

Informationsblatt 3-11/08

Wann Sie in ihrem Unternehmen Daten verschlüsseln sollten

Schon die alten Römer wussten die Verschlüsselung zu nutzen. Julius Cäsar nutzte verschlüsselte Botschaften für seine militärische Kommunikation. Bei ihm kam der so genannte Verschiebealgorithmus zum Einsatz. Bei dieser Methode werden alle Buchstaben um 3 Plätze im Alphabet verschoben. So wird aus „ABCDE“ die Buchstabenfolge „DEFGH“, aus dem Begriff „AUTO“ entsteht „DXWR“.

Diese Verschlüsselungstechnik ist heute natürlich nicht mehr zeitgemäß, aber der Einsatz von Verschlüsselung ist bei bestimmten Einsatzgebieten aus Gründen des Datenschutzes heute mehr den je notwendig und auch vorgeschrieben.

Nutzen Sie die folgenden 6 Prüfpunkte, um zu untersuchen, ob in Ihrem Unternehmen die Verschlüsselung von Daten überall dort, wo sie notwendig ist, zum Einsatz kommt.

Die gesetzlichen Anforderungen

Personenbezogene Daten werden auf Laptops, USB-Sticks, CD-ROMs etc. transportiert und über VPN-Verbindungen, ISDN-Leitungen etc. weitergeleitet. Bei diesen Übertragungen muss sichergestellt sein, dass die Daten nicht „unbefugt“ gelesen, kopiert, verändert oder entfernt werden können ... Dies wird im Rahmen der Weitergabekontrolle (Nr. 4 der Anlage zu §9 Satz 1 BDSG) gefordert. Um dies zu erreichen, stellt die Nutzung der Verschlüsselung ein adäquates Mittel dar.

Die praktische Umsetzung

Im Wesentlichen müssen Sie in Ihrem Unternehmen in den folgenden Anwendungsgebieten prüfen, ob eine Verschlüsselung notwendig oder sinnvoll ist:

Prüfpunkt 1: E-Mail

Sprechen Sie mit den Abteilungen, die bevorzugt personenbezogene Daten bearbeiten oder nutzen, ob diese solche Daten per E-Mail versenden oder dies planen. Bringen Sie hier in Erinnerung, dass jede über das Internet versendete E-Mail den Status einer „Postkarte“ hat.

Aus diesem Grund sollten per E-Mail versendete personenbezogene Daten grundsätzlich verschlüsselt werden. Suchen Sie gemeinsam mit der IT-Abteilung technische Lösungen. Bei regelmäßigen Übertragungen lohnt sich die Implementierung einer Public-Key-Infrastruktur,

PC KLINIK MOSEL, Moselstr. 25, 56841 Traben-Trarbach

DE 253124234

Abteilung Datenschutz info@datenschutzbeauftragter-mosel.de Tel. 06541 814422

Fax 040 38017859756

Bankverbindung: Kontonr. 5852798 BLZ 58760954 Raiffeisenbank Bernkastel-Kues

sofern die Übertragung regelmäßig nur von einer Person durchgeführt wird, die Installation einer Client-Software auf einem Arbeitsplatz.

Prüfpunkt 2: WLAN

Die Übertragung von Daten über ein Wireless LAN ist immer zu verschlüsseln. Achten Sie hier darauf, dass möglichst nur WPA (Wi-Fi Protected Access) eingesetzt wird. Für die hierzu notwendiger Erstauthendifizierung wird bei kleineren oder mittleren Unternehmen mit Pre-Shared Keys gearbeitet.

Hierbei müssen sichere Passwörter verwendet werden. Deshalb sollte die maximale Passwortlänge von 63 Zeichen ausgenutzt und eine möglichst unsinnige Kombination von Buchstaben, Zahlen und Sonderzeichen eingesetzt werden, um Angriffe über Wörterbücher oder Brute-Force-Angriffe (dem Ausprobieren sämtlicher Buchstabenkombinationen) zu erschweren.

Prüfpunkt 3: Backup

Sofern Backup-Medien Ihres Unternehmens extern gelagert werden, müssen Sie sich über den Transportweg Gedanken machen. Hier bietet es sich an, neben einer physikalischen Sicherung der Datenträger (in einem abgeschlossenen Transportbehälter) die Daten auf diesen Bändern ausschließlich verschlüsselt abzulegen. Achten Sie aber hier darauf, dass nach einem Katastrophenfall diese Bänder auch wieder genutzt werden können. So müssen für diesen Fall auch die für die Entschlüsselung notwendige Software, Schlüssel etc. verfügbar sein.

Prüfpunkt 4: Internet/Intranet

Testen Sie sowohl das Intranet- als auch das Internetportal des Unternehmens. Sobald personenbezogene Daten (beispielsweise in Kundenformularen, Bewerbungsformularen etc.) abgefragt werden, sollten diese Seiten über eine SSL-Verbindung verschlüsselt sein. Diese Verschlüsselung erkennen Sie durch die Voranstellung von https:// in der Adresszeile oder an einem kleinen Schloss unten rechts in Ihrem Internet-Browser.

Prüfpunkt 5: Laptops/PDAs

Bei der Vielzahl der jährlich gestohlenen oder vergessenen Geräte sollten Sie auf eine Verschlüsselung dieser Ausrüstung hinwirken. Bringen Sie sich hier schon in den Beschaffungsprozess mit ein, da viele Hersteller entsprechende Technik bereits in der Hardware integriert mitliefern können. Gegebenfalls können Sie auch den Einsatz von Betriebssystemen mit integrierter Verschlüsselung (z.B. Microsoft Windows Vista Ultimate) vorschlagen.

Prüfpunkt 6: Sonstige Übertragungen

In vielen Unternehmen gibt es noch weitere Übertragungen personenbezogener Daten (beispielsweise an Dienstleister, externe Steuerbüros, o.Ä.). Fragen Sie Ihre IT-Abteilung nach einer Aufstellung der von ihr eingerichteten Übertragungen und prüfen Sie für jeden Übertragungsweg ab,

PC KLINIK MOSEL, Moselstr. 25, 56841 Traben-Trarbach

DE 253124234

Abteilung Datenschutz info@datenschutzbeauftragter-mosel.de Tel. 06541 814422

Fax 040 38017859756

Bankverbindung: Kontonr. 5852798 BLZ 58760954 Raiffeisenbank Bernkastel-Kues

Zertifizierter Datenschutzbeauftragter (FH) Elmar Hilgers

Wildbadstr. 93 56841 Traben-Trarbach

www.datenschutzbeauftragter-mosel.de

- ob personenbezogene Daten übertragen werden – fragen Sie hierzu nach dem Zweck der Übertragung – und
- ob diese Übertragung verschlüsselt erfolgt.

Prüfpunkt 7: Arbeitsanweisungen

Die in den ersten 6 Prüfpunkten genannten Einsatzbereiche von Verschlüsselungstechniken können nicht immer durch technische Rahmenbedingungen vorgegeben werden. So sollten Sie auf die Vereinbarung entsprechender Arbeitsanweisungen hinwirken bzw. vorhandene überprüfen, mit denen etwa:

- die jeweiligen Mitarbeiter verpflichtet werden, personenbezogene Daten ausschließlich verschlüsselt per E-Mail zu versenden,
- Die Mitarbeiter der IT-Abteilung zum Einsatz einer Verschlüsselung bei Backup-Medien, Laptops, PDAs, WLAN, VPN usw. angewiesen werden,
- Die Empfänger von portablen Geräten auf die Nutzung einer Verschlüsselung verpflichtet werden.

PC KLINIK MOSEL, Moselstr. 25, 56841 Traben-Trarbach

DE 253124234

Abteilung Datenschutz info@datenschutzbeauftragter-mosel.de Tel. 06541 814422

Fax 040 38017859756

Bankverbindung: Kontonr. 5852798 BLZ 58760954 Raiffeisenbank Bernkastel-Kues