NETZWERKGRUNDLAGEN FÜR DEN EINSTIEG

Netzwerke verstehen und absichern

OSI, TCP/IP, Protokolle und praktische Abwehrmechanismen verständlich verbinden

> Ein kompakter Lern- und Nachschlageleitfaden: Ordne Netzwerkfunktionen den Schichten zu, verfolge den Paketweg, verstehe DNS, DHCP, ARP und NAT und wende grundlegende Firewall-, VPN- und Segmentierungsprinzipien in konkreten Szenarien an.

01 So nutzt du diese Kurzanleitung

02 1. OSI-Modell: sieben Aufgabenebenen

03 2. TCP/IP und der Paketweg

04 3. Zentrale Protokolle und typische Risiken

05 4. Basis-Abwehr: Regeln, Tunnel und Segmentierung

06 5. Praxis: verdächtige Umleitung im Büronetz

07 6. Härtungs-Checkliste

01

So nutzt du diese Kurzanleitung

Dieser Leitfaden führt vom Schichtenmodell über den Weg eines Datenpakets zu zentralen Netzwerkdiensten und Schutzmaßnahmen. Lies ihn der Reihe nach oder nutze die Abschnitte als Nachschlagehilfe. Die Beispiele sind bewusst vereinfacht; reale Netzwerke können zusätzliche Geräte, Regeln und Protokolle enthalten.

1. **Einordnen**

   Ordne eine Beobachtung einer Schicht oder einem Netzwerkdienst zu.

2. **Datenfluss verfolgen**

   Prüfe, welche Anfrage, Antwort und Weiterleitung beteiligt sind.

3. **Schutz wählen**

   Wähle eine passende Kontrolle und prüfe ihre Wirkung anhand des Szenarios.

- Beginne mit OSI und TCP/IP, um Netzwerkaufgaben einzuordnen.
- Verfolge anschließend DNS, DHCP, ARP und NAT im typischen Datenfluss.
- Nutze die Szenarien und Checklisten, um Sicherheitsentscheidungen praktisch zu prüfen.

> **Sicherheitsgrenze**
>
> Die Beispiele erklären technische Zusammenhänge und ersetzen weder eine Prüfung der eigenen Umgebung noch eine Diagnose oder konkrete Behandlungsempfehlung für einen Sicherheitsvorfall.

02

1. OSI-Modell: sieben Aufgabenebenen

Das OSI-Referenzmodell zerlegt Kommunikation in sieben logisch aufeinander aufbauende Schichten. Es ist ein Denk- und Diagnosemodell, keine zwingende Abbildung jeder konkreten Implementierung. Beim Senden wird Information schrittweise verpackt; beim Empfang werden die jeweiligen Protokollinformationen wieder ausgewertet.

1. **Anwendung erzeugt Daten**

   Ein Programm erstellt beispielsweise eine DNS-Anfrage oder eine Webanfrage.

2. **Schichten ergänzen Informationen**

   Transport, IP und Link fügen jeweils eigene Steuerinformationen hinzu; auf dem Medium werden Signale übertragen.

3. **Netz leitet weiter**

   Router werten IP-Informationen aus und wählen den nächsten Netzpfad; lokale Link-Informationen gelten jeweils für den betreffenden Link.

4. **Empfang setzt zusammen**

   Das Zielsystem verarbeitet die Informationen schichtweise und übergibt Nutzdaten an den passenden Dienst.

- 7 Anwendung: Dienste für Programme, etwa HTTP oder DNS.
- 6 Darstellung: Datenformate, Kodierung und gegebenenfalls Verschlüsselungsfunktionen.
- 5 Sitzung: Aufbau und Verwaltung logischer Dialoge.
- 4 Transport: Ende-zu-Ende-Kommunikation; TCP bietet geordnete, zuverlässige Übertragung, UDP datagrammbasierte Übertragung ohne eingebaute Zustellgarantie.
- 3 Vermittlung: logische Adressierung und Weiterleitung, vor allem IP.
- 2 Sicherung: Übertragung innerhalb eines lokalen Links, etwa Ethernet oder WLAN; Frames und MAC-Adressen.
- 1 Bitübertragung: elektrische, optische oder Funk-Signale und physische Medien.

> **Fehler eingrenzen**
>
> Funktioniert die Funkverbindung nicht, prüfe zuerst Medium und Link. Ist der Link intakt, aber ein Zielnetz unerreichbar, sind IP-Konfiguration und Routing naheliegender. Ein funktionierender Netzwerkpfad garantiert noch nicht, dass der Anwendungsdienst verfügbar ist.

03

2. TCP/IP und der Paketweg

Die Internetprotokollfamilie wird oft als TCP/IP-Stack beschrieben. Eine gebräuchliche Vier-Schichten-Darstellung fasst die OSI-Schichten 5 bis 7 zur Anwendungsschicht zusammen. Die Zuordnung ist eine Orientierung, keine perfekte Eins-zu-eins-Übersetzung: Protokolle und Funktionen können mehrere Schichten berühren.

1. **Dienst bestimmen**

   Die Anwendung wählt ein Ziel, etwa einen Hostnamen und einen Dienst.

2. **Transport zuordnen**

   TCP oder UDP transportiert Daten zwischen Endpunkten; Ports ordnen sie den jeweiligen Diensten zu.

3. **IP weiterleiten**

   IP-Pakete werden anhand ihrer Zieladresse über Router in Richtung Zielnetz vermittelt.

4. **Link zustellen**

   Auf jedem einzelnen Link werden passende lokale Link-Informationen verwendet; am nächsten Hop kann der Link-Rahmen neu entstehen.

- Anwendung: etwa HTTP, DNS und DHCP; Anwendungen nutzen Dienste darunter.
- Transport: TCP oder UDP; Ports unterscheiden Dienste auf einem Endsystem.
- Internet: IP-Adressierung und Weiterleitung zwischen Netzen.
- Netzzugang/Link: Zugriff auf das jeweilige Übertragungsmedium, zum Beispiel Ethernet oder WLAN.

> **Adresse ist nicht gleich Adresse**
>
> Eine IP-Adresse hilft, ein Ziel über Netze hinweg zu erreichen. Eine MAC-Adresse wird für die Zustellung auf einem lokalen Link verwendet. Ein Port bezeichnet einen Transportdienst auf einem Endsystem; er ist keine Geräteadresse.

04

3. Zentrale Protokolle und typische Risiken

Netzwerkdienste machen Kommunikation praktikabel, eröffnen aber auch Angriffsflächen. Die folgenden Risiken sind Beispiele für mögliche Fehlkonfigurationen oder Angriffe, keine Aussage, dass ein Protokoll allein eine Schwachstelle bedeutet.

1. **Client startet**

   Ein Gerät benötigt Netzwerkparameter und fragt gegebenenfalls per DHCP nach Konfiguration.

2. **Name wird aufgelöst**

   Der Client fragt seinen konfigurierten Resolver nach der Adresse eines Zielnamens.

3. **Lokaler Hop wird gefunden**

   Für ein Ziel im lokalen IPv4-Link kann ARP die passende MAC-Adresse ermitteln; bei einem entfernten Ziel gilt das typischerweise für das Gateway.

4. **Paket wird weitergeleitet**

   Router leiten IP-Verkehr weiter; am Netzrand kann NAT Adressinformationen übersetzen. Eine Firewall-Regel entscheidet unabhängig davon über erlaubten Verkehr.

- DNS übersetzt Namen in Ressourcendaten, häufig IP-Adressen. Manipulierte Antworten, unerwünschte Umleitungen oder Missbrauch offener Resolver sind mögliche Risiken. Prüfe Resolverzugriff, Protokollierung und Schutz der Antworten passend zur Umgebung.
- DHCP verteilt Konfigurationsdaten wie IP-Adresse, Präfix, Gateway und DNS-Server an Clients. Ein unberechtigter DHCP-Server kann falsche Werte ausgeben; begrenze daher, welche Geräte DHCP-Antworten liefern dürfen.
- ARP ordnet in IPv4-Netzen lokale IPv4-Adressen MAC-Adressen zu. Gefälschte ARP-Antworten im selben lokalen Netz können Verkehr umleiten oder stören. Segmentierung und geeignete Switch-Schutzfunktionen können das Risiko reduzieren.
- NAT verändert bei der Weiterleitung typischerweise IP-Adressen und oft auch Ports. NAT ist keine Firewall-Garantie und ersetzt keine Zugriffskontrolle; explizite Freigaben können erreichbare Dienste nach außen sichtbar machen.

> **DNS ist nicht automatisch verschlüsselt**
>
> Traditionelle DNS-Abfragen können für Netzbeobachter sichtbar sein. Verschlüsselte DNS-Verfahren schützen den Transport zum Resolver, lösen aber nicht automatisch alle Fragen zu Vertrauen, Richtlinien oder falschen Zielsystemen.

05

4. Basis-Abwehr: Regeln, Tunnel und Segmentierung

Schutz entsteht aus mehreren aufeinander abgestimmten Kontrollen. Eine Firewall filtert Verkehr anhand von Regeln; ein VPN schützt einen Kommunikationsweg; Segmentierung begrenzt, welche Systeme einander erreichen können. Keine einzelne Maßnahme macht ein Netz automatisch sicher.

1. **Schutzbedarf erfassen**

   Notiere Systeme, Daten und erforderliche Kommunikationsbeziehungen.

2. **Bereiche festlegen**

   Trenne unterschiedliche Vertrauens- und Funktionsbereiche in geeignete Segmente oder VLANs.

3. **Verbindungen begrenzen**

   Erlaube nur dokumentierte Quellen, Ziele, Protokolle und Dienste; verwirf nicht benötigten Verkehr.

4. **Fernzugriff absichern**

   Nutze einen passend konfigurierten VPN-Zugang mit starker Authentisierung und begrenzten Berechtigungen.

5. **Wirksamkeit prüfen**

   Teste erlaubte und unerlaubte Pfade, protokolliere relevante Ereignisse und passe Regeln bei Änderungen an.

- Paketfilter prüfen ausgewählte Headerfelder und erlauben oder verwerfen Verkehr nach Regeln.
- Stateful Firewalls verfolgen den Zustand von Verbindungen und können Rückverkehr zu einer erlaubten Sitzung zuordnen. Regeln sollten nur benötigte Richtungen, Dienste und Quellen freigeben.
- Next-Generation-Firewalls können zusätzlich Funktionen wie Anwendungs- oder Bedrohungserkennung anbieten. Erkennung hängt von Konfiguration, Sichtbarkeit und Grenzen der jeweiligen Technik ab.
- IPsec schützt IP-Kommunikation auf Netzwerkebene, häufig für Standort- oder Remote-Verbindungen. TLS-basierte VPNs schützen den Tunnel auf Basis von TLS. Beide benötigen sichere Authentisierung, passende Konfiguration und Schlüsselpflege.
- VLANs teilen ein Layer-2-Netz logisch auf. Kommunikation zwischen VLANs läuft üblicherweise über Routing und kann dort durch Regeln kontrolliert werden; ein VLAN allein ist keine vollständige Sicherheitsgrenze.
- Segmentiere nach Zweck und Vertrauensniveau, zum Beispiel Clients, Server und Administration. Erlaube zwischen Bereichen nur begründete Verbindungen und überprüfe Ausnahmen regelmäßig.

> **Firewall und NAT unterscheiden**
>
> NAT verändert Adressinformationen; eine Firewall setzt Zugriffsregeln durch. Heimrouter kombinieren häufig beide Funktionen, doch die Konzepte sind nicht austauschbar.

06

5. Praxis: verdächtige Umleitung im Büronetz

Szenario: Ein Arbeitsplatz erreicht plötzlich eine unerwartete Anmeldeseite. Das allein beweist keinen Angriff. Eine strukturierte Prüfung hilft, Namensauflösung, lokale Konfiguration und Netzpfad auseinanderzuhalten, ohne vorschnell eine Ursache zu behaupten.

1. **Beobachtung festhalten**

   Notiere Gerät, Zeitpunkt, betroffenen Namen und genaue Meldung, ohne Zugangsdaten auf der verdächtigen Seite einzugeben.

2. **Konfiguration vergleichen**

   Prüfe DHCP-Gateway und DNS-Server gegen die freigegebene Netzkonfiguration.

3. **Lokalen Pfad prüfen**

   Lass zuständige Personen ARP-Zuordnung, Switch-Port und Segmentkonfiguration vergleichen.

4. **Eindämmen und melden**

   Folge dem Incident-Prozess; Änderungen oder Trennung vom Netz nur nach geltender Zuständigkeit und Richtlinie.

- Vergleiche die aufgelöste Zieladresse mit einem bekannten, vertrauenswürdigen Referenzweg oder internen Dokumentation.
- Prüfe, ob der Client unerwartete DHCP-Konfiguration oder einen unbekannten DNS-Resolver erhalten hat.
- Bei Verdacht auf ARP-Manipulation: Beobachtung durch Netzwerkverantwortliche im betroffenen Segment prüfen lassen; nicht eigenmächtig andere Geräte angreifen oder scannen.
- Melde den Vorfall nach dem lokalen Verfahren und sichere relevante Zeitpunkte, Fehlermeldungen und Konfigurationsdaten.

> **Vorsicht bei Belegen**
>
> Eine abweichende DNS-Antwort oder MAC-Zuordnung ist ein Hinweis zur Untersuchung, aber nicht allein ein Beweis für böswillige Aktivität. Auch Änderungen, Caches oder legitime Netzwerkdienste können Unterschiede verursachen.

07

6. Härtungs-Checkliste

Diese kurze Prüfung eignet sich für ein kleines Lern- oder Testnetz. In produktiven Umgebungen müssen Regeln, Zuständigkeiten und Änderungen zur jeweiligen Organisation passen.

- [ ] Geräte und Netzwerkbereiche sind inventarisiert; unnötige Dienste sind deaktiviert.
- [ ] DHCP- und DNS-Konfiguration ist auf vorgesehene Server beziehungsweise Resolver begrenzt.
- [ ] Firewall-Regeln dokumentieren Zweck, Quelle, Ziel, Dienst und verantwortliche Stelle.
- [ ] Verwaltungszugänge sind getrennt und nur für berechtigte Systeme erreichbar.
- [ ] VPN-Zugänge verwenden starke Authentisierung und werden auf benötigte Ziele beschränkt.
- [ ] VLAN- und Routing-Regeln wurden für erlaubte sowie nicht erlaubte Verbindungen getestet.
- [ ] Protokolle und Alarme sind für relevante Infrastrukturereignisse verfügbar; Aufbewahrung und Zugriff sind geregelt.
- [ ] Änderungen und Ausnahmen werden überprüft und nicht mehr benötigte Freigaben entfernt.

> **Klein anfangen**
>
> Für ein Heim- oder Übungsnetz genügt als erster Schritt oft ein Netzplan mit Geräten, Gateway, DNS-Quelle und den tatsächlich benötigten Freigaben. Dokumentiere, was du geändert hast, damit du Fehler zurückverfolgen kannst.