Was sollen wir? Daten verschlüsseln?

Das vierte Gebot: Die Weitergabekontrolle

Die Weitergabekontrolle soll verhindern, dass personenbezogene Daten bei der elektronischen Übertragung, beim Transport oder bei der Speicherung auf Datenträgern unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Die Mehrheit der Anwender stellt sich jedoch die Frage: Wie mache ich das denn?

Die Weitergabe- oder Übermittlungskontrolle ist seitens des Datenschutzbeauftragten umfassend zu betrachten. Sie betrifft nicht nur die Übermittlung von Daten an Dritte oder externe Stellen, sondern umfasst auch die Datenverarbeitung innerhalb der verantwortlichen Stelle.

Zudem ist in der Regel die Weitergabe im Rahmen einer Auftragsdatenverarbeitung nach § 11 BDSG zwischen Auftraggeber und Auftragnehmer berührt. Auch die Übermittlung direkt an den Betroffenen fällt unter das Gebot der Weitergabekontrolle.

Nutzen Sie betriebliche Regelungen

Bei der Prüfung oder Neufassung betrieblicher Regelungen hat es sich in der Praxis bewährt, in den E-Mail-Vorgaben den Satz aufzunehmen: „Versenden Sie sensitive, d.h. personenbezogene und vertrauliche Informationen, nicht ungeschützt als E-Mail.“ Selbst in IT-Abteilungen stößt diese Forderung allerdings oft erst einmal auf Unverständnis: „Was, Verschlüsseln? Wie soll das gehen?“

Klassifizieren Sie zunächst die Übermittlungsdaten

In der Regel ist die datenschutzkonforme Umsetzung zur Erfüllung der Weitergabeanforderungen eine technische sowie auch eine organisatorische Sisyphusarbeit. Analysieren Sie zuerst die Unternehmenskommunikation. Aus den Beschreibungen der Verfahrensübersichten haben Sie als DSB bereits Anhaltspunkte zu den Datenflüssen. Hieraus gilt es nun, die Sensitivität der Daten festzulegen.

Wichtig: Struktur der Datenempfänger

Im Rahmen von durchdachten und praktikablen Übermittlungsgrundsätzen dürfen Sie auf keinen Fall die Struktur bzw. die Möglichkeiten Ihrer Datenempfänger außer Acht lassen: Businesskunden, bei denen eine funktionierende IT-Struktur im Hintergrund läuft, eröffnen andere Möglichkeiten zur Datenübermittlung als Endkunden mit eingeschränkter IT-Erfahrung.

Nicht zuletzt: Was kostet das Ganze?

Für jedes Unternehmen steht auch der Kostenfaktor zur Disposition. Es muss nicht immer eine Komplettlösung für x-Tausend Euro sein. Im Rahmen der Verhältnismäßigkeit genügt oft eine „bescheidenere“ Lösung, womöglich aus dem Freeware-Bereich.

Beispiel: Datenlieferung an Dienstleister

Sollten Sie regelmäßig Daten an externe Dienstleister zur Weiterverarbeitung liefern, bietet sich z.B. der Einsatz eines SFTP-Servers an. Das Secure File Transfer Protocol (engl. für „sicheres Dateiübertragungsverfahren“) ist allemal besser, als Dateien über ungeschützte E-Mails zu transportieren.

Verschlüsselungspflicht beim Webshop

Eine ungesicherte Verbindung vom Webshop-Server zu Ihren Kunden bei der Erhebung personenbezogener Daten sollte der Vergangenheit angehören. Ohne Verschlüsselung sind Webdaten leicht als Klartext lesbar.

Mit der Verbreitung von Funkverbindungen, die etwa an WLAN-Hotspots häufig unverschlüsselt ablaufen, nimmt die Bedeutung von HTTPS zu, da hiermit die Inhalte unabhängig vom Netz verschlüsselt werden. Es stellt dabei das einzige Verschlüsselungsverfahren dar, das ohne gesonderte Softwareinstallation auf allen internetfähigen Computern unterstützt wird.

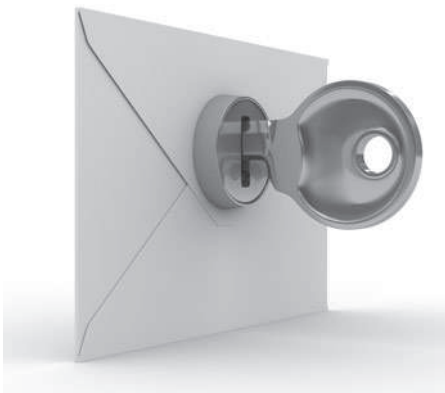
Konzentrieren Sie sich auf den häufigsten Transportweg, die E-Mail

Vielen Unternehmen wäre bereits geholfen, wenn zumindest die Übermittlung personenbezogener Daten über E-Mail einer vernünftigen Übermittlungskontrolle unterliegen würde. Leider verhindert das in der Regel die Vielzahl unterschiedlicher Mailsysteme.

Einen Ausweg zur datenschutzkonformen Übermittlung von Attachments bieten lediglich Verschlüsselungsprogramme. ZIP, RAR & Co. schützen bei Bedarf vertrauliche Daten, sofern die Anwender ein vernünftiges Passwort einsetzen.

Zumindest vertrauliche Dokumente schützen!

Die Mitarbeiter sollten zumindest den in Microsoft-Produkten implemen-



Die Verschlüsselung von E-Mails ist eines der zentralen Elemente der Weitergabekontrolle

tierten Dokumentschutz verwenden. Er ist zwar anfällig, was das Passwortcracking betrifft – aber besser als nichts.

Gesicherter Medientransport

Nicht alle Daten lassen sich über elektronische Medien zustellen. Es gibt recht häufig noch Bereiche, in denen Datenträger wie Disketten, CD/DVD, Backup- oder Papiermedien Verwendung finden. Kontrollieren Sie daher unbedingt die folgenden Bereiche:

- Transport von Backup-Medien zum Bankschließfach
- Datenbankkopien auf DVD, die an Dienstleister zur Fehleranalyse gehen
- Datenaustausch an Steuerberater oder Wirtschaftsprüfer z.B. per USB-Stick
- Weitergabe eines Aktenarchivs an Dienstleister zur datenschutzkonformen Vernichtung

Wie steht es eigentlich um den internen Datenfluss?

Die Weitergabekontrolle betrifft nicht nur den externen Datenfluss. Doch bisher wird das innerbetriebliche Übermittlungsgebot in den meisten Unternehmen kaum beachtet.

Fundgrube öffentliche Laufwerke

In der Regel wird in jeder Netzwerkumgebung im Unternehmen ein sogenannter Public-Bereich freigegeben. Er soll einen einfachen Daten- und Informationsaustausch zwischen den Abteilungen ermöglichen.

So weit, so gut – aber was findet man alles auf öffentlichen Laufwerken: Zeit- und Überstundenaufstellungen, Geburtstagslisten oder schon mal einen Textvorschlag zu einer bevorstehenden Abmahnung eines Mitarbeiters. Von vertraulichen Unterlagen einzelner Bereiche ganz zu schweigen.

Es bleibt doch in der „Familie“ …

Die Standardargumentation „Es bleibt doch alles in der Familie“ können Sie als DSB nicht gelten lassen. Sofern es sich um personenbezogene Daten handelt, die lediglich zur Aufgabenerfüllung in bestimmten Bereichen eingesetzt werden sollen, dürfen sie keinesfalls in einem öffentlichen Ordner zur allgemeinen Verfügung stehen.

Interne Datenübermittlung: Verschlüsselung unter IBM/Lotus Domino Notes

Auch in der internen E-Mail-Kommunikation lässt sich in vielen Fällen ein vernünftiger Schutz der Informationen relativ leicht bewerkstelligen. Als Beispiel sei auf die E-Mail-Verschlüsselung unter Lotus Notes hingewiesen. Hier reicht ein Klick unter „Zustelloptionen“ und „Verschlüsseln“, um der Weitergabekontrolle zu genügen.

Gehen Sie mit gutem Beispiel voran

Gehen Sie unbedingt mit gutem Beispiel voran: Lassen Sie sich Informationen für Ihre Datenschutzaktivitäten grundsätzlich sicher, d.h. verschlüsselt, zusenden!

Hermann Keck

Maßnahmen zur Weitergabekontrolle	Erfüllt	
	Ja	Nein
Ist festgelegt, welche Datenarten der Weitergabekontrolle unterliegen?	☐	☐
Findet die Datenübermittlung über eine gesicherte Verbindung statt?	☐	☐
Werden die Daten nur in anonymisierter oder pseudonymisierter Form weitergegeben?	☐	☐
Sind die Daten kryptografisch verschlüsselt?	☐	☐
Findet der Datentransfer über gesicherte Webverbindungen statt (https/SFTP)?	☐	☐
Checkliste für den physischen Datentransport:		
Ist ein zuverlässiges Transportunternehmen beauftragt?	☐	☐
Sind die Transportfahrzeuge sicher?	☐	☐
Gibt es sichere Transportbehälter?	☐	☐
Sind die Begleitpapiere o.k.?	☐	☐
Existiert ein Aus-/Eingangsprotokoll?	☐	☐
Kann der Empfänger seine Identität nachweisen?	☐	☐
Kontrollpunkte für elektronische Übermittlung z.B. via E-Mail:		
Ist mit dem mit Empfänger ein kryptografisches Verfahren abgestimmt?	☐	☐
Sind die Attachments verschlüsselt?	☐	☐
Sind ausreichend sichere Kennwörter im Einsatz?	☐	☐
Fand vor dem Mailversand eine Empfängerkontrolle/ein Adresscheck statt?	☐	☐
Existieren getrennte Wege zur Kennwortübermittlung?	☐	☐

Standardmöglichkeiten für eine datenschutzkonforme Datenweitergabe. Sie finden die Checkliste unter www.datenschutz-praxis.de/fachwissen/vorlagen/checklisten.