16.4 Netzwerkangriffe: DoS, DDoS, Spoofing und Man-in-the-Middle

Netzwerkangriffe richten sich gegen Kommunikation, Erreichbarkeit, Identitäten oder Datenübertragung in Netzwerken.

Sie können auf verschiedenen OSI-Schichten stattfinden.

Typische Netzwerkangriffe sind:

- DoS
- DDoS
- Man-in-the-Middle
- ARP-Spoofing
- DNS-Spoofing
- IP-Spoofing
- MAC-Spoofing
- Sniffing
- Session Hijacking
- Rogue DHCP
- Evil Twin
- WLAN-Angriffe

Merksatz:

Netzwerkangriffe nutzen Schwächen in Kommunikation,
Adressierung,
Namensauflösung
oder Erreichbarkeit aus.

Warum Netzwerkangriffe gefährlich sind

Netzwerke verbinden Systeme miteinander.

Wenn ein Angreifer Netzwerkkommunikation beeinflusst, kann er unter Umständen:

Daten mitlesen
Daten verändern

Benutzer auf falsche Ziele lenken
Dienste überlasten
Verbindungen unterbrechen
Zugangsdaten abgreifen
Sitzungen übernehmen
interne Systeme erreichen
Kommunikation manipulieren

Merksatz:

Wer Netzwerkverkehr kontrolliert,
kann viele weitere Angriffe vorbereiten.

DoS

DoS steht für:

Denial of Service

Denial of Service bedeutet:

Ein Dienst wird absichtlich so gestört,
dass er nicht mehr nutzbar ist.

Ziel:

Verfügbarkeit angreifen

Beispiele:

Webserver antwortet nicht mehr.
Anwendung ist überlastet.
Netzwerkleitung ist voll.
Firewall ist überfordert.
Datenbank nimmt keine Verbindungen mehr an.

Merksatz:

DoS greift die Verfügbarkeit an.

DoS einfach erklärt

Ein Dienst kann nur eine begrenzte Menge an Anfragen verarbeiten.

Wenn ein Angreifer sehr viele Anfragen sendet, kann der Dienst überlastet werden.

Folge:

normale Benutzer können den Dienst nicht mehr nutzen.

Merksatz:

DoS bedeutet:
Dienst wird durch Störung oder Überlastung unbenutzbar.

DDoS

DDoS steht für:

Distributed Denial of Service

Distributed bedeutet:

verteilt

Bei DDoS kommt der Angriff von vielen Systemen gleichzeitig.

Häufig werden Botnetze genutzt.

Merksatz:

DDoS ist ein verteilter DoS-Angriff.

DoS und DDoS vergleichen

Merkmal	DoS	DDoS

Angriffsquelle	eine oder wenige Quellen	viele verteilte Quellen
Abwehr	oft einfacher	deutlich schwieriger
typische Technik	Überlastung oder Störung	massenhafte verteilte Überlastung
Ziel	Verfügbarkeit	Verfügbarkeit

Merksatz:

```
DoS = Dienstverweigerung.
DDoS = verteilte Dienstverweigerung.
```

Typische DDoS-Ziele

DDoS-Angriffe richten sich häufig gegen:

```
Webseiten
Online-Shops
DNS-Server
VPN-Gateways
Firewalls
Load Balancer
APIs
Gaming-Server
Cloud-Dienste
Unternehmensanschlüsse
```

Merksatz:

```
DDoS trifft oft öffentlich erreichbare Dienste.
```

DDoS-Angriffsarten

DDoS kann unterschiedliche Ebenen treffen.

Beispiele:

```
Volumenangriff:
Leitung wird mit Datenverkehr überlastet.
```

Protokollangriff:
Netzwerk- oder Transportprotokolle werden ausgenutzt.

Anwendungsschichtangriff:
Webanwendung wird mit vielen echten oder scheinbar echten Anfragen belastet.

Merksatz:

DDoS kann Leitung,
Protokoll
oder Anwendung treffen.

Volumenangriff

Ein Volumenangriff versucht, möglichst viel Datenverkehr zu erzeugen.

Ziel:

Bandbreite überlasten

Beispiele:

sehr viele UDP-Pakete
große Datenmengen
reflektierter Verkehr

Folge:

legitimer Verkehr kommt nicht mehr durch.

Merksatz:

Volumenangriff überlastet die Bandbreite.

Protokollangriff

Ein Protokollangriff nutzt Eigenschaften von Netzwerkprotokollen aus.

Ziel:

Netzwerkgeräte,
Firewalls,
Load Balancer
oder Serverzustände überlasten

Beispiele:

viele halboffene Verbindungen
viele Verbindungsversuche
ausgenutzte Protokollmechanismen

Merksatz:

Protokollangriff belastet Netzwerk- oder Transportmechanismen.

Anwendungsschichtangriff

Ein Anwendungsschichtangriff richtet sich gegen Dienste auf OSI-Schicht 7.

Beispiele:

viele HTTP-Anfragen
teure Suchanfragen
Loginversuche
API-Anfragen
Warenkorbaktionen
Datenbanklast durch Webanfragen

Problem:

Der Angriff kann wie normaler Benutzerverkehr aussehen.

Merksatz:

Anwendungsschichtangriffe sind oft schwerer von echter Nutzung zu unterscheiden.

Reflexionsangriff

Bei einem Reflexionsangriff sendet der Angreifer Anfragen an fremde Server und fälscht dabei die Absenderadresse des Opfers.

Die fremden Server antworten dann an das Opfer.

Beispiele für missbrauchte Dienste:

```
DNS
NTP
Memcached
SSDP
andere UDP-basierte Dienste
```

Merksatz:

```
Reflexionsangriff lenkt Antworten fremder Systeme auf das Opfer.
```

Amplification

Amplification bedeutet:

```
Verstärkung
```

Der Angreifer sendet eine kleine Anfrage, die eine deutlich größere Antwort erzeugt.

Wenn die Antwort an das Opfer geht, wird der Angriff verstärkt.

Merksatz:

```
Amplification macht aus kleinen Anfragen große Angriffsdatenmengen.
```

Schutz vor DoS und DDoS

Mögliche Schutzmaßnahmen:

```
DDoS-Schutzdienst
Provider-Unterstützung
```

Content Delivery Network
Load Balancer
Rate Limiting
Anycast
Firewall-Regeln
Web Application Firewall
Skalierung
Monitoring
Notfallplan
Blackholing als Notmaßnahme

Merksatz:

DDoS-Schutz braucht Vorbereitung,
weil man im Angriff oft wenig Zeit hat.

Rate Limiting

Rate Limiting begrenzt, wie viele Anfragen in einer bestimmten Zeit erlaubt sind.

Beispiele:

maximal 100 Anfragen pro Minute pro IP

maximal 5 Loginversuche pro Minute

API-Limit pro Benutzer

Vorteil:

automatisierte Überlastung wird erschwert.

Merksatz:

Rate Limiting begrenzt Anfragehäufigkeit.

Anycast

Anycast bedeutet:

```
dieselbe IP-Adresse wird an mehreren Standorten angekündigt.
```

Der Verkehr wird zum nächstgelegenen oder passenden Standort geleitet.

Vorteil bei DDoS:

```
Angriffslast kann verteilt werden.
```

Merksatz:

```
Anycast verteilt Verkehr auf mehrere Standorte.
```

Blackholing

Blackholing bedeutet:

```
Verkehr zu einem Ziel wird verworfen.
```

Das kann bei DDoS als Notmaßnahme genutzt werden.

Nachteil:

```
Der angegriffene Dienst ist dann ebenfalls nicht erreichbar.
```

Merksatz:

```
Blackholing schützt Infrastruktur,
macht den Dienst aber meist unerreichbar.
```

Man-in-the-Middle

Man-in-the-Middle wird oft abgekürzt:

```
MitM
```

Dabei positioniert sich ein Angreifer zwischen zwei Kommunikationspartnern.

Ziele:

```
Daten mitlesen
Daten verändern
Anmeldedaten abgreifen
Sitzung übernehmen
Zertifikatswarnungen ausnutzen
Benutzer auf falsche Dienste lenken
```

Merksatz:

```
MitM bedeutet:
Angreifer sitzt zwischen Sender und Empfänger.
```

Man-in-the-Middle einfach erklärt

Normale Kommunikation:

```
Client
↔
Server
```

Mit Man-in-the-Middle:

```
Client
↔
Angreifer
↔
Server
```

Der Benutzer glaubt, direkt mit dem Server zu kommunizieren.

Tatsächlich läuft die Kommunikation über den Angreifer.

Merksatz:

```
Bei MitM wird Kommunikation heimlich zwischengeschaltet.
```

Typische MitM-Szenarien

Beispiele:

```
unsicheres WLAN
gefälschter Access Point
ARP-Spoofing im lokalen Netz
DNS-Spoofing
manipuliertes Gateway
kompromittierter Router
Proxy-Angriff
gefälschtes Zertifikat
Session-Cookie-Diebstahl
```

Merksatz:

```
MitM kann über WLAN,
LAN,
DNS,
Router
oder Zertifikate entstehen.
```

Schutz vor Man-in-the-Middle

Maßnahmen:

```
TLS korrekt nutzen
HTTPS erzwingen
Zertifikatswarnungen nicht ignorieren
VPN in unsicheren Netzen
HSTS bei Webseiten
sichere WLAN-Konfiguration
ARP-Schutz in Switches
DNSSEC je nach Einsatz
sichere DNS-Resolver
MFA
Session-Cookies schützen
```

Merksatz:

```
TLS schützt nur dann,
wenn Zertifikate korrekt geprüft werden.
```

Sniffing

Sniffing bedeutet:

```
Netzwerkverkehr wird mitgeschnitten oder beobachtet.
```

Legitime Nutzung:

```
Fehlersuche
Protokollanalyse
Performanceanalyse
Sicherheitsanalyse
```

Missbrauch:

```
Passwörter abfangen
Daten mitlesen
interne Kommunikation analysieren
Sitzungen übernehmen
Schwachstellen finden
```

Merksatz:

```
Sniffing ist ein Werkzeug,
das für Analyse oder Angriff genutzt werden kann.
```

Sniffing und Verschlüsselung

Unverschlüsselter Verkehr kann direkt lesbar sein.

Beispiele für riskanten Klartextverkehr:

```
HTTP
Telnet
FTP
POP3 ohne TLS
IMAP ohne TLS
SMTP ohne TLS
alte Protokolle
```

Verschlüsselter Verkehr schützt Inhalte besser.

Beispiele:

```
HTTPS
SSH
SFTP
FTPS
IMAPS
SMTPS
VPN
```

Merksatz:

```
Verschlüsselung reduziert den Schaden durch Sniffing.
```

Spoofing

Spoofing bedeutet:

```
Eine falsche Identität,
Adresse
oder Herkunft wird vorgetäuscht.
```

Typische Arten:

```
IP-Spoofing
MAC-Spoofing
ARP-Spoofing
DNS-Spoofing
```

E-Mail-Spoofing

Merksatz:

Spoofing täuscht Herkunft oder Identität vor.

IP-Spoofing

IP-Spoofing bedeutet:

Der Angreifer fälscht die Quell-IP-Adresse.

Ziele:

Herkunft verschleiern
Reflexionsangriffe ermöglichen
Filter umgehen
Vertrauen in IP-Adressen ausnutzen

Grenze:

Bei TCP-Verbindungen ist IP-Spoofing schwieriger,
weil Antworten an die gefälschte Adresse gehen.

Merksatz:

IP-Spoofing fälscht die Quell-IP-Adresse.

MAC-Spoofing

MAC-Spoofing bedeutet:

Ein Gerät gibt sich mit einer anderen MAC-Adresse aus.

Mögliche Ziele:

```
MAC-Filter umgehen
Identität im LAN vortäuschen
Netzwerkzugang erschleichen
Geräteverwechslung erzeugen
```

Merksatz:

```
MAC-Adressen können gefälscht werden
und sind kein starker Sicherheitsnachweis.
```

ARP

ARP steht für:

```
Address Resolution Protocol
```

ARP ordnet im lokalen IPv4-Netz eine IP-Adresse einer MAC-Adresse zu.

Beispiel:

```
Welche MAC-Adresse hat 192.168.1.1?
```

Antwort:

```
192.168.1.1 hat MAC-Adresse aa:bb:cc:dd:ee:ff
```

Merksatz:

```
ARP verbindet IPv4-Adressen mit MAC-Adressen im lokalen Netz.
```

ARP-Spoofing

ARP-Spoofing manipuliert ARP-Zuordnungen im lokalen Netz.

Angreifer behauptet zum Beispiel:

```
Ich bin das Gateway.
```

Dann senden Clients ihren Verkehr an den Angreifer.

Mögliche Folgen:

```
Man-in-the-Middle
Sniffing
Sitzungsdiebstahl
Verbindungsstörung
```

Merksatz:

```
ARP-Spoofing greift lokale Layer-2-Kommunikation an.
```

Schutz vor ARP-Spoofing

Maßnahmen:

```
Dynamic ARP Inspection
DHCP Snooping
statische ARP-Einträge in Sonderfällen
Netzwerksegmentierung
Switch-Sicherheitsfunktionen
Verschlüsselung durch TLS
Monitoring auf ARP-Anomalien
```

Merksatz:

```
Gegen ARP-Spoofing helfen Switch-Schutzfunktionen und Verschlüsselung.
```

DNS

DNS steht für:

```
Domain Name System
```

DNS löst Namen in IP-Adressen auf.

Beispiel:

```
www.example.de
→
203.0.113.10
```

Merksatz:

```
DNS übersetzt Namen in IP-Adressen.
```

DNS-Spoofing

DNS-Spoofing manipuliert die Namensauflösung.

Ziel:

```
Benutzer wird zu falscher IP-Adresse geleitet.
```

Beispiel:

```
Benutzer ruft eine echte Domain auf,
landet aber auf einer gefälschten Webseite.
```

Mögliche Folgen:

```
Phishing
Malware-Verteilung
Man-in-the-Middle
Datenabfluss
```

Merksatz:

```
DNS-Spoofing führt Namen zu falschen Zielen.
```

DNS-Cache-Poisoning

DNS-Cache-Poisoning bedeutet:

falsche DNS-Antworten werden in einem DNS-Cache gespeichert.

Folge:

Mehrere Benutzer erhalten falsche DNS-Antworten,
bis der Cache abläuft oder korrigiert wird.

Merksatz:

DNS-Cache-Poisoning vergiftet zwischengespeicherte DNS-Antworten.

Schutz vor DNS-Spoofing

Maßnahmen:

vertrauenswürdige DNS-Resolver
DNSSEC
DNS-over-TLS oder DNS-over-HTTPS je nach Umgebung
Monitoring ungewöhnlicher DNS-Antworten
TLS-Zertifikatsprüfung
keine unbekannten DNS-Server per DHCP erlauben
sichere Router- und DHCP-Konfiguration

Merksatz:

DNS-Schutz und TLS-Prüfung ergänzen sich.

DNSSEC

DNSSEC steht für:

Domain Name System Security Extensions

DNSSEC ermöglicht kryptografische Prüfung von DNS-Antworten.

Ziel:

Manipulation von DNS-Antworten erkennbar machen.

Wichtig:

DNSSEC verschlüsselt DNS-Anfragen nicht automatisch.
Es prüft vor allem Echtheit und Integrität.

Merksatz:

DNSSEC schützt DNS-Integrität,
aber nicht automatisch DNS-Vertraulichkeit.

Rogue DHCP

Rogue DHCP bedeutet:

Ein nicht autorisierter DHCP-Server verteilt Netzwerkeinstellungen.

Mögliche Folgen:

falsches Gateway
falscher DNS-Server
falsche IP-Konfiguration
Man-in-the-Middle
Netzwerkstörungen

Merksatz:

Rogue DHCP verteilt falsche Netzwerkkonfiguration.

Schutz vor Rogue DHCP

Maßnahmen:

DHCP Snooping
Switchports absichern

ungenutzte Ports deaktivieren
Netzwerksegmentierung
Monitoring
physische Zugangskontrolle
nur autorisierte DHCP-Server zulassen

Merksatz:

DHCP Snooping schützt vor unautorisierten DHCP-Servern.

DHCP Snooping

DHCP Snooping ist eine Switch-Sicherheitsfunktion.

Sie unterscheidet:

vertrauenswürdige Ports

und

nicht vertrauenswürdige Ports

DHCP-Antworten sind nur auf vertrauenswürdigen Ports erlaubt.

Merksatz:

DHCP Snooping verhindert DHCP-Antworten von falschen Ports.

Session Hijacking

Session Hijacking bedeutet:

Ein Angreifer übernimmt eine bestehende Sitzung.

Mögliche Wege:

Session-Cookie stehlen
Token stehlen

XSS
Malware
Man-in-the-Middle
unsichere Verbindung
kompromittiertes Endgerät

Merksatz:

Session Hijacking übernimmt eine laufende Anmeldung.

Schutz vor Session Hijacking

Maßnahmen:

HTTPS überall
HttpOnly Cookies
Secure Cookies
SameSite Cookies
kurze Session-Laufzeiten
Session-Rotation nach Login
Schutz vor XSS
MFA
Geräte- und Standortprüfung
Logout-Funktion
Token widerrufen können

Merksatz:

Sitzungen müssen genauso geschützt werden wie Passwörter.

WLAN-Angriffe

WLAN ist besonders angreifbar, weil Funk nicht an Wände gebunden ist.

Typische Risiken:

schwache Verschlüsselung
unsichere Passwörter

```
Evil Twin
Rogue Access Point
unsichere Gastnetze
Abhören unverschlüsselter Verbindungen
Deauthentication-Angriffe
falsche Captive Portals
```

Merksatz:

```
WLAN braucht starke Verschlüsselung und saubere Trennung.
```

Evil Twin

Ein Evil Twin ist ein gefälschter WLAN-Access-Point, der wie ein echtes WLAN aussieht.

Ziel:

```
Benutzer verbinden sich mit dem falschen WLAN.
```

Folgen:

```
Man-in-the-Middle
Phishing
Datenmitschnitt
falsche Loginseiten
Malware-Verteilung
```

Merksatz:

```
Evil Twin imitiert ein echtes WLAN.
```

Rogue Access Point

Ein Rogue Access Point ist ein nicht autorisierter Access Point im Netzwerk.

Beispiele:

Mitarbeiter steckt eigenen WLAN-Router an.
Angreifer platziert Access Point im Gebäude.
falsch konfigurierte Geräte öffnen WLAN.

Risiko:

Sicherheitsregeln werden umgangen.
internes Netz wird unkontrolliert erreichbar.

Merksatz:

Rogue Access Point ist ein unerlaubter WLAN-Zugangspunkt.

Schutz vor WLAN-Angriffen

Maßnahmen:

WPA2-Enterprise oder WPA3 nutzen
starke Passwörter
Gastnetz vom internen Netz trennen
802.1X
Zertifikatsprüfung
Rogue-AP-Erkennung
regelmäßige WLAN-Überprüfung
sichere Captive-Portals
VPN in unsicheren WLANs
keine offenen internen WLANs

Merksatz:

WLAN-Sicherheit braucht Verschlüsselung,
Authentifizierung
und Segmentierung.

802.1X

802.1X ist ein Standard für netzwerkbasierte Zugangskontrolle.

Er wird genutzt bei:

```
LAN
WLAN
Enterprise-Netzen
```

Grundidee:

```
Gerät oder Benutzer muss sich authentifizieren,
bevor Netzwerkzugriff erlaubt wird.
```

Merksatz:

```
802.1X kontrolliert Netzwerkzugang vor der Freigabe.
```

Netzwerksegmentierung gegen Angriffe

Segmentierung trennt Netzbereiche voneinander.

Beispiele:

```
Clientnetz
Servernetz
Gastnetz
Managementnetz
Produktionsnetz
Backupnetz
WLAN-Gastnetz
IoT-Netz
```

Vorteil:

```
Angriffe können sich schlechter ausbreiten.
Zugriffe können gezielter gefiltert werden.
```

Merksatz:

Segmentierung begrenzt Schaden und Ausbreitung.

Firewall-Regeln gegen Netzwerkangriffe

Firewalls begrenzen, welche Kommunikation erlaubt ist.

Gute Regeln sind:

so eng wie möglich
dokumentiert
begründet
regelmäßig geprüft
nach Quelle,
Ziel,
Port
und Protokoll definiert

Merksatz:

Firewall-Regeln sollen erlauben,
was nötig ist,
und blockieren,
was nicht nötig ist.

IDS und IPS gegen Netzwerkangriffe

IDS:

erkennt verdächtigen Netzwerkverkehr
und meldet ihn

IPS:

erkennt verdächtigen Netzwerkverkehr
und kann ihn blockieren

Beispiele für Erkennung:

Portscans
bekannte Angriffssignaturen
ungewöhnlicher Datenverkehr
Exploit-Versuche
verdächtige DNS-Anfragen

Merksatz:

IDS erkennt.
IPS blockiert zusätzlich.

Netzwerk-Monitoring

Netzwerk-Monitoring hilft, Angriffe und Störungen zu erkennen.

Überwacht werden können:

Bandbreite
Paketverlust
Latenz
ungewöhnliche Verbindungen
DNS-Anfragen
Firewall-Drops
VPN-Zugriffe
ARP-Anomalien
DHCP-Anomalien
Portscans
DDoS-Anzeichen

Merksatz:

Netzwerk-Monitoring erkennt Auffälligkeiten im Datenverkehr.

Typische Anzeichen für Netzwerkangriffe

Mögliche Hinweise:

plötzlich sehr hohe Netzwerklast
viele fehlgeschlagene Verbindungen
ungewöhnliche DNS-Antworten
Benutzer landen auf falschen Webseiten
Zertifikatswarnungen
viele Loginversuche
unbekannte DHCP-Server
doppelte IP-Adressen
ungewöhnliche ARP-Einträge
unbekannte Access Points
viele Firewall-Drops

Merksatz:

Netzwerkangriffe zeigen sich oft durch ungewöhnliche Muster.

Fehlersuche bei Verdacht auf Netzwerkangriff

Sinnvolle Reihenfolge:

1. Betroffene Systeme bestimmen.
2. Zeitpunkt eingrenzen.
3. Änderungen prüfen.
4. Netzwerklogs prüfen.
5. Firewall-Logs prüfen.
6. DNS prüfen.
7. DHCP prüfen.
8. ARP-Tabelle prüfen.
9. Routing prüfen.
10. Paketmitschnitt erstellen.
11. Benutzerberichte vergleichen.
12. Angriff eingrenzen.
13. Schutzmaßnahmen aktivieren.
14. Vorfall dokumentieren.

Merksatz:

Netzwerkangriffe systematisch mit Logs,
Tabellen,
Routen
und Mitschnitten untersuchen.

Typische Schutzmaßnahmen gegen Netzwerkangriffe

Wichtige Maßnahmen:

Firewall
IDS
IPS
Netzwerksegmentierung
VLANs
sichere WLAN-Konfiguration
WPA2-Enterprise oder WPA3
802.1X
DHCP Snooping
Dynamic ARP Inspection
DNSSEC je nach Einsatz
TLS
VPN
DDoS-Schutz
Rate Limiting
Monitoring
Logging
Patchmanagement
sichere Router- und Switch-Konfiguration

Merksatz:

Netzwerkangriffsschutz besteht aus Technik,
Konfiguration
Überwachung
und klaren Regeln.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was ist ein DoS-Angriff?
- Was ist ein DDoS-Angriff?
- Was ist der Unterschied zwischen DoS und DDoS?
- Was ist ein Man-in-the-Middle-Angriff?
- Was bedeutet Sniffing?
- Was bedeutet Spoofing?
- Was ist IP-Spoofing?
- Was ist MAC-Spoofing?
- Was ist ARP-Spoofing?
- Was ist DNS-Spoofing?
- Was ist DNS-Cache-Poisoning?
- Was ist DNSSEC?
- Was ist Rogue DHCP?
- Was ist DHCP Snooping?
- Was ist Session Hijacking?
- Was ist ein Evil Twin?
- Was ist ein Rogue Access Point?
- Wie schützt Netzwerksegmentierung gegen Angriffe?
- Was ist der Unterschied zwischen IDS und IPS?
- Welche Schutzmaßnahmen helfen gegen DDoS?

Typische Prüfungsfallen

DoS und DDoS unterscheiden.

DDoS ist verteilt.

DoS greift Verfügbarkeit an.

MitM sitzt zwischen Kommunikationspartnern.

Sniffing ist nicht automatisch Angriff,
kann aber missbraucht werden.

Spoofing täuscht Identität oder Herkunft vor.

ARP-Spoofing betrifft lokale IPv4-Netze.

DNS-Spoofing führt Namen zu falschen IP-Adressen.

DNSSEC schützt Integrität,
nicht automatisch Vertraulichkeit.

Rogue DHCP verteilt falsche Netzwerkeinstellungen.

DHCP Snooping schützt vor falschen DHCP-Servern.

Session Hijacking betrifft laufende Sitzungen.

WLAN ist wegen Funkreichweite besonders zu schützen.

Evil Twin imitiert ein echtes WLAN.

Rogue Access Point ist ein unerlaubter Access Point.

MAC-Filter allein ist keine starke Sicherheit.

TLS-Zertifikatswarnungen nicht ignorieren.

Segmentierung begrenzt Ausbreitung.

IDS erkennt,
IPS blockiert zusätzlich.

DDoS-Schutz muss vorbereitet sein.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
DoS	Dienstverweigerung
DDoS	verteilte Dienstverweigerung
Botnet	viele fremdgesteuerte Systeme
Volumenangriff	Überlastung durch Datenmenge
Protokollangriff	Ausnutzung von Protokollmechanismen

Begriff	Kurze Erklärung
Anwendungsschichtangriff	Überlastung einer Anwendung
Reflexionsangriff	Antworten fremder Systeme treffen Opfer
Amplification	Verstärkung kleiner Anfragen
Rate Limiting	Begrenzung von Anfragen
Anycast	gleiche IP an mehreren Standorten
Blackholing	Verwerfen von Verkehr
MitM	Man-in-the-Middle
Sniffing	Mitschneiden von Netzwerkverkehr
Spoofing	Vortäuschen falscher Identität
IP-Spoofing	gefälschte Quell-IP
MAC-Spoofing	gefälschte MAC-Adresse
ARP	Zuordnung IPv4 zu MAC im LAN
ARP-Spoofing	Manipulation von ARP-Zuordnungen
DNS	Namensauflösung
DNS-Spoofing	Manipulation von DNS-Antworten
DNS-Cache-Poisoning	falsche DNS-Antwort im Cache
DNSSEC	Schutz der DNS-Integrität
Rogue DHCP	unautorisierter DHCP-Server
DHCP Snooping	Schutz vor falschen DHCP-Servern
Session Hijacking	Übernahme einer laufenden Sitzung
Evil Twin	gefälschter WLAN-Access-Point
Rogue Access Point	unerlaubter Access Point
802.1X	Netzwerkzugangskontrolle
IDS	Angriffserkennung
IPS	Angriffserkennung mit Blockierung

IHK-sichere Kurzformulierung

Netzwerkangriffe richten sich gegen Kommunikation, Erreichbarkeit, Adressierung oder Namensauflösung in Netzwerken. DoS und DDoS greifen die Verfügbarkeit von Diensten an, wobei DDoS von vielen verteilten Quellen ausgeht. Bei einem Man-in-the-Middle-Angriff befindet sich ein Angreifer zwischen zwei Kommunikationspartnern und kann Daten mitlesen oder manipulieren. Spoofing täuscht Identität oder Herkunft vor, zum Beispiel durch gefälschte IP-, MAC-, ARP- oder DNS-Informationen. Schutzmaßnahmen sind Firewalls, IDS/IPS, Netzwerksegmentierung, sichere

WLAN-Konfiguration, TLS, VPN, DNSSEC, DHCP Snooping, Dynamic ARP Inspection, DDoS-Schutz, Rate Limiting, Monitoring und Logging.

Merksätze

Netzwerkangriffe treffen Kommunikation und Erreichbarkeit.

DoS greift Verfügbarkeit an.

DDoS ist verteilter DoS.

DDoS-Schutz muss vorbereitet sein.

Volumenangriff überlastet Bandbreite.

Protokollangriff belastet Netzwerkmechanismen.

Anwendungsschichtangriff trifft Dienste auf Schicht 7.

Reflexionsangriff nutzt fremde Systeme.

Amplification verstärkt Angriffsdaten.

Rate Limiting begrenzt Anfragen.

Anycast verteilt Verkehr.

Blackholing verwirft Verkehr.

MitM sitzt zwischen Client und Server.

Sniffing schneidet Verkehr mit.

Verschlüsselung schützt gegen Mitlesen.

Spoofing täuscht Herkunft oder Identität vor.

IP-Spoofing fälscht Quell-IP.

MAC-Spoofing fälscht MAC-Adresse.

ARP verbindet IPv4 und MAC.

ARP-Spoofing manipuliert lokale Zuordnung.

DNS übersetzt Namen in IP-Adressen.

DNS-Spoofing führt zu falschen Zielen.

DNSSEC schützt DNS-Integrität.

Rogue DHCP verteilt falsche Einstellungen.

DHCP Snooping schützt vor Rogue DHCP.

Session Hijacking übernimmt Sitzungen.

WLAN braucht starke Absicherung.

Evil Twin imitiert echtes WLAN.

Rogue Access Point ist unerlaubt.

802.1X kontrolliert Netzwerkzugang.

Segmentierung begrenzt Ausbreitung.

IDS erkennt.

IPS blockiert zusätzlich.

Netzwerk-Monitoring erkennt Auffälligkeiten.

Logs und Mitschnitte helfen bei Analyse.