

1.2 Datensicherheit – Bedrohungen, Härtung und ISMS

Überblick

Hier übst du, Bedrohungen zu erkennen, Schutzmaßnahmen zu begründen und technische Sicherheit in ein geregeltes Vorgehen einzuordnen.

So lernst du: Nenne zuerst Angriff, betroffenes Schutzziel und Gegenmaßnahme. Klappe dann die Antwort auf.

Bedrohungen und Gegenmaßnahmen

1. Was ist SQL-Injection und wie verhindert man sie?

Ungeprüft zusammengesetzte Datenbankabfragen können Eingaben als SQL-Befehle interpretieren. **Parametrisierte Abfragen beziehungsweise Prepared Statements** trennen Befehlsstruktur und Daten. Zusätzlich: Eingaben passend validieren und dem Datenbankkonto nur erforderliche Rechte geben. Eingabeprüfung allein ersetzt keine Parametrisierung.

2. Was ist Cross-Site Scripting (XSS)?

Eine Anwendung gibt fremde Inhalte so aus, dass der Browser sie als ausführbaren Code behandelt. Schutz: **kontextgerechte Ausgabekodierung**, sichere Framework-Funktionen und bei erlaubtem HTML eine geeignete Bereinigung. Eine bloße Suche nach verdächtigen Wörtern reicht nicht.

3. Was unterscheidet SQL-Injection und XSS?

SQL-Injection beeinflusst Datenbankabfragen. XSS betrifft die Ausführung eingeschleuster Inhalte im Browser. Deshalb unterscheiden sich die Hauptmaßnahmen: **Abfragen parametrisieren** beziehungsweise **Ausgaben sicher kodieren**.

4. Was ist Phishing und welche Maßnahmen helfen?

Gefälschte Nachrichten oder Anmeldeseiten sollen etwa Zugangsdaten erbeuten. Gegenmaßnahmen: Absender und Zieladresse prüfen, bekannte Zugangswege nutzen, verdächtige Nachrichten melden, Schulungen und MFA einsetzen. MFA senkt das Risiko, macht aber nicht jede Phishing-Variante wirkungslos.

5. Was bedeutet Social Engineering?

Angreifer nutzen Hilfsbereitschaft, Angst oder Zeitdruck, um Menschen zu unerwünschten Handlungen zu bewegen. Beispiel: ein angeblicher Supportmitarbeiter verlangt einen Anmeldecode. Schutz: Identität über einen bekannten, unabhängigen Kontaktweg prüfen und Freigabeprozesse einhalten.

6. Was sind Malware, Virus, Trojaner und Ransomware?

Malware ist der Oberbegriff für Schadsoftware. Ein **Virus** verbreitet sich über infizierte Wirtsdateien. Ein **Trojaner** tarnt sich als nützliches Programm. **Ransomware** sperrt oder verschlüsselt Daten zur Erpressung; auch Datendiebstahl kann dazugehören.

7. Welche Schutzmaßnahmen gegen Schadsoftware ergänzen sich?

Aktuelle Software, geeigneter Endgeräteschutz, eingeschränkte Benutzerrechte, vorsichtiger Umgang mit Anhängen und überprüfte Backups. Kein einzelnes Produkt verhindert jeden Angriff.

8. Was ist ein Brute-Force-Angriff?

Automatisiertes Durchprobieren möglicher Zugangsdaten. Lange, einzigartige Passwörter erschweren das Erraten. Rate-Limiting begrenzt Versuche; MFA ergänzt den Schutz. Fehlversuche sollten überwacht werden.

9. Was ist ein Man-in-the-Middle-Angriff?

Ein Angreifer positioniert sich zwischen Kommunikationspartnern, um Daten mitzulesen oder zu verändern. Korrekt eingesetztes **TLS mit Zertifikatsprüfung** schützt die Verbindung. Zertifikatswarnungen dürfen nicht einfach übergangen werden.

10. Was ist DDoS, und reicht Load Balancing als Schutz?

Viele verteilte Quellen überlasten einen Dienst oder dessen Anbindung. Hauptsächlich betroffen ist die **Verfügbarkeit**. Lastverteilung kann helfen, reicht bei überlasteter Leitung aber nicht aus. Vorgeschaltete Filterung und DDoS-Schutz beim Anbieter können notwendig sein.

Härtung und Sicherheitsmanagement

11. Was bedeutet Betriebssystemhärtung?

Die Angriffsfläche gezielt verkleinern: unnötige Dienste und Schnittstellen abschalten, Updates einspielen, Rechte begrenzen, sichere Anmeldung durchsetzen, Firewall-Regeln einschränken sowie Protokollierung und Überwachung einrichten.

12. Warum ist Härtung keine einmalige Aufgabe?

Neue Schwachstellen, installierte Programme und geänderte Anforderungen beeinflussen die Sicherheitslage. Konfigurationen, Updates und Berechtigungen müssen deshalb regelmäßig überprüft werden.

13. Was ist ein ISMS?

Ein **Informationssicherheitsmanagementsystem** legt fest, wie eine Organisation Informationssicherheit steuert: Verantwortlichkeiten, Risiken, Ziele, Maßnahmen und deren Überprüfung. Es umfasst Menschen und Abläufe ebenso wie Technik.

14. Wofür stehen BSI IT-Grundschutz und ISO/IEC 27001?

IT-Grundschutz: Methodik und Anforderungen des BSI zur systematischen Absicherung.

ISO/IEC 27001: internationaler Standard mit Anforderungen an ein ISMS. Eine Zertifizierung bezieht sich auf einen festgelegten Geltungsbereich; sie garantiert keine absolute Angriffssicherheit.

Anwendungsaufgabe

15. Ein angeblicher Administrator verlangt telefonisch dein Passwort für eine dringende Reparatur. Wie reagierst du?

Keine Zugangsdaten herausgeben. Anfrage über den bekannten Supportkanal überprüfen und den Verdacht melden. **Einordnung:** Social Engineering; die behauptete Dringlichkeit soll die normale Prüfung umgehen.

Merksatz

Bedrohung erkennen → Angriffsweg verstehen → passende Maßnahmen kombinieren.

Prüfungshinweis

Vermeide pauschale Antworten wie „Firewall installieren“. Begründe, warum eine Maßnahme zum Angriff passt. Unterscheide Vorbeugung, Erkennung und Wiederherstellung.

Quellen und Einordnung

Themenrahmen: [FI-Wiki – Datensicherheit](#). Eigenständig formulierte Lernfragen und ergänzende Praxisbeispiele; keine offiziellen IHK-Prüfungsfragen.

Technische Vertiefung: [OWASP – SQL Injection Prevention](#) und [OWASP – Cross Site Scripting Prevention](#).