Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 4. Übung im SoSe 2022:
Einführung in IT-Sicherheit

4.1 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.

4.1 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*

4.1 Organisation von IT-Sicherheit (1)

- Planung des Aufbaus eines Informationssicherheitsmanagements → Baustein ISMS.1 des IT-Grundschutzkompendiums (Sicherheitsmanagement)
- Umgang mit Sicherheitsvorfällen → Baustein DER2.3 des IT-Grundschutzkompendiums (Bereinigung weitreichender Sicherheitsvorfälle – bedarf jedoch einer Verallgemeinerung, da derzeit nur APT darin behandelt werden)
- Wesentlich: Basis-Maßnahmen, siehe https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

4.1 Organisation von IT-Sicherheit (2)

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

4.1 Organisation von IT-Sicherheit (3)

Umgang mit Sicherheitsvorfällen	GF/CIO	IT-Leiter	IT-SiBe	Sysadmin
Einrichtung Organisation zum Umgang mit Sicherheitsvorfällen	A	C	R	
Entscheidung über anzuwendende Bereinigungsstrategie	I	A	R	I
Behebung des Sicherheitsvorfalls (u.a. Isolierung betroffener Netzabschnitte, Sperrung/Änderung von Zugangsdaten)		A	C	R
Rückführung in den Produktivbetrieb nach Sicherheitsvorfällen		A	C	R

4.2 Bedrohungen & Verwundbar-keiten 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!

4.2 Bedrohungen & Verwundbar-keiten 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 4.2:

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

4.2 Bedrohungen & Verwundbar-keiten (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

4.2 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

4.2 Bedrohungen & Verwundbar-keiten (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**

4.2 Bedrohungen & Verwundbar-keiten (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**

4.2 Bedrohungen & Verwundbar-keiten (5)

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

4.2 Bedrohungen & Verwundbar-keiten (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**

4.3 Gegenmaßnahmen

Aufgabe:

- Geben Sie zu einem frei gewählten IT-System aufgrund der ermittelten Bedrohung und potenziellen Verwundbarkeit (= Gefahr) aus Aufgabe 4.2 geeignete **Maßnahmen** an, die dazu führen, dass das IT-System nicht mehr dieser Gefahr ausgesetzt ist.

4.3 Gegenmaßnahmen (1)

- Ein Website-Defacing kann z.B. bei einem Web-Server zum Erfolg führen, wenn ein Web-Server z.B. mittels Speicherüber-lauf 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)

4.3 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

4.3 Gegenmaßnahmen (3)

Maßnahmen gegen Bedrohungen der Integrität:

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

4.3 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

4.3 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

4.3 Gegenmaßnahmen (6)

Maßnahmen gegen Bedrohungen der Rechtsverbindlichkeit:

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

4.4 Sicherheitskonzept IT-Infrastruktur

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!

4.4 Sicherheitskonzept IT-Infrastruktur (1)

Abwehr gängigster Schwachstellen durch folgende Controls:

- Sensibilisierung und Schulung der Mitarbeiter, da Fehlbedienungen einerseits und unzutreffende Reaktionen auf Sicherheitsvorfälle andererseits die IT-Infrastruktur gefährden können
- Authentisierung bei Zugang und Zugriff anhand Wissen / Besitz / Merkmal, damit ein unbefugter Zugang deutlich erschwert wird
- Aktueller Schutz vor Viren, Würmer, Trojanische Pferde etc., damit zumindest bereits bekannte Malware abgewehrt werden kann
- Protokollierung (→ Überwachung der Technik & Datenströme; z.B. Netzwerkmonitoring, Intrusion Detection System), um feststellen zu können, welche Schwachstellen bisher angegriffen wurden
- Änderung von Produktivsystemen erst nach Erfolg bei Testsystemen, um Bugs rechtzeitig erkennen zu können

4.4 Sicherheitskonzept IT-Infrastruktur (2)

Abwehr gängigster Schwachstellen durch folgende Controls:

- Dokumentation von Änderungen an Systemeinstellungen, damit rekonstruiert werden kann, ab wann kein sicherer Systemzustand mehr bestanden hat
- Einrichtung eines Vulnerability Managements, um systematisch Schwachstellen ermitteln und beheben zu können
- regelmäßige Kontrollen (z.B. durch Penetrationstests), um durch Angreifersicht ermitteln zu können, welche Sicherheitslücken ausgenutzt werden können

Bei Verschränkung mit Datenschutzkonzept auch Orientierung an Gewährleistungsziele nach Art. 32 EU-DSGVO sinnvoll

4.5 Sicherheitskonzept Home Office

Aufgabe:

- Entwerfen Sie ein **Sicherheitskonzept** zur pandemiebedingten Nutzung dienstlich ausgegebener Laptops im Home Office, mit deren Hilfe auch vertrauliche Daten bearbeitet und an den eigentlichen Unternehmensstandort übertragen werden!

4.5 Sicherheitskonzept Home Office (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

4.5 Sicherheitskonzept Home Office (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
- 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

4.5 Sicherheitskonzept Home Office (3)

- Für Home Office 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 heimischen Arbeitsplatz 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