Repetitionsfragen Information Security Management

1. Was verstehen Sie unter Informationssicherheit?

- der Schutz relevanter Daten vor inneren und äusseren Einflüssen
- der Schutz von Gefahren, denen man ausgesetzt ist

2. Welche Werte werden durch Sicherheit erzeugt?

- wichtigste:
  - Confidentiality (Vertraulichkeit)
  - Integrity (Integrität)
  - Availability (Verfügbarkeit)
- weitere:
  - Non-Repudiation (Nicht-Abstreitbarkeit)
  - Traceability (Nachverfolgbarkeit)
  - Auditability (Auditierbarkeit)
  - Authentication (Authentifizierung)
  - Authorization (Berechtigung)
  - Accountability (Verrechenbarkeit)

3. Erklären Sie die Begriffe Abhängigkeitsanalyse, Verletzlichkeit und Bedrohung!

- Abhängigkeitsanalyse: Katalogisieren und Klassifizieren von Abhängigkeiten zur Planung von Alternativen
- Verletzlichkeit: möglicher Schwachpunkt an einem System (innerlich), Systemschwachstelle
- Bedrohung: mögliche äussere Gefahrenquelle (äusserliche Einwirkung)

4. Was ist ein Ereignis und was ist ein potenzielles Ereignis?

- Ein Ereignis ist, wenn eine Bedrohung auf eine Verletzlichkeit trifft.
- Ein potenzielles Ereignis ist ein Risiko.

5. Beim Risikomanagement gibt es vier typische Schritte. Erkären Sie diese!

Risikomanagement: Umgang mit Risiken

1. verhindern
2. vermindern
3. versichern
4. tragen

6. Können Sie aus einem Ereignis auch Vorteil ziehen?

- Lerneffekt
- Aufdecken von Risiken
- Zwang zu Verbesserungen
- Rechtfertigung für Investitionen in Sicherheit

7. Wie stellen Sie sicher, dass Sie bei einer Risikoanalyse möglichst alle Risiken finden?

- mithilfe von Standards und Frameworks
- diese behandeln alle Themen, die abgedeckt werden müssen

8. Nennen Sie drei Rahmenwerke!

- wichtigste:
  - Grundschutzhandbuch des BSI
  - ISMS (Information Security Management System, von ISO 27000)
  - NIST
- weitere:
  - Prince 2
  - COBIT (für Auditoren)
  - ITIL (für Operation)

9. Erklären Sie die Bildung der Stufungen für Eintretenswahrscheinlichkeit und Schadensausmass!

- Eintretenswahrscheinlichkeit: zeitliche Skala
  - täglich bis wöchentlich
  - jährlich
  - weniger als alle 10 Jahre
- Schadensausmass: Abhängig vom Betroffenen
  - Student
    - gering: < CHF 10
    - mittel: CHF 10-100
    - hoch: > CHF 100
  - KMU
    - gering: < CHF 1'000
    - mittel: CHF 1'000-10'000
    - hoch: > CHF 10'000
- HILF: High Impact, Low Frequency

10. Wie fliessen Post-Incident-Vorbereitungen in die Risikoanalyse ein?

- Der Schaden kann auf ein erträgliches Mass reduziert werden.

11. Welche Bedeutung hat die Mitarbeiterschulung in der Informationssicherheit?

- eine sehr hohe Bedeutung: Sicherheit kann nur gewährleistet werden, wenn sich die Mitarbeiter auch korrekt verhalten (Sicherheit muss „gelebt“ werden!)

12. Welche Art von Ereignissen deckt sich wann (zeitlich) auf?

- Availability (Verfügbarkeit): sofort
- Integirty (Integrität): etwas später
- Confidentiality (Vertraulichkeit): später bis gar nie

13. Erklären Sie, was ein nutzloser Überschutz ist und wie dieser verhindert werden kann!

- Nutzloser Überschutz: Schutzmassnahmen, die keine höhere Sicherheit schaffen
- Verhinderung: mittels Risikoanalyse

14. Erklären Sie die Funktionsweise der Prinzipien „Need to Know“ und „Need to Restrict“!

- „Need to Know“: Informationen sollen geheim gehalten werden
  - nur veröffentlichen, was wirklich veröffentlich werden soll
- „Need to Restrict“: Informationen sollen öffentlich gemacht werden
  - nur geheimhalten, was wirklich geheim gehalten werden muss

→ Die beiden Prinzipien sind gegensätzlich!

15. Erklären Sie den Unterschied zwischen Datensicherheit und Datenschutz!

- Datensicherheit: Synonym für Backup, Daten dürfen nicht verlorengehen
- Datenschutz: Gesetzgebung betreffend schützenswerter Daten von Privatpersonen

16. Erklären Sie die Diagramme Spinnendiagramm und Risikomatrix!

- Risikomatrix: teilt Risiken in verschiedene Bereiche auf
  - x-Achse: Schadensausmass

  - y-Achse: Eintretenswahrscheinlichkeit
  - Felder: Risiko = Schadensausmass × Eintretenswahrscheinlichkeit
  - Einteilung in drei Bereiche
    1. akzeptabel
    2. akzeptabel mit Schadensminderung
    3. inakzeptabel
- Spinnendiagramm: bietet Überblick über Gesamtrisiko
  - Nullpunkt in der Mitte
  - pro Risiko eine Achse vom Nullpunkt ausgehend
  - Risiko = Entfernung vom Nullpunkt
  - Gesamtfläche = Gesamtrisiko

17. Wer ist verantwortlich für die IT-Sicherheit in einem Unternehmen? Ist das die gleiche Person, welche die Sicherung des Unternehmens vornimmt?

- Verantwortung ist einerseits geteilt
  - jemand trägt die Verantwortung für die Umsetzung der Sicherung
  - jemand trägt den finanziellen Schaden
    * Besitzer des Unternehmens
    * Aktionäre, vertreten durch den Verwaltungsrat
- Verantwortung muss andererseits von jedem mitgetragen werden!

18. Was bedeutet Resilienz?

- Widerstandsfähigkeit
  - protect: Schutz im Voraus
  - detect: Überwachung
  - response: Vorbereitung auf Schadensfall