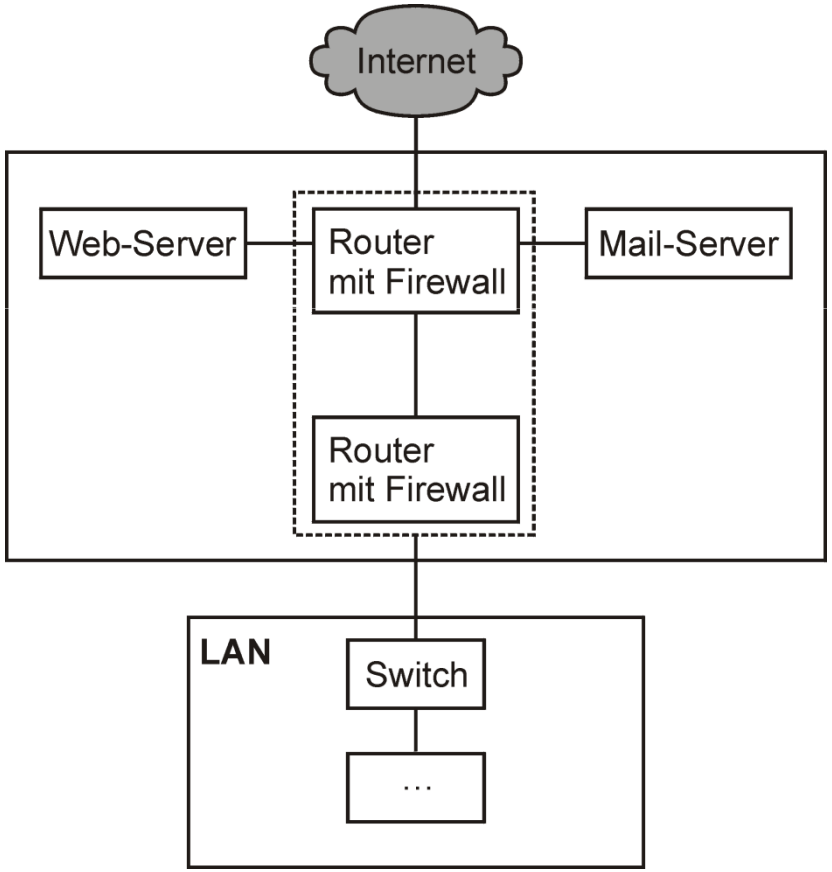
Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 8. Übung im SoSe 2008:
Konzeption von IT-Sicherheit

8.1 DMZ


Internet
Web-Server
Router
mit Firewall
Mail-Server
Router
mit Firewall
LAN
Switch
...

8.2 Notfall-Vorsorge-Konzept

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

Ein mittelständisches Unternehmen wird sich auf Kernfragen konzentrieren → Baustein 1.3, Maßnahmen der Kategorie A (Einstieg in Grundschutz)

Bestandteile eines Notfallvorsorgekonzepts folglich:

- Übersicht zu Verfügbarkeitsanforderungen (M 6.1 unter Festlegung maximal tolerierbarer Ausfallzeiten der eingesetzten IT-Infrastruktur)
- Definition eines Notfalls & Festlegung von Verantwortlichkeiten (M 6.2 & M 6.7)
- Festlegung Alarmierungsplan (M 6.8)
- Aufstellung des Datensicherungsplans (M 6.13 → Disaster Recovery mittels Back-Up-Konzept [inkl. Konfigurationen!] & Redundanzkonzept unter Beachtung von Baustein 1.4 Datensicherungskonzept)

8.3 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)

8.4 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 Administrationsrechte)
- 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

8.4 Sicherheitskonzept Telearbeit (2)

- Konfiguration minimal entsprechend der zu erfüllenden Aufgaben
- Protokollierung aller sicherheitsrelevanten Aktivitäten
- Virenscanner so installieren, dass dieser bei jeder Anmeldung am LAN und in regelmäßigen Abständen auch während einer bestehenden Verbindung automatisch aktualisiert wird
- kein freier Zugriff auf das Internet
- 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

8.4 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
- streng vertrauliche Unterlagen dürfen außerhalb der Arbeitszeit bzw. Tätigkeit des betreffenden Beschäftigten ausschließlich in verschließbaren Behältnissen gelagert werden

8.5 PDCA-Vorgehen bei der Erstellung des IT-Sicherheitskonzepts (1)

PLAN:

- Festlegung der Zielsetzung und der Abgrenzung des Sicherheitskonzepts (Scope)
- Festlegung der zugrunde liegenden Vorgehensweisen und Methodiken (insb. welche Methoden beim Risk Assessment angewandt werden sollen)
- Ermittlung der zu schützenden Vermögenswerte (Assets)
- Bestimmung der Kritikalität (und Wertigkeit) der Assets
- Durchführung des Risk Assessments, um das aktuelle Risiko der Assets bestimmen zu können
- Festlegung der Gegenmaßnahmen und Prüfsteine, um das festgestellte Risiko auf ein akzeptables Restrisiko reduzieren zu können

→ Grundlagen ermitteln für Planung und Entwurf des Sicherheitskonzepts

8.5 PDCA-Vorgehen bei der Erstellung des IT-Sicherheitskonzepts (2)

DO:

- Erstellung des (vorläufigen) Sicherheitskonzepts und Einbettung spezifischer Sicherheitskonzepte (z.B. zur Telearbeit) in übergreifende (einrichtungsweit geltende) Sicherheitskonzepte
- Umsetzung der geplanten Gegenmaßnahmen (Basismaßnahmen, die Asset-übergreifend gelten, sowie Asset-spezifischer Maßnahmen)
- Umsetzung der vorgesehenen Prüfsteine, so dass insbesondere auch das gemessen werden kann, was gemessen werden soll
- Einstellung der entsprechenden Konfigurationen bei der IT-Infrastruktur
- Erstellung erforderlicher Handbücher
- Durchführung von Schulungsmaßnahmen und Sensibilisierung der Mitarbeiter hinsichtlich der Schutzziele

→ Umsetzung der Vorgaben aus der Planungsphase

8.5 PDCA-Vorgehen bei der Erstellung des IT-Sicherheitskonzepts (3)

CHECK:

- Auswertung der aufgetretenen Sicherheitsvorfälle (Störfälle und Notfälle) sowie der vorgenommenen Veränderungen im Rahmen des Change-Managements
- Überprüfung, ob (im Rahmen der Policies) festgelegte Prüfsteine wirkungsvoll einen Anstieg des Risikos vermieden haben
- Überprüfung, ob der umgesetzte Maßnahmenplan geeignet war, die vorab ermittelten und tatsächlich eingetretenen Risiken im geplanten Umfang zu reduzieren
- Berichterstattung über den aktuellen Stand hinsichtlich der IT Governance, des Risikomanagements und der Compliance zu allen relevanten Regelungen (Gesetze, vertragliche Vereinbarungen wie SLAs, geltende Standards, interne Richtlinien & Policies & Anweisungen)

→ Überwachung im Sinne einer Erfolgskontrolle

8.5 PDCA-Vorgehen bei der Erstellung des IT-Sicherheitskonzepts (4)

ACT:

- Feststellung über den Grad erreichter IT-Sicherheit
- Anpassung der Maßnahmenpläne, Policies und Prüfsteine aufgrund der Erkenntnisse aus der Überprüfungsphase
- Bestimmung ergänzender Kontrollmaßnahmen (z.B. in Form von Computer-Aided Audit Tools)
- Festlegung der ggf. modifizierten bzw. ergänzten Anforderungen hinsichtlich der Compliance (z.B. durch Korrektur einer bestehenden Policy oder durch Erlass einer weiteren Handlungsanweisung)
- Anpassung des bestehenden Sicherheitskonzepts, sofern erforderlich

→ Optimierung des Sicherheitsprozesses und Konsolidierung des Sicherheitskonzepts