

Technisch-organisatorische Sicherungsmaßnahmen (Fernzugriff):

- Einmalpasswort mit Verschlüsselung
- Verschlüsselte Übertragung (VPN)
- Protokollierung der Handlungen

Technisch-organisatorische Verfügbarkeitskontrolle (Bsp.: Datenbank):

- USV
- Plattenspiegelung
- Clustern
- Regelmäßige Backups
- Transaktionskontrolle
- Dynamische Bestandssicherung (RAID)

Unternehmer will Mitarbeitern Nutzung vom privaten Internet erlauben. Gesetze:

- Telekommunikationsgesetz (TKG)
- Telemediengesetz (TMG)
- Strafgesetzbuch (StGB)
- Jugendschutzgesetz
- Urheberrechtsgesetz
- Betriebsverfassungsgesetz
- Fernmeldegesetz

Wer muss informiert werden, wenn Nutzung von privatem Internet:

- IT-Sicherheitsbeauftragter
- Betriebsrat
- Mitarbeiter

Sicherheitsrisiken bei privater Internetnutzung in einem Unternehmen:

- Unkontrollierte Daten nach Außen
- Überlastung
- Unlizenzierte Software
- Geheimnisverrat
- Vergeudung von Arbeitszeit (Verfügbarkeitsprinzip)
- Fahrlässiges und auch vorsätzliches Handeln der Mitarbeiter
- Schadenstiftende Software (Viren, Würmer, Trojaner, SPAM)
- Cookies

Sicherheitsmaßnahmen um Internet Risiken zu mindern:

- Viren-, Spam, Paket-, Contentfilters
- Firewall, Portsperrung
- Ausgefeilte Zugangs- und Zugriffssicherung
- Ausgewogenes Bestands- und Wiederanlaufkonzept

Zu beachtende Gesetze bei Schaffung von privater Internet-Nutzung am Arbeitsplatz:

Wer muss informiert werden?

- IT-Sicherheitsbeauftragter
 - Betriebsrat
 - Mitarbeiter
-
- § 9 BDSG Technische und organisatorische Maßnahmen
 - § 88 TKG Fernmeldegeheimnis
 - § 109 TKG Technische Schutzmaßnahmen
 - §§ 13, 14, 15 TMG
 - BetrVG

Private Nutzung von Internet am Arbeitsplatz (mit Protokollierung):

- Die Mitarbeiter müssen in die Auswertung der Protokollierung einwilligen nach Fernmeldegeheimnis (Fernmeldegesetz). Außerdem BR informieren und gegebenenfalls eine Betriebsvereinbarung über die private Nutzung des Internets abschließen. Der Betriebsrat hat nach (§ 87) BetrVG Mitbestimmungsrecht.

Dienstliche Nutzung von Internet am Arbeitsplatz (mit Protokollierung):

- Um Einsicht in die Protokolldatei zu erlangen ist die Zustimmung des Betriebsrates notwendig.

Verweigerung zur Verpflichtung aufs Datengeheimnis. Was kann man tun?

- Schulung/Unterweisung und Unterschrift unter Teilnehmerliste,
- Zeugenregelung.
- Jemanden von seiner Funktion zu entbinden sollte das letzte Mittel sein und ist eigentlich unangemessen.

Gesetzliche Basis zur Gestaltung einer Internet Seite:

- S.37 (mitte)

Kontrollrecht von Vorgesetzten:

- Vorgesetzte haben Zugriffskontrolle (z.B.: über eine Berechtigungstabelle). Die Zugangskontrolle unterliegt jedoch den untergebenen Mitarbeitern des Vorgesetzten. Geregelt nach § 9 BDSG. Will der Vorgesetzte die Passworte zur Kontrolle von seinen Mitarbeitern erfahren, dann droht im nach § 43 (2) ein Bußgeld, da die Erhebung und Verarbeitung von personenbezogenen Daten, die nicht allgemein frei zugänglich sind nicht rechtmäßig ist.

Sicherheitsmaßnahmen bei Notebooks:

- NB sicher verwahren, nicht liegen lassen.
- NB nicht im heißen oder kalten Kofferraum liegen lassen.
- NB nur mit Benutzerkennung und qualifiziertem Passwort nutzen.
- Pausenschaltung ordnungsgemäß.
- Unbefugte Nutzung durch Dritte ausschließen.
- Keine private SW speichern.
- Keine privaten Daten speichern.
- Keine private Internetnutzung.

- Antiviren-SW-Pflege.
- Tägliche Bestandssicherung.
- Reparaturaufträge nicht selbst erteilen.
- Betriebliche Kontrollen zulassen (Vorgesetzter, IT, DSB, AB).
- Serveran kopplung nur über vorgeschriebenen Pfad.
- BIOS Passwort setzen.
- Transponderkarte
- Nur vorgeschrieben Übertragungskanal nutzen (z.B. VPN)

Personbezogene Daten über Internet verschlüsseln?

- Ohne Verschlüsselung sind Daten im Internet von jedem frei mit lesbar. Z.B. mit Hilfe eines Paket-Sniffers. Daher müssen personbezogene Daten vor Mißbrauch verschlüsselt werden. Hierzu gibt es verschiedene Methoden. Z.B. Symmetrische sowie asymmetrische Verfahren.

Checkliste DSB zur Durchführung der Auftragskontrolle:

- Klare Vertragsgestaltung
- Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und Auftraggeber
- Sorgfältige Auswahl des Auftragnehmers
- Definition von Sicherheitsmaßnahmen
- Kontrolle der ordnungsgemäßen Vertragsausführung

Von Max:

- Auftrag in Schriftform (§ 11 (2) BDSG)
- alle DS-relevanten Aspekte in Auftrag behandelt (§ 11 (2) BDSG)
- Auftragnehmer hat ausreichende technisch-organisatorische Maßnahmen getroffen (§ 11 (2) BDSG)
- persönliche Kontrolle vor Ort (§ 11 (2) BDSG)
- Berichtswesen bei etwaigen Verstößen (§ 11 (3) BDSG)
- ständige Wiederholung der Kontrolle (da Verantwortlichkeit beim Auftraggeber)

Ist eine Arzthelferin einer Zahnarztpraxis auf das Datengeheimnis gem. BDSG zu verpflichten, obwohl nur drei Personen in der Praxis tätig sind und der Arzt meint, die Verpflichtung auf § 203 StGB würde ausreichen? Begründung!

- Die ärztliche Schweigepflicht (§2 der Berufsordnung für Ärzte - gilt auf für "Gehilfen", § 203 StGB) deckt einige Anforderungen des BDSG nicht ab (Speicherung und Verarbeitung - abgedeckt ist allerdings die Weitergabe). Daher ist eine Verpflichtung auf das Datengeheimnis § 5 BDSG unerlässlich.
- s. Skript S. 32 (Subsidiaritätsprinzip)