CYBERSECURITY MINDMAP-SERIE – BEGLEITDOKUMENTATION

# Cybersecurity Begriffsglossar: Kernterminologie von A bis Z

## Zentrales Begriffsglossar zur Standardterminologie der IT-Sicherheit

> Strukturiertes Nachschlagewerk mit präzisen Definitionen zu den Kernbegriffen der 150 Mindmaps. Behandelt Schutzziele, Angriffsvektoren, Netzwerkprotokolle und Reaktionsphasen für Lernende ohne Vorkenntnisse.


01 Leitfaden und Nutzung des Nachschlagewerks

02 Glossar: A bis E

03 Glossar: F bis M

04 Glossar: N bis Z

05 Standardablauf Incident Response

06 Entscheidungsbaum: Vorfallkategorisierung

07 Begriffs-Notizen und individuelle Lerndokumentation

01

# Leitfaden und Nutzung des Nachschlagewerks

Dieses Glossar dient als kompaktes, alphabetisch geordnetes Nachschlagewerk zu den 150 Mindmaps der Cybersecurity-Reihe. Es vermittelt Einsteigern präzise Definitionen grundlegender Sicherheitskonzepte, Netzwerkmechanismen und kryptografischer Verfahren ohne vorausgesetztes Vorwissen.

- Verwendung parallel zur Durcharbeitung der thematischen Mindmaps zur Festigung von Schlüsselbegriffen.
- Klarer Fokus auf standardisierte Branchenterminologie gemäß anerkannten Sicherheitsmodellen (z. B. CIA-Triade, Zero Trust, Incident Response).
- Praktische Hilfestellung bei der Analyse von Netzwerktraffic, Schwachstellenberichten und Systemmeldungen.

> **Hinweis für Lernende**
>
> Nutzen Sie dieses Glossar bei Unklarheiten während der praktischen Übungen in Netzwerk-Labs oder Python-Skripten, um begriffliche Überschneidungen (wie Authentifizierung vs. Autorisierung) sauber zu trennen.

02

# Glossar: A bis E

Grundbegriffe der Angriffserkennung, Benutzerverwaltung und kryptografischen Basisverfahren.

- Advanced Persistent Threat (APT): Zielgerichteter, komplexer Cyberangriff, bei dem Angreifer unbemerkt über längere Zeiträume im Zielnetzwerk verbleiben.
- Asymmetrische Kryptografie: Verschlüsselungsverfahren mit Schlüsselpaaren (öffentlicher Schlüssel zum Ver-/Prüfen, privater Schlüssel zum Ent-/Signieren).
- Authentifizierung: Verifikation der behaupteten Identität eines Nutzers oder Systems (z. B. via Passwort, Biometrie oder Token).
- Autorisierung: Festlegung und Durchsetzung der Zugriffsrechte eines bereits authentifizierten Nutzers auf bestimmte Ressourcen.
- Botnetz: Zusammenschluss kompromittierter Rechner ('Bots'), die von einem Angreifer ferngesteuert für Denial-of-Service-Angriffe oder Spam-Versand missbraucht werden.
- CIA-Triade: Fundamentales Sicherheitsmodell bestehend aus Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability).
- Cross-Site Scripting (XSS): Einschleusen bösartigen Codes in Webanwendungen, der im Browser legitimer Anwender ausgeführt wird.
- Denial of Service (DoS / DDoS): Gezielte Überlastung eines Rechnersystems oder Netzwerkdienstes durch konzentrierte Datenfluten zur Verhinderung legitimer Anfragen.
- Endpoint Detection and Response (EDR): Sicherheitslösung zur kontinuierlichen Überwachung von Endgeräten auf verdächtige Verhaltensweisen und Bedrohungen.

03

# Glossar: F bis M

Konzepte rund um Netzwerküberwachung, Sicherheitsarchitektur und Schadsoftware.

- Firewall: Netzwerkkomponente (Hardware oder Software), die Datenverkehr anhand definierter Regeln filtert und segmentiert.
- Identity and Access Management (IAM): Rahmenwerk von Richtlinien und Systemen zur Verwaltung digitaler Identitäten und Zugriffsrechte.
- Incident Response: Strukturierter Prozess zur Erkennung, Eindämmung, Beseitigung und Nachbereitung von IT-Sicherheitsvorfällen.
- Intrusion Detection/Prevention System (IDS/IPS): System zur passiven Erkennung (IDS) oder aktiven Blockierung (IPS) unautorisierter Zugriffsversuche im Netzwerk.
- Man-in-the-Middle (MitM): Angriffsform, bei der sich ein unbefugter Dritter unbemerkt zwischen zwei Kommunikationspartner schaltet, um Daten abzufangen oder zu manipulieren.
- Multi-Faktor-Authentifizierung (MFA): Absicherung von Logins durch Kombination aus mindestens zwei voneinander unabhängigen Faktoren (Wissen, Besitz, Inhärenz).

04

# Glossar: N bis Z

Terminologie zu Infrastruktur, Sicherheitsstrategien und modernen Bedrohungsformen.

- Phishing: Täuschungsversuche zur Erbeutung sensibler Informationen (wie Passwörter oder Sitzungsdaten) über gefälschte Nachrichten oder Webseiten.
- Public Key Infrastructure (PKI): System aus Zertifizierungsstellen, Richtlinien und technischen Komponenten zur Ausgabe und Verwaltung digitaler Zertifikate.
- Ransomware: Schadsoftware, die Nutzerdaten oder Systeme verschlüsselt und Lösegeld für deren Entschlüsselung fordert.
- Social Engineering: Taktiken zur Manipulation von Personen, um vertrauliche Informationen preiszugeben oder schädigende Aktionen auszulösen.
- Virtual Private Network (VPN): Verschlüsselte Punkt-zu-Punkt-Verbindung über ein unsicheres Netzwerk zur sicheren Datenübertragung.
- Zero Trust: Sicherheitsarchitektur nach dem Grundsatz 'Never Trust, Always Verify', bei der jedem Zugriff unabhängig vom Standort misstraut wird.

> **Achtung vor Begriffsverwechslung**
>
> Verwechseln Sie nicht DoS (lokaler Ausfall / Einzelauslöser) mit DDoS (verteilte Botnetze) sowie Verschlüsselung (Vertraulichkeit) mit Hashing (Integritätsprüfung).

05

# Standardablauf Incident Response

Phasenorientierter Leitfaden zur Behebung eines Sicherheitsvorfalls gemäß gängigen IT-Forensik- und Sicherheitsstandards.

1

### 1. Vorbereitung (Preparation)

Bereitstellung von Tools, Festlegung von Notfallplänen und Definition von Meldeketten vor Eintritt eines Vorfalls.

2

### 2. Identifikation (Identification)

Erkennung von Anomalien, Analyse verdächtiger Logs und Bestätigung des Sicherheitsvorfalls.

3

### 3. Eindämmung (Containment)

Isolation betroffener Systeme aus dem Netzwerk, um eine Ausbreitung des Schadens zu stoppen.

4

### 4. Beseitigung (Eradication)

Vollständiges Entfernen der Schadsoftware, Schließen der Sicherheitslücke und Bereinigen infizierter Komponenten.

5

### 5. Wiederherstellung (Recovery)

Kontrollierter Wiederanlauf gereinigter Systeme aus sauberen Backups unter verstärkter Überwachung.

6

### 6. Nachbereitung (Lessons Learned)

Dokumentation des Vorfalls, Ursachenanalyse und Ableitung präventiver Schutzmaßnahmen.

- Verfolgt die standardisierten NIST- und SANS-Phasen von der Erkennung bis zur Lessons-Learned-Phase.
- Hilft Einsteigern, den Unterschied zwischen bloßer Erkennung und vollständiger Beseitigung zu verstehen.

06

# Entscheidungsbaum: Vorfallkategorisierung

Strukturierte Entscheidungshilfe zur Ersteinschätzung von Anomalien und sicherheitskritischen Ereignissen.

**Welche primäre Auswirkung wird im betroffenen System festgestellt?**

**Dateien wurden unerwartet verschlüsselt und Lösegeldforderung angezeigt**

Sofortige Trennung des Systems vom lokalen Netzwerk (LAN/WLAN) und Meldung an das Incident-Response-Team zur Ransomware-Eindämmung.

**Dienste sind durch massenhafte eingehende Netzwerkanfragen nicht erreichbar**

Aktivierung des DDoS-Schutzes, Analyse von Quell-IPs und vorgeschaltetes Traffic-Filtering an der Perimeter-Firewall.

**Unbefugter Zugriff über bestehende Nutzeranmeldedaten registriert**

Umgehendes Zurücksetzen der Anmeldedaten im IAM-System, Sitzungsentzug aller aktiven Sessions und Überprüfung der Multi-Faktor-Protokolle.

- [ ] Schnelle Zuordnung der Angriffsart basierend auf primären Beobachtungen.
- [ ] Direkte Handlungsanweisungen für Ersthelfer im Systembetrieb.

07

# Begriffs-Notizen und individuelle Lerndokumentation

Nutzen Sie diesen Arbeitsbereich, um im Rahmen Ihres Mindmap-Studiums eigene Ergänzungen, Fragen oder konkrete Befehle zu den Termini festzuhalten.

- Festhalten von Praxiserkenntnissen aus Übungsszenarien.
- Dokumentation von projektspezifischen Begriffsausprägungen.

### Schlüsselbegriff & persönlicher Merksatz

### Konkreter Anwendungsfall / Toolbeispiel (z. B. Wireshark, nmap)

### Offene Fragen zur Vertiefung in den Mindmaps