betrachten. Sind beim Kopieren, Scannen oder Faxen personenbezogene Daten auf den Dokumenten enthalten, so sind die Voraussetzungen zur Anwendung des Bundesdatenschutzgesetzes erfüllt (§ 3 Abs. 1 BDSG). In jedem Fall werden in den Geräten Kopien erzeugt und somit Daten unter Einsatz einer Datenverarbeitungsanlage gespeichert und verarbeitet. Damit ist in der Regel auch der Dateibegriff erfüllt. Die Zwischenspeicherung erfolgt entweder auf Festplatten oder auf digitale Speicherkarten, die ohne besonderen Aufwand nicht rückstandsfrei gelöscht werden können.

Damit erhalten die Multifunktionsgeräte den Status eines PCs. Dieses ist auch immer dann gegeben, wenn durch Faxeingänge elektronische Post aufgenommen wird. Die Anforderungen der Verfügbarkeit gem. Ziffer 7 der Anlage zu § 9 BDSG müssen erfüllt sein, ebenso wie die Anforderungen der Eingabekontrolle gem. Ziffer 5 zur Anlage § 9 BDSG. Zur Löschsicherheit könnte aber auch eine technische Lösung über die Firmware der Multifunktionsgeräte beitragen, wenn über Standardeinstellungen gewährleistet ist, dass die Kopiervorgänge keine Spuren hinterlassen. Durch ausgeprägte Löschvorgänge kann das erreicht werden.

Da die Multifunktionsgeräte in den Unternehmen fast immer von einer größeren Anzahl Mitarbeitern bedient werden, ist das Datensicherheitsziel der Vertraulichkeit, wie es in den Ziffern 1, 2, 3 und 4 der Anlage zu § 9 BDSG beschrieben ist, zu gewährleisten. Unbefugte dürfen keinen Zugriff auf die Daten erhalten. Eine Möglichkeit besteht darin, jedem Anwender über eine Nutzerauthentisierung und Rechteverwaltung, die über die normale Passwortlösung hinausgehen, eigene Zugriffsbefugnisse zu erteilen. Stichworte sind hierzu die Verwaltung der Anwender über so genannte Meta-Directories oder das Netzwerk-Protokoll LDAP (Lightweight Directory Access Protocol (LDAP)).

Irgendwann hat auch der Einsatz des konkreten Multifunktionsgerätes aufgrund der technischen Veralterung, der Miet- oder Leasingabläufe oder anderer firmeninterner Gründe ein Ende. Geleaste und gemietete Geräte sind Eigentum der Leasing- oder Vermietungsgesellschaft, so dass nach Ablauf der Vertragszeit die Geräte an die Eigentümer zurückgegeben werden. Hier ist in den Verträgen sicherzustellen, dass die Eigentümer vor einer weiteren Verwendung der Geräte die Daten hinreichend zu löschen haben. Bei einem gekauften Gerät ist das Unternehmen selbst für eine entsprechende Löschung der Daten vor einer Weitergabe oder einer Entsorgung verantwortlich. Als Stichwort möchte ich nur auf die Elektronikschrottverordnung hinweisen.

F. Empfehlungen aus der Sicht des Datenschutzes

1. Multifunktionsgeräte sollten grundsätzlich wie PCs betrachtet werden. Das bedeutet, dass der Einsatz eines Multifunktionsgerätes der Vorabkontrolle unterliegt und der Einsatz ins Verzeichnissverzeichnis aufgenommen werden muss.
2. Es sollten aus Datenschutzgründen Geräte bevorzugt werden, die über datenschutzgerechte Mechanismen, wie beispielsweise eine Verschlüsselung der vom Kopiergerät eingelesenen Daten und eine Löschroutine verfügen. Dabei sind bei der Beurteilung die erzielten Vertrauenswürdigkeitsstufen (Evaluation Assurance Level) zu beachten.
3. Generell müssen Zugang und Zugriff auf das Gerät kontrollierbar sein.
4. Nach jedem Kopier-, Scan-, Druck- oder Versandvorgang muss die zugehörige Datei auf der Festplatte gelöscht werden.
5. Über eine Speicherung und Speicherdauer muss der Benutzer selbst entscheiden.
6. Wenn möglich, sollten die Daten verschlüsselt abgespeichert werden.
7. Es sollte sichergestellt werden, dass Mitarbeiter nur auf ihre Dateien Zugriff haben. Wenn vom Kopierer unterstützt, sollten passwortgeschützte Mitarbeiterverzeichnisse genutzt werden.
8. Beim Löschen sollten die Maßnahmen der Löschung im Sinne der Datenschutzbestimmungen betrachtet werden. Es gibt Geräte, die gespeicherte Dateien nicht nur löschen, sondern überschreiben.
9. Wartungsfirmen sind auf die Einhaltung der Bestimmungen des BDSG zu verpflichten.
10. Eine Weiter- oder Rückgabe der Kopierer und Drucker darf nur nach der physikalischen Löschung aller gespeicherten personenbezogenen Daten erfolgen. Auf besondere Vorsicht ist bei Leasing- und Mietgeräten ebenso zu achten wie beim Verkauf der Geräte.

G. Einzelne Geräte

Lassen Sie mich nun noch einmal ganz kurz auf die Hardwarehersteller eingehen. Bei allen Geräten ist eine PIN-Code-Identifizierung und eine Netzwerkeinbindung Standardausrüstung. Brother MFC-8840D ist beispielsweise ein typischer Abteilungsdrucker mit diversen Sicherheitsfunktionen, sollte aber nur für mittlere Arbeitsgruppen eingesetzt werden. Canon ImageRunner 3000: die Systeme verfügen unter anderem auch über biometrische Identifikationen. Hewlett Packard schützt alle Systeme auf verschiedenen Ebenen. Kyocera Mita: neben hauseigenen Chipkarten steuern auch noch berührungslose Transponder den individuellen Zugriff. Nashua Docu-Station DCc460 findet keinen Einsatz als Abteilungsdrucker, sondern seinen Platz in zentralen Hausdruckereien. Die Sicherheitssysteme werden individuell angepasst. Panasonic WORKI-Serie verfügt über Abteilungscode-Einrichtungen und benutzerspezifische MAILBOXEN. Hier haben die Produktionsstellen Anforderungen des betrieblichen DSB umgesetzt. Ricoh Aficio verfügt über alle gängigen Sicherheitsfunktionen. Sharp Systeme arbeiten mit einem Security-Kit, wobei nur die Zusammenarbeit zwischen der Kopiermaschine und der Festplatte den Entschlüsselungscode liefert. Xerox-Systeme verfügen über zusätzliche Optimierungssysteme für die verschiedensten Sicherheits- und Netzwerkeinbindungen.

Im Datenschutzberater 04/2006 finden Sie auch eine Vorlage für eine Verpflichtungserklärung für externe Mitarbeiter gem. § 17 UWG und den dazugehörigen Wortlaut des § 17 UWG; Verrat von Geschäfts- und Betriebsgeheimnissen.

H. Fall aus der Praxis

Einem Angestellten wurden die Speicherfunktionen eines Multifunktionsdruckers zum Verhängnis. Anlässlich seiner Kündigung hatte er vertrauliche Unternehmensunterlagen mit einem Firmenkopierer vervielfältigt. Der Speicher des Gerätes dokumentierte seine Tat später.

I. Fazit

Die Anschaffung von Multifunktionsgeräten, die keine datenschutzgerechte Konfiguration erlauben, ist heute nicht mehr verantwortbar, da eine datenschutzkonforme Nutzung ohne technische und personelle Kontrolle nicht möglich ist. Durch Benutzeridentifikationen gibt es noch für viele Unternehmen den begrüßenswerten Nebeneffekt der korrekten Kostenstellenzuordnung.

Ich sage „Vielen Dank“ für Ihre Aufmerksamkeit und bedanke mich besonders bei Dr. Philipp Kramer für die inhaltliche Unterstützung.