

Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 6. Übung im SoSe 2016:
Einführung in IT-Sicherheit

6.1 Organisation von IT-Sicherheit

Aufgabe:

- Bei einem Unternehmen ist unter Verwendung des **RACI-Modells** festzulegen, welche Stelle welche Aufgabe im Rahmen der Gewährleistung von Informationssicherheit zu erfüllen hat. Erstellen Sie eine Übersicht, in der Sie typische Aufgaben zur Gewährleistung von Informationssicherheit folgenden Stellen zuweisen:
 - Geschäftsführer (in der Funktion als Chief Information Officer)
 - IT-Leiter (als Verantwortlicher für alle Aufgaben mit IT-Bezug)
 - IT-Sicherheitsbeauftragter (Manager von Informationssicherheit)
 - Systemadministrator (ausführender IT-Mitarbeiter)Berücksichtigen Sie in Ihrer Lösung nur die Kernprozesse zur Gewährleistung von Informationssicherheit, bestehend aus:
 - Einrichtung eines Informationssicherheitsmanagements (generelle Funktionsweise)
 - Umgang mit Sicherheitsvorfällen (Störungsmeldung und –beseitigung)Konzentrieren Sie sich dabei auf das Wesentliche und gehen Sie bei Ihrer Lösung von einer einfachen IT-Infrastruktur aus, weisen Sie also nur grundlegende Aufgaben zu. Beachten Sie bei Ihrer Lösung, dass niemand eine Aufgabe umzusetzen hat, der diese Aufgabe zugleich zu genehmigen hat.

6.1 Organisation von IT-Sicherheit

Aufgabe:

- Hinweis:
Beim **RACI-Modell** gibt es vier Rollen, nämlich
R = Responsible → Umsetzung einer Aufgabe
A = Accountable → Genehmigung einer Aufgabe
C = Consulted → Anhörungsinstanz bei einer Aufgabe
I = Informed → Mitteilungsempfangsinstanz bei einer Aufgabe

6.1 Organisation von IT-Sicherheit (1)

- Planung des Aufbaus eines Informationssicherheitsmanagements → Baustein 1.0 der IT-Grundschutzkataloge (Sicherheitsmanagement)
- Umgang mit Sicherheitsvorfällen → Baustein 1.8 der IT-Grundschutzkataloge (Behandlung von Sicherheitsvorfällen)
- Wesentlich: Maßnahmen der Siegelstufe A (Einstieg in IT-Grundschutz)
 - Maßnahmen 2.192, 2.335, 2.336, 2.193, 2.195, 2.197, 2.337, 2.199 zu Baustein 1.0
 - Maßnahmen 6.58, 6.121, 6.59, 6.60, 6.125, 6.64, 6.65, 6.130, 6.131, 6.132, 6.133 zu Baustein 1.8

6.1 Organisation von IT-Sicherheit (2)

Aufbau Sicherheitsmanagement	GF/CIO	IT-Leiter	IT-SiBe	Sysadmin
Erstellung der Leitlinie zur Informationssicherheit	A	C	R	I
Festlegung der Sicherheitsziele und -strategie	A	C	R	I
Aufbau der Organisationsstruktur für Informationssicherheit	A	C	R	
Erstellung des Sicherheitskonzepts	A	C	R	I
Integration der Mitarbeiter in den Sicherheitsprozess	I	R	A	I
Integration der Informationssicherheit in Abläufe & Prozesse	I	R	A	I
Aufrechterhaltung der Informationssicherheit	I	R	A	I

6.1 Organisation von IT-Sicherheit (3)

Umgang mit Sicherheitsvorfällen	GF/CIO	IT-Leiter	IT-SiBe	Sysadmin
Etablierung der Vorgehensweise zum Sicherheitsvorfallumgang	A	C	R	
Erstellung der Richtlinie zum Umgang mit Sicherheitsvorfällen	A	C	R	
Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen	A	C	R	
Festlegung von Meldewegen für Sicherheitsvorfälle	C	R	A	I
Einrichtung der Kontaktstelle zur Sicherheitsvorfallmeldung	I	R	A	I
Behebung von Sicherheitsvorfällen		A	C	R
Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen		C	A	R
Erkennen und Erfassen von Sicherheitsvorfällen		A	C	R
Qualifizieren und Bewerten von Sicherheitsvorfällen		A	C	R
Eindämmen der Auswirkung von Sicherheitsvorfällen		A	C	R
Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen		A	C	R

6.2 Bedrohungen & Verwundbarkeiten I

Aufgabe:

- Die mehrseitige IT-Sicherheit bestimmt sich anhand der Einhaltung der Sicherheitsziele:
 - Verfügbarkeit
 - Integrität
 - Vertraulichkeit
 - Zurechenbarkeit (im Sinne von Authentizität)
 - Rechtsverbindlichkeit (im Sinne von Nachweisbarkeit)

a) Konstruieren Sie je ein Beispiel für eine **Bedrohung** der einzelnen Sicherheitsziele und begründen Sie, warum die von Ihnen angegebene Bedrohung für die Gewährleistung des betreffenden Sicherheitszieles gefährlich ist!

6.2 Bedrohungen & Verwundbarkeiten II

Aufgabe:

- b) Geben Sie für ein frei gewähltes IT-System eine potentielle **Verwundbarkeit** an, über die die unter a) angegebene Bedrohung jeweils zu einer erfolgreichen Schädigung des IT-Systems bzw. der dort gespeicherten Daten führen kann!

Hinweis zu 6.2:

- *Ein Vermögenswert (**asset**), hierzu zählen u.a. IT-Systeme als Support Assets (primary assets stellen dagegen die zu schützenden Informationen dar), kann von einer Bedrohung (**threat**) erfolgreich geschädigt werden, wenn die Bedrohung eine bestehende Verwundbarkeit (**vulnerability**) des Vermögenswertes ausnutzen kann. Sicherheitsmaßnahmen (**safeguards**) verhindern die Ausnutzbarkeit entsprechender Verwundbarkeiten. Als Verwundbarkeit kann insoweit auch eine unterlassene Schutzmaßnahme angesehen werden.*

6.2 Bedrohungen & Verwundbarkeiten (1)

Bedrohung der Verfügbarkeit:

- **Denial-of-Service-Angriff** kann IT-System zur Überlastung bringen, so dass der auszuführende Dienst nicht mehr seiner eigentlichen Funktion nachkommen kann

Bedrohung der Integrität:

- **Virenangriff** kann dazu führen, dass beim Aufruf eines Files Daten verändert werden, so dass die gespeicherten Daten nicht mehr originalgetreu und unverfälscht sind

Bedrohung der Vertraulichkeit:

- Network Analyzer (**Sniffing**) können dazu genutzt werden, dass eingehender Datenverkehr unbefugt mitprotokolliert wird, so dass die gespeicherten Daten für Dritte nicht mehr geheim sind

6.2 Bedrohungen & Verwundbarkeiten (2)

Bedrohung der Zurechenbarkeit (Authentizität):

- **Session Hijacking** kann dazu führen, dass ein Angreifer eine bestehende Verbindung übernimmt und unbemerkt einen Kommunikationspartner ersetzt, so dass der Kommunikationspartner nicht korrekt erkannt wird

Bedrohung der Rechtsverbindlichkeit:

- **Web-Defacing** kann dazu führen, dass einem Angreifer unbefugt Zugriffsrechte zugebilligt werden, da der Nutzer optisch den Eindruck hat, die korrekte Web-Site geladen zu haben, so dass tatsächlich die Identität eines Kommunikationspartners nicht sicher festgestellt werden kann

6.2 Bedrohungen & Verwundbarkeiten (3)

- Eine DoS-Attacke kann z.B. bei einem Web-Server zum Erfolg führen, wenn dieser ohne Firewall betrieben wird (oder diese keine sinnvollen Regeln aufweist)
 - **Verwundbarkeit: mangelhafter Firewall-Schutz**
oder die Verbindung zum Web-Server nicht hochverfügbar ausgelegt ist
 - **Verwundbarkeit: fehlende Hochverfügbarkeit**
oder kein adäquates Berechtigungskonzept auf dem Web-Server eingerichtet wurde, indem z.B. noch Default-Passwörter vorhanden sind
 - **Verwundbarkeit: schlechtes Passwort-Management**

6.2 Bedrohungen & Verwundbarkeiten (4)

- Ein Virenangriff kann z.B. bei einem Web-Server zum Erfolg führen, wenn dieser ohne wirksamen Virenschutz betrieben wird (z.B. keine automatisierte tägliche Aktualisierung)
 - **Verwundbarkeit: unzureichender Virenschutz**
 - oder der Web-Server nicht vom LAN abgeschottet ist oder auf dem Web-Server selbst andere Tätigkeiten (z.B. Bearbeitung eingegangener Mails) ausgeführt werden
 - **Verwundbarkeit: unzureichende Netzwerksegregation**

6.2 Bedrohungen & Verwundbarkeiten (5)

- Sniffing kann z.B. bei einem Web-Server zum Erfolg führen, wenn vertraulicher Datenverkehr unverschlüsselt oder nur mäßig verschlüsselt übertragen wird
 - **Verwundbarkeit: unzureichende Transportverschlüsselung**
 - oder der Raum, in dem der Web-Server steht, nicht wirksam unterbindet, dass man sich dort einstöpseln kann
 - **Verwundbarkeit: unzureichender Zutrittsschutz**

6.2 Bedrohungen & Verwundbarkeiten (6)

- Ein Session Hijacking kann z.B. bei einem Web-Server zum Erfolg führen, wenn beim Verbindungsaufbau via TCP kein Pseudozufallszahlengenerator verwendet wird
 - Verwundbarkeit: **schwache Authentifizierung**
 - oder eine Session unbegrenzt ablaufen kann
 - Verwundbarkeit: **fehlende Timeout-Funktion**

6.3 Gegenmaßnahmen

Aufgabe:

- Geben Sie zu einem frei gewählten IT-System aufgrund der ermittelten Bedrohung und potenziellen Verwundbarkeit (= Gefahr) aus Aufgabe 6.2 geeignete **Maßnahmen** an, die dazu führen, dass das IT-System nicht mehr dieser Gefahr ausgesetzt ist.

6.3 Gegenmaßnahmen (1)

- Ein Website-Defacing kann z.B. bei einem Web-Server zum Erfolg führen, wenn ein Web-Server z.B. mittels Speicherüberlauf übernommen werden konnte
 - **Verwundbarkeit: Buffer-Overflow**
oder ein Web-Seiten-Aufruf gezielt umgeleitet wurde
 - **Verwundbarkeit: DNS-Cache-Poisoning**
(Anm.: i.d.R. zu aufwändig für Angreifer, da in vielen Fällen bereits eine Phishing-Mail ausreicht, dass auf eine manipulierte Adresse geklickt wird)

6.3 Gegenmaßnahmen (2)

Maßnahmen gegen Bedrohungen der Verfügbarkeit:

- Denial-of-Service-Angriff durch mangelhaften Firewall-Schutz
→ Web-Server in DMZ ansiedeln & Firewall-Regeln nach Stand der Technik formulieren
- Denial-of-Service-Angriff durch fehlende Hochverfügbarkeit
→ Aufbau redundanter und parallelisierter Technik, die sich vorzugsweise in getrennten Räumen befindet
- Denial-of-Service-Angriff durch schlechtes Passwortmanagement → Dienstanweisung erstellen, dass voreingestellte Start-Kennwörter stets abgeändert werden und dabei die Komplexitätsanforderungen erfüllt werden

6.3 Gegenmaßnahmen (3)

Maßnahmen gegen Bedrohungen der Integrität:

- Virenangriff durch unzureichenden Virenschutz
→ Einsatz eines mindestens tagesaktuellen Virenscanners, der automatisch vorhandene Updates von nachgewiesenen vertrauenswürdigen Webseiten herunterlädt
- Virenangriff durch unzureichende Netzwerksegregation
→ Einrichtung separierter Schutzzone, die nicht durch Regel-lücken in Firewalls (oder aus Bequemlichkeit) umgangen werden können

6.3 Gegenmaßnahmen (4)

Maßnahmen gegen Bedrohungen der Vertraulichkeit:

- Sniffing durch unzureichende Transportverschlüsselung
→ Versand vertraulicher Dokumente ausschließlich unter Ausnutzung einer Verschlüsselung nach dem Stand der Technik
- Sniffing durch unzureichenden Zutrittsschutz
→ Einrichtung einer Schutzzone für den Serverraum (und die jeweiligen Verteilerkästen/Patchschränke), so dass sichergestellt ist, dass lediglich befugte Personen Zutritt erlangen können

6.3 Gegenmaßnahmen (5)

Maßnahmen gegen Bedrohungen der Zurechenbarkeit:

- Session Hijacking durch schwache Authentifizierung
→ Sicherstellung, dass ein echter Pseudozufallszahlengenerator verwendet wird
- Session Hijacking durch fehlende Timeout-Funktion
→ Einrichtung einer Timeout-Funktion in der genutzten Web-Applikation

6.3 Gegenmaßnahmen (6)

Maßnahmen gegen Bedrohungen der Rechtsverbindlichkeit:

- Web-Defacing durch Buffer-Overflow
→ Abfangen von Steuerungssymbolen bei Befehlsabarbeitung und Verwendung stabiler Bibliotheksfunktionen, die nicht durch längenbedingte Angaben zu einem Überschreiben unvorherbestimmter Speicherblöcken führen
- Web-Defacing durch DNS-Cache-Poisoning
→ den eigenen DNS-Server als Secure Proxy (statt als Cache Proxy) konfigurieren

6.4 Richtlinien zur Informationssicherheit

Aufgabe:

- Zu welchen Themenbereichen sollte ein Unternehmen **Richtlinien** erlassen, um **Informationssicherheit** adressieren zu können?

Gehen Sie bei Ihrer Lösung davon aus, dass das Unternehmen Mails und Webaccess nur zu dienstlichen Zwecken gestattet und keinerlei Tätigkeiten im Home-Office erbracht werden. In den Richtlinien sollen verbindliche Vorgaben festgeschrieben werden, die die Beschäftigten zu beachten haben.

6.4 Richtlinien zur Informationssicherheit (1)

- Oberste Richtlinie ist die Richtlinie zur Informationssicherheit (Information Security Policy)
- In dieser Richtlinie werden u.a. die Control Objectives (Kontrollziele) der themenspezifischen Richtlinien / Policies benannt, damit sich diese unmittelbar aus der obersten Richtlinie ableiten
- Die oberste Richtlinie beschreibt die strategischen Ziele, die hinsichtlich der Informationssicherheit verfolgt werden, während die themenspezifischen Richtlinien / Policies die taktischen Ziele definieren.
- Die oberste Richtlinie benötigt die Verabschiedung durch die Unternehmens-/Behördenleitung

6.4 Richtlinien zur Informationssicherheit (2)

Regelungsbedürftige Themen nach der ISO/IEC 27002:2013:

1. Access Control
2. Information Classification (and Handling)
3. Physical and Environmental Security
4. End User oriented Topics (= acceptable use of assets, clear desk & clear screen, information transfer, mobile devices & teleworking, restrictions on software installations & use)
5. Backup
6. Information Transfer
7. Protection from Malware
8. Management of Technical Vulnerabilities
9. Cryptographic Control
10. Communication Security
11. Privacy and Protection of personally identifiable Information
12. Supplier Relationships

6.5 Sicherheitskonzept

Aufgabe:

- Welche Aspekte sollten in einem **Sicherheitskonzept**, das den laufenden Betrieb der IT-Infrastruktur gewährleisten soll, auf jeden Fall geregelt werden, um die gängigsten Schwachstellen abzudecken? Begründen Sie Ihre Antwort!

6.5 Sicherheitskonzept

Abwehr gängigster Schwachstellen durch folgende Controls:

- Sensibilisierung und Schulung der Mitarbeiter
- Authentisierung bei Zugang und Zugriff anhand Wissen / Besitz / Merkmal
- Aktueller Schutz vor Viren, Würmer, Trojanische Pferde etc.
- Protokollierung (→ Überwachung der Technik & Datenströme; z.B. Netzwerkmonitoring, Intrusion Detection System)
- Änderung von Produktivsystemen erst nach Erfolg bei Testsystemen
- Dokumentation von Änderungen an Systemeinstellungen
- Einrichtung eines Vulnerability Managements
- regelmäßige Kontrollen (z.B. durch Penetrationstests)

Bei Verschränkung mit Datenschutzkonzept auch Orientierung an Kontrollbereiche aus BDSG sinnvoll