Cyber Security – Zusammenfassung

1. Einführung in Cyber Security

Cyber Security befasst sich mit dem Schutz von Computersystemen, Netzwerken und Daten vor Angriffen, Sc
Ziele:
- Vertraulichkeit (Confidentiality)
- Integrität (Integrity)
- Verfügbarkeit (Availability)

2. Arten von Bedrohungen

- Malware (Viren, Würmer, Trojaner, Ransomware)
- Phishing & Social Engineering
- Denial-of-Service (DoS/DDoS)
- Insider Threats

3. Authentifizierung und Zugriffskontrolle

Methoden:
- Passwörter
- Zwei-Faktor-Authentifizierung (2FA)
- Biometrische Verfahren

Zugriffsmodelle:
- DAC (Discretionary Access Control)
- MAC (Mandatory Access Control)
- RBAC (Role-Based Access Control)

4. Kryptografie-Grundlagen

Symmetrische Verschlüsselung (z.■B. AES)
Asymmetrische Verschlüsselung (z.■B. RSA, ECC)
Hashfunktionen (z.■B. SHA-256)
Digitale Signaturen & Zertifikate

5. Netzwerksicherheit

Sichere Protokolle:
- HTTPS, TLS, VPN

Firewalls & Intrusion Detection Systems (IDS)
Netzwerksegmentierung & Zero-Trust-Ansatz

6. Sicherheit in Webanwendungen

Typische Schwachstellen:
- SQL-Injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)

Schutzmaßnahmen:
- Input-Validierung
- Prepared Statements
- Content Security Policy

7. Sicherheitsrichtlinien & Awareness

- IT-Sicherheitsrichtlinien im Unternehmen
- Schulungen & Sensibilisierung der Mitarbeitenden
- Umgang mit Vorfällen & Meldepflichten

8. Sicherheit im Cloud-Umfeld

- Verantwortungsteilung (Shared Responsibility Model)
- Datenverschlüsselung in Ruhe und Übertragung
- Zugriffskontrollen & Identitätsmanagement (IAM)