Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 4. Übung im SoSe 2010:

Datenschutz & IT-Sicherheit

4.1 Datenschutzrisiko gemäß Vorabkontrolle

Aufgabe:

- Für ein geplantes Kundenbetreuungsverfahren (alle Kunden sind Endverbraucher) mittels Web-Portal wurden seitens des Vertriebs folgende Anforderungen formuliert:
  - ° Das Web-Portal soll auf die Kundendaten des CRM-Systems automatisiert zugreifen können (sowohl lesend als auch schreibend)
  - ° Die Kunden sollen eine fortlaufende Nummer als Benutzerkennung erhalten und das Web-Portal nach Eingabe eines frei gewählten Passwortes nutzen können
  - ° Für durchgeführte Bestellungen sollen die Kunden eine Bestätigungsmail erhalten
  - ° Im Web-Portal sollen die Kunden ihre Bestellhistorie einsehen können

  Geben Sie an, welche potenziellen Datenschutzrisiken Sie im Rahmen einer Vorabkontrolle sehen, schätzen Sie die Eintrittsstufe dieser Datenschutzrisiken ab und ermitteln Sie den Handlungsbedarf gemäß der in der Vorlesung (Teil 1c) angegebenen 5x5-Risk Map. Sofern Handlungsbedarf besteht, geben Sie eine passende Maßnahme an.

4.1 Datenschutzrisiko gemäß Vorabkontrolle (1)

A) Ermittlung potenzieller Datenschutzrisiken:

- Lesender & schreibender Zugriff des Web-Portals auf CRM-System
  1. Unbeschränkter Zugriff auf alle CRM-Daten
  2. Manipulationsgefahr der CRM-Daten durch Web-Eingaben
- Benutzerkennung via fortlaufender Nummer & freie Passwortwahl
  3. Enumerative Zugangsdaten
  4. Mangelnder Zugriffsschutz bei geringer Passwortgüte
- Bestätigungsmail für durchgeführte Bestellungen
  5. Mail-Server mit Web-Portal (bzw. CRM-System) direkt verbunden
- Einsicht in Bestellhistorie via Web-Portal
  6. Unbefugter Zugriff ermöglicht Persönlichkeitsprofil

Bei 1., 2., 5. und 6. unmittelbarer Zugriff auf personenbezogenen Daten

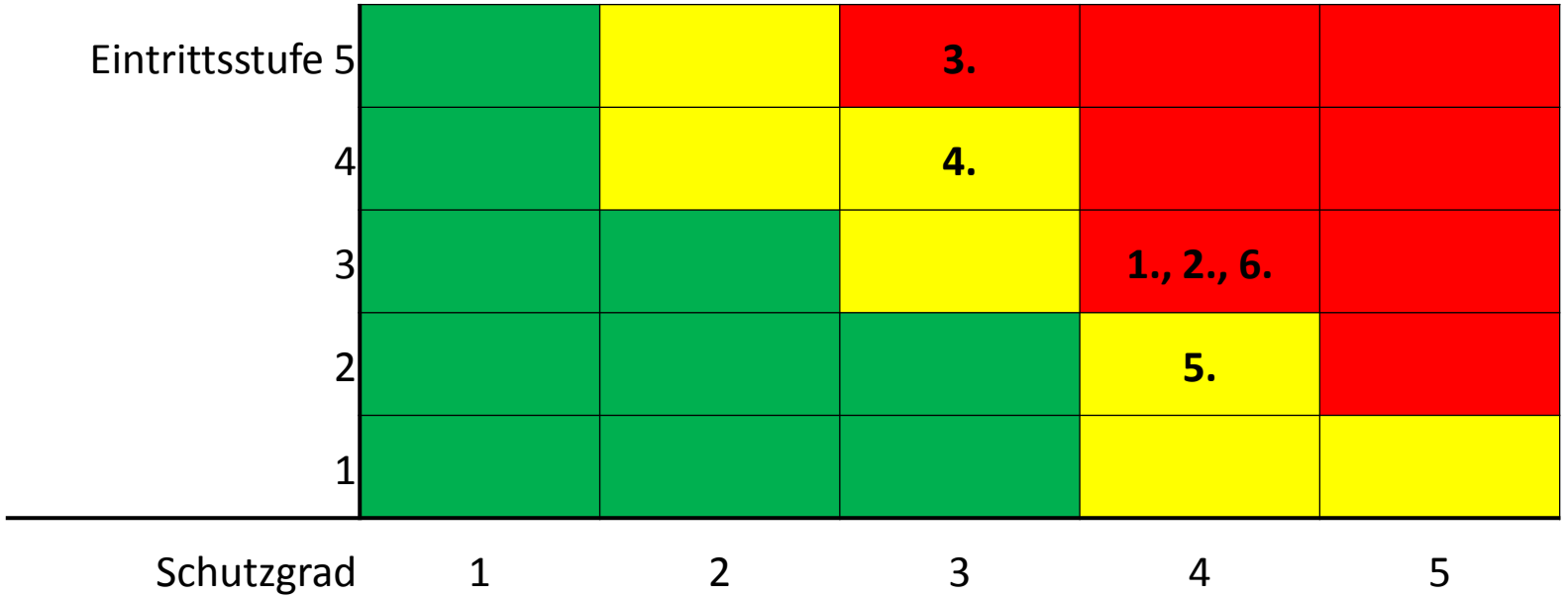
→ Schutzgrad 4; bei 3. und 4. dagegen Schutzgrad 3 (Pseudonym)

4.1 Datenschutzrisiko gemäß Vorabkontrolle (2)

B) Abschätzung der Eintriffsstufe:

1. Unbeschränkter Zugriff auf alle CRM-Daten: 3, da Angreifer über begrenzte Fähigkeiten & Ressourcen verfügen muss, um Daten z.B. via SQL-Injection abrufen zu können
2. Manipulationsgefahr der CRM-Daten durch Web-Eingaben: 3, da ebenfalls via SQL-Injection
3. Enumerative Zugangsdaten: 5, da Ausprobieren voraussetzungslos
4. Mangelnder Zugriffsschutz bei geringer Passwortgüte: 4, da Passwort-Cracker leicht downloadbar sind & schlechte Passwörter i.d.R. bereits leicht zum Erfolg führen (z.B. Benutzerkennung = Passwort)
5. Mail-Server mit Web-Portal (bzw. CRM-System) direkt verbunden: 2, da Verbindungspfad erst ermittelt werden muss
6. Unbefugter Zugriff ermöglicht Persönlichkeitsprofil: 4, wg. 3. & 4.

4.1 Datenschutzrisiko gemäß Vorabkontrolle (3)



Rot = Aktivität nötig; **Gelb** = Aktivität prüfen; **Grün** = Akzeptabel

4.1 Datenschutzrisiko gemäß Vorabkontrolle (4)

C) Handlungsempfehlung:

1. Unbeschränkter Zugriff auf alle CRM-Daten
   → Datenvalidierung sicherstellen
2. Manipulationsgefahr der CRM-Daten durch Web-Eingaben
   → Schreibenden Zugriff auf CRM unterbinden
3. Enumerative Zugangsdaten
   → Benutzerkennung frei wählen lassen
4. Mangelnder Zugriffsschutz bei geringer Passwortgüte
   → Mindestvorgaben für Passwortgüte festlegen
5. Mail-Server mit Web-Portal (bzw. CRM-System) direkt verbunden
   → ggf. akzeptierbar
6. Unbefugter Zugriff ermöglicht Persönlichkeitsprofil
   → nach Änderung zu 3. & 4. ggf. akzeptierbar

4.2 Beispiele für Bedrohungen der IT-Sicherheit

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)
  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 Beispiele für Bedrohungen der IT-Sicherheit (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 Beispiele für Bedrohungen der IT-Sicherheit (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 Kommunikations-partner nicht korrekt erkannt wird

Bedrohung der Rechtsverbindlichkeit:

- **Web-Defacing** kann dazu führen, dass einem Angreifer unbe-fugt 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

4.3 Beispiele für Verwundbar-keiten von IT-Systemen

Aufgabe:

- Geben Sie für ein frei gewähltes IT-System eine potentielle Verwundbarkeit an, über die die unter 4.2 angegebene Bedrohung jeweils zu einer erfolgreichen Schädigung des IT-Systems bzw. der dort gespeicherten Daten führen kann.

4.3 Beispiele für Verwundbarkeiten von IT-Systemen (1)

<u>Anmerkung:</u>

***IT-System** = systematisch verbundene informationstechnische Komponenten*

*Für die Lösung wurde ein **Web-Server** als IT-System gewählt*

- 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) → **mangelhafter Firewall-Schutz** oder die Verbindung zum Web-Server nicht hochverfügbar ausgelegt ist → **fehlende Hochverfügbarkeit** oder kein adäquates Berechtigungskonzept auf dem Web-Server eingerichtet wurde, indem z.B. noch Default-Passwörter vorhanden sind → **schlechtes Passwort-Management**

4.3 Beispiele für Verwundbarkeiten von IT-Systemen (2)

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

4.3 Beispiele für Verwundbarkeiten von IT-Systemen (3)

- Ein Session Hijacking kann z.B. bei einem Web-Server zum Erfolg führen, wenn beim Verbindungsaufbau via TCP kein Pseudozufallszahlengenerator verwendet wird → **schwache Authentifizierung** oder eine Session unbegrenzt ablaufen kann → **fehlende Timeout-Funktion**
- Ein **Website-Defacing** kann z.B. bei einem Web-Server zum Erfolg führen, wenn ein Web-Server z.B. mittels Speicherüberlauf übernommen werden konnte → **Buffer-Overflow** oder ein Web-Seiten-Aufruf gezielt umgeleitet wurde → **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)

4.4 Empfohlene Gegen-maßnahmen für Security

Aufgabe:

- Welche Maßnahme(n) würden Sie dem IT-Leiter empfehlen, der den von Ihnen unter 4.2 angegebenen Bedrohungen unter Beachtung der von Ihnen angegebenen Verwund-barkeit aus 4.3 angemessen zu begegnen hat?

4.4 Empfohlene Gegen-maßnahmen für Security (1)

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 Passwortmanage-ment → Dienstanweisung erstellen, dass voreingestellte Start-Kennwörter stets abgeändert werden und dabei die Komplexi-tätsanforderungen erfüllt werden

4.4 Empfohlene Gegen-maßnahmen für Security (2)

Maßnahmen gegen Bedrohungen der Integrität:

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

4.4 Empfohlene Gegen-maßnahmen für Security (3)

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

4.4 Empfohlene Gegen-maßnahmen für Security (4)

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

4.4 Empfohlene Gegen-maßnahmen für Security (5)

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

4.5 Gegensätze von Datenschutz und IT-Sicherheit

Aufgabe:

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

4.5 Gegensätze von Datenschutz und IT-Sicherheit

- **Datenschutz**: Grundsatz der Datensparsamkeit
  IT-Sicherheit: Datensicherung durch Redundanz zur Ausfallsicherheit
- **Datenschutz**: Informationelles Selbstbestimmungsrecht
  IT-Sicherheit: Nachvollziehbarkeit und Überwachung von Aktionen
- **Datenschutz**: Transparenz der Verfahren
  IT-Sicherheit: Verschleierung von Sicherheitseinstellungen
- **Datenschutz**: Inhaltsebene der Daten im Vordergrund
  IT-Sicherheit: Transportebene der Daten im Vordergrund
- **Datenschutz**: Schutzbereich personenbezogene Daten
  IT-Sicherheit: Schutzbereich alle (Unternehmens-)Daten
- **Datenschutz**: Ausgangspunkt = Interesse von Betroffenen
  IT-Sicherheit: Ausgangspunkt = Interesse von Systembetreibern