Lernhilfe Klausur 1 – ITG

Schutzziele Verfügbarkeit, Vertraulichkeit, Integrität (und Authentizität) definieren

können und deren Beeinträchtigung in realen Schadensszenarien erkennen und

zuordnen können.

Verfügbarkeit, die Informationen müssen autorisierten Personen zur Verfügung stehen, wenn sie diese benötigen. Nicht-Verfügbarkeit von Systemen oder Daten durch z.B. Denial-of-Service-Angriffe oder Ausfälle.

Vertraulichkeit, nur befugte Personen dürfen Informationen einsehen, nutzen oder weitergeben. Unbefugte Offenlegung von sensiblen Daten durch z.B. Datenlecks oder Spionage.

Integrität, bedeutet Informationen müssen korrekt und unverändert sein. Manipulation oder Zerstörung von Daten durch z.B. Hackerangriffe oder Fehler.

Authentizität, heißt die Identität von Personen, Systemen oder Daten muss eindeutig und überprüfbar sein. Fälschung von Identitäten oder Nachrichten durch z.B. Phishing-Angriffe oder Man-in-the-Middle-Angriffe.

Grundaufbau eines BSI-Bausteins kennen.

Die Bausteine sind alle gleich aufgebaut, Kurzbeschreibung, Gefährdung, Sicherheitsanforderung und Umsetzungshinweise

Genaue Bedeutung der Modalverben „Muss“, „Darf“ und „Sollte“ auch in Kombination mit „Nicht“ kennen und definieren können.

Muss ist die Verpflichtung, Darf ist die Erlaubnis, Sollte die Empfehlung.

Muss nicht ist ohne Verpflichtung, Darf nicht ist das Verbot, Sollte Nicht eine Empfehlung

Niveaus des Schutzbedarfs nach BSI kennen.

Normal gilt für allgemeine Informationen und Systeme, die keine erhöhten Anforderungen an die Vertraulichkeit, Integrität oder Verfügbarkeit haben.

Hoch gilt für Informationen und Systeme mit erhöhten Anforderungen, z.B. aufgrund ihres Werts oder ihrer Kritikalität.

Sehr hoch gilt für sensible Informationen und Systeme mit besonders hohen Anforderungen, z.B. für die nationale Sicherheit oder den Schutz von Menschenleben.

Sicherheits-Anforderungs-Niveaus nach BSI-Definition kennen und zueinander in

Beziehung setzen können.

SAN 1 ist die Basis für alle anderen SAN.

SAN 2 baut auf SAN 1 auf und bietet zusätzlichen Schutz.

SAN 3 bietet den höchstmöglichen Schutz und beinhaltet alle Anforderungen aus SAN 1 und SAN 2.

Kriterien für die Bewertung der Eignung von Verschlüsselungssoftware verstehen

und ihre Bedeutung für die Szenarien „Einzelverschlüsselung von Dateien“ oder

„Anlegen eines Tresors/Safes“ beurteilen können. Prinzip der Berechnung von Hash-Werten kennen.

Kriterien könnten Sachen, wie diese sein: Algorithmus (AES, RSA), Schlüssellänge, Benutzerfreundlichkeit, Kompatibilität, Reputation des Herstellers, Unabhängige Tests

Der Absender berechnet einen Hashwert aus seiner Nachricht. Diesen Hashwert verschlüsselt er mit seinem privaten Schlüssel und übermittelt die Nachricht zusammen mit dem verschlüsselten Hashwert an den Empfänger.

~~Grundprinzip der symmetrischen und der asymmetrischen Verschlüsselung~~

~~kennen.~~

~~Bei der Symmetrische Verschlüsselung verwenden beide Kommunikationspartner den gleichen geheimen Schlüssel zum Verschlüsseln und Entschlüsseln von Nachrichten.~~

~~Bei der Asymmetrische Verschlüsselung hat jeder Kommunikationspartner einen öffentlichen Schlüssel und einen privaten Schlüssel.~~

Arten von Cyberangriffen definieren und konkreten Angriffsszenarien zuordnen

können: Pishing, Malware, Ransomware, DoS, DDos.

Phishing ist eine Betrugsmasche, um sensible Informationen wie Passwörter zu erlangen.

Malware ist schädliche Software, die Computer oder Netzwerke angreift.

Ransomware verschlüsselt Daten und fordert Lösegeld für ihre Freigabe.

DoS-Angriffe machen ein System für legitime Nutzer unzugänglich.

DDoS-Angriffe sind groß angelegte DoS-Angriffe von mehreren Systemen.

Gefährdungen aus dem BSI-Katalog den Kategorien „Schaden“ oder „Einfallstor“ zuordnen können.

Bei Schäden zählen Bedrohungen, welche das System direkt angreifen.

Bei Einfallstoren sind es Bedrohungen, die Zugriff auf Systemen haben.

Vom BSI empfohlene Erste-Hilfe-Maßnahmen nach Eintreten eines

Sicherheitsvorfalls kennen und ihre Sinnhaftigkeit einordnen und begründen

können.

1. Identifizierung und Eindämmung des Vorfalls
2. Sicherung von Beweismitteln
3. Kommunikation und Meldungen
4. Ursachenanalyse und Wiederherstellung
5. Nachsorge und Dokumentation

Die Anzahl der Kombinationsmöglichkeiten zur Bildung eines Passworts in

Abhängigkeit von der Anzahl der möglichen Zeichen und der Anzahl der Stellen

berechnen können.

x = numOfChars^length

100.000.000 = 10^8 // Case: 0-9, max. 8 lang

Kombinationen