

Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 5. Übung im SoSe 2012:
Konzepte zur IT-Sicherheit

5.1 Gegensätze von Datenschutz und IT-Sicherheit

Aufgabe:

- Welche **Gegensätze** sehen Sie zwischen den Anforderungen zum Datenschutz und zur IT-Sicherheit? Begründen Sie Ihre Antwort.

5.1 Gegensätze von Datenschutz und IT-Sicherheit

- **Datenschutz:** Grundsatz der Datensparsamkeit
IT-Sicherheit: Redundante Datensicherung zur Ausfallsicherheit
- **Datenschutz:** Informationelles Selbstbestimmungsrecht
IT-Sicherheit: Nachvollziehbarkeit und Überwachung von Aktionen
- **Datenschutz:** Transparenz der Verfahren
IT-Sicherheit: Verschleierung von Sicherheitsmechanismen
- **Datenschutz:** Inhaltsebene der Daten im Vordergrund
IT-Sicherheit: Transportebene der Daten im Vordergrund
- **Datenschutz:** Schutzbereich personenbezogene Daten
IT-Sicherheit: Schutzbereich alle (Unternehmens-)Daten
- **Datenschutz:** Vertraulichkeit zentral
IT-Sicherheit: Vertraulichkeit nur ein Ziel unter vielen
- **Datenschutz:** Ausgangspunkt = Interesse von Betroffenen
IT-Sicherheit: Ausgangspunkt = Interesse von Systembetreibern

5.2 Sicherheitskonzept Telearbeit

Aufgabe:

- Entwerfen Sie ein **Sicherheitskonzept** zur Nutzung von Laptops, mit denen im Zuge von Telearbeit (Home Office oder Außendienst) auch vertrauliche Daten bearbeitet und an den eigentlichen Unternehmensstandort übertragen werden!

5.2 Sicherheitskonzept Telearbeit (1)

- Festplatte des Laptops gemäß dem Stand der Technik verschlüsseln
- systemseitiges Abklemmen externer Laufwerke & Wechseldatenträger; Einrichtung eines Boot-Schutzes
- kein Zugriff auf Betriebssystemebene und Konfigurationen der eingesetzten IT-Komponenten (→ Nutzerrechte, keine Admin-Rechte)
- vorzugsweise Identifizierungs- und Authentisierungsmechanismus mittels Smartcard- oder Fingerabdruckverfahren
- monatliche Änderung der Zugangs- und Zugriffspassworte durch den Beschäftigten unter Einhaltung der Komplexitätsvorschriften
- Erschwerung mehrfach missglückter Neuanmeldeversuche (durch Geringhalten zulässiger Fehlversuche und sukzessive Erhöhung der Zeitabstände für erneute Versuche)
- Automatische Bildschirmsperre bei fehlender Aktivität von 10 Minuten und deren Aufhebung nur mittels Authentifizierung

5.2 Sicherheitskonzept Telearbeit (2)

- Konfiguration minimal entsprechend der zu erfüllenden Aufgaben
- Protokollierung aller sicherheitsrelevanten Aktivitäten
- Virens Scanner so installieren, dass dieser bei jeder Anmeldung am LAN und in regelmäßigen Abständen auch während einer bestehenden Verbindung automatisch aktualisiert wird
- Freischaltung nur der zur Aufgabenerfüllung zwingend erforderlichen Ports
- Kommunikation zwischen Laptop und LAN nur unter Ausnutzung einer dem Stand der Technik entsprechende starke Transportverschlüsselung (üblicherweise Triple-DES); ein Verbindungsaufbau darf nur nach ausdrücklicher Bestätigung durch den Beschäftigten erfolgen
- Absicherung einer erfolgreichen Datenübertragung mittels Quittierungsverfahren

5.2 Sicherheitskonzept Telearbeit (3)

- zur Telearbeit dürfen ausschließlich gestellte IT-Komponenten (Hardware und Software) eingesetzt, an den Einstellungen keine Änderungen vorgenommen und keine weiteren IT-Komponenten angeschlossen werden
- Zutrittsrecht des Arbeitgebers zum Telearbeitsplatz ist mit dem Beschäftigten zu vereinbaren
- Laptop ist in einem klar separierten und verschließbaren Arbeitszimmer so aufzustellen, dass keine unbefugte Einsichtnahme auf den Bildschirm (weder im Zuge des Betretens des betreffenden Arbeitszimmers noch durch Beobachtung durch etwaige Fenster) stattfinden kann
- vertrauliche Unterlagen dürfen außerhalb der Arbeitszeit bzw. Tätigkeit des betreffenden Beschäftigten ausschließlich in verschließbaren Behältnissen gelagert werden

5.3 Notfall-Vorsorge-Konzept

Aufgabe:

- Welche Bestandteile sollte ein **Notfall-Vorsorge-Konzept** bei einem mittelständischen Unternehmen Ihrer Ansicht nach auf alle Fälle beinhalten? Sehen Sie sich hierzu die entsprechenden Ausführungen in den BSI-Grundschutzkatalogen bzw. den BSI-Standards auf www.bsi.de an und wählen Sie begründet aus.

5.3 Notfall-Vorsorge-Konzept (1)

Ein Notfallvorsorgekonzept beschreibt, wie das Eintreten eines Notfalls vorzugsweise verhindert werden kann/soll → **präventiver Schutz**

- Komplettes Notfallmanagement ist auf den BSI-Seiten beschrieben im **BSI-Standard 100-4** (abrufbar unter:
https://www.bsi.bund.de/cae/servlet/contentblob/471456/publicationFile/31045/standard_1004.pdf)
- Darin **Kapitel 5.5 Notfallvorsorgekonzept** auswerten
- **Bestandteile** (Inhalt des Notfallvorsorgekonzepts):
 - Verantwortlichkeiten, Geltungsbereich, Inhaltsangabe
 - Abgrenzungen, Ziele, Zuständigkeiten, Ablauforganisation
 - betrachtete Notfallszenarien, Wiederanlauf-Anforderungen, Priorisierungen
 - Alarmierungsverfahren, Beschreibung vorbeugender Maßnahmen
 - Einbinden des Notfallmanagements in Unternehmenskultur
 - Aufrechterhaltung & Kontrolle

5.3 Notfall-Vorsorge-Konzept (2)

Ein mittelständisches Unternehmen wird sich auf Kernfragen konzentrieren

- In Grundschatzkatalogen nach Notfallmanagement suchen
- **Baustein 1.3 zum Notfallmanagement** wählen (abrufbar unter:
https://www.bsi.bund.de/cln_183/sid_AB2A5EAB735FF0FE0D1D3C525AB43C3D/ContentBSI/grundschatz/kataloge/baust/b01/b01003.html)
- Im Baustein 1.3 lediglich Maßnahmen der Kategorie A (Einstieg in Grundschatz) auswählen (M 6.111 zur Leitlinie, M 6.112 zur Organisationsstruktur, **M 6.114 Notfallkonzept** & M 6.118 Aufrechterhaltung des Notfallmanagements)

Bestandteile eines Notfallvorsorgekonzepts nach M 6.114:

- Übersicht zu Verfügbarkeitsanforderungen (maximal tolerierbare Ausfallzeiten, Wiederanlaufparameter, Prioritäten für Wiederanlauf)
- Vorgehen zur Durchführung einer Business Impact Analyse (BIA) & einer Risikoanalyse
- Auflistung der Maßnahmen zur Risikobehandlung

5.4 Notfallplan

Aufgabe:

- Welche Bestandteile sollte dagegen ein **Notfallplan** aufweisen?
Begründen Sie Ihre Antwort!

5.4 Notfallplan

Ein Notfallplan beschreibt, was bei Eintritt eines Notfalls zu tun ist!

→ **reaktiver Schutz**

→ Notwendige **Bestandteile** eines Notfallplans:

- Zielsetzung des Notfallplans und ggf. geltende Abgrenzungen (hinsichtlich des Scope)
- Festlegung der Verantwortlichkeiten (wer macht was?)
- Aufstellung des Alarmierungsplans (wer ist wann anzurufen?)
- Ablaufpläne für entsprechende Notfallszenarien (im Sinne von Checklisten)
- Dokumentationen zur eingesetzten IT-Infrastruktur und den Maßnahmen zur Notfall-Vorsorge
- Bereitstellung aller wesentlichen Unterlagen und Nachweise (z.B. zu durchgeführten Notfall-Übungen)

5.5 Verfügbarkeitsberechnung

Aufgabe:

- Die **Verfügbarkeit** eines IT-Systems kann als das Produkt der Verfügbarkeiten ihrer jeweiligen Komponenten verstanden werden, sofern diese Komponenten seriell miteinander verbunden sind. Diese werden unter Berücksichtigung etwaiger Ausfallzeiten in % gegenüber der vereinbarten Servicezeit berechnet:

$$\text{Verfügbarkeit einer IT-Komponente} = \frac{(\text{vereinbarte Servicezeit} - \text{Ausfallzeit})}{\text{vereinbarte Servicezeit}} \text{ [in \%]}$$

- Wenn hingegen Komponenten eines IT-Systems parallel betrieben werden, erhöht sich die Verfügbarkeit für diesen technisch redundanten Cluster in Abhängigkeit zur Anzahl der technisch redundant ausgelegten IT-Komponenten auf:

$$\text{Redundanz-Verfügbarkeit} = 1 - (1 - \text{Verfügbarkeit}_{\text{normal}})^{\text{Anzahl}}$$

- A) Das zu betrachtende IT-System bestehe aus einem Server, der während der Betriebszeit zu 8 Stunden pro Jahr ausfällt, einem Client, der dabei zu 16 Stunden pro Jahr ausfällt, und einer Vernetzungskomponente, die während des Betriebs zu 24 Stunden pro Jahr ausfällt. Als Servicezeit sei ein 12-Stunden-Betrieb von Montag bis Freitag vereinbart worden. Wie hoch ist die Verfügbarkeit jeder einzelnen Komponente und des gesamten IT-Systems?
- B) Wie wirkt sich es sich auf die Verfügbarkeit des gesamten IT-Systems aus, wenn die Vernetzungskomponente mit einer identisch konfigurierten weiteren geclustert wird? Die Prozentangaben sind dabei auf drei Nachkommastellen anzugeben (also 12,345%).

5.5 Verfügbarkeitsberechnung

Teil A)

$$V_{\text{server}} = (12 \cdot 5 \cdot 52 - 8) / (12 \cdot 5 \cdot 52) = 3112 / 3120 = 99,744\%$$

$$V_{\text{client}} = (12 \cdot 5 \cdot 52 - 16) / (12 \cdot 5 \cdot 52) = 3104 / 3120 = 99,487\%$$

$$V_{\text{netz}} = (12 \cdot 5 \cdot 52 - 24) / (12 \cdot 5 \cdot 52) = 3096 / 3120 = 99,231\%$$

$$V_{\text{gesamt}} = V_{\text{server}} \cdot V_{\text{client}} \cdot V_{\text{netz}} = 99,744\% \cdot 99,487\% \cdot 99,231\% = 98,469\%$$

Teil B)

$$V_{\text{netzcluster}} = 1 - (1 - V_{\text{netz}})^2 = 1 - (1 - 0,99231)^2 = 99,994\%$$

$$\begin{aligned} V_{\text{gesamt_neu}} &= V_{\text{server}} \cdot V_{\text{client}} \cdot V_{\text{netzcluster}} = \\ &99,744\% \cdot 99,487\% \cdot 99,994\% \\ &= 99,226\% \end{aligned}$$