11.4 DMZ und Sicherheitszonen im Detail

DMZ steht für:

```
Demilitarized Zone
```

Eine DMZ ist ein separates Netzwerksegment für Dienste, die von außen erreichbar sein müssen.

Typische Dienste in einer DMZ:

```
- Webserver
- Reverse Proxy
- Mailgateway
- VPN-Gateway
- öffentlicher DNS-Server
- öffentliche API
- Proxyserver
- Bastion Host
```

Merksatz:

```
DMZ = eigenes Netz für öffentlich erreichbare Dienste.
```

Warum braucht man eine DMZ?

Öffentlich erreichbare Dienste sind stärker gefährdet als rein interne Dienste.

Beispiel:

```
Ein Webserver ist aus dem Internet erreichbar.
```

Wenn dieser Webserver kompromittiert wird, soll der Angreifer nicht direkt Zugriff auf das interne LAN bekommen.

Die DMZ trennt deshalb öffentliche Dienste vom internen Netz.

Merksatz:

Eine DMZ begrenzt den Schaden,
wenn ein öffentlich erreichbarer Dienst angegriffen wird.

Grundidee einer DMZ

Eine DMZ liegt logisch zwischen:

externem Netz
und
internem Netz

Vereinfacht:

Internet
→ Firewall
→ DMZ
→ Firewall-Regeln
→ internes LAN

Die DMZ ist nicht so vertrauenswürdig wie das interne LAN.

Aber sie ist kontrollierter als das Internet.

Merksatz:

DMZ liegt kontrolliert zwischen außen und innen.

DMZ ist nicht das interne LAN

Ein häufiger Fehler ist:

Ein öffentlich erreichbarer Server steht direkt im internen LAN.

Das ist riskant.

Besser:

öffentliche Dienste in DMZ stellen
und Zugriffe ins LAN stark einschränken.

Warum?

Wird ein DMZ-System kompromittiert,
soll der Angreifer nicht automatisch interne Clients,
Server oder Verwaltungsdienste erreichen.

Merksatz:

Öffentliche Dienste gehören nicht ungefiltert ins interne LAN.

DMZ als Sicherheitszone

Eine DMZ ist eine Sicherheitszone.

Eine Sicherheitszone ist ein Netzbereich mit eigenem Schutzbedarf.

Typische Zonen:

- WAN
- LAN
- DMZ
- Servernetz
- Managementnetz
- Gastnetz
- IoT-Netz
- VPN-Zone

Zwischen diesen Zonen gelten Firewall-Regeln.

Merksatz:

Sicherheitszonen trennen Netze nach Vertrauensniveau.

Vertrauensniveau von Zonen

Nicht jedes Netz ist gleich vertrauenswürdig.

Beispiel:

Zone	Vertrauensniveau	Beispiel
WAN	sehr gering	Internet
Gastnetz	gering	Besuchergeräte
IoT-Netz	gering bis mittel	Kameras, Sensoren
DMZ	mittel / eingeschränkt	öffentliche Dienste
LAN	höher	interne Clients
Servernetz	hoch	interne Server
Managementnetz	sehr hoch	Adminzugänge

Merksatz:

```
Je kritischer eine Zone ist,
desto strenger müssen Zugriffe kontrolliert werden.
```

Typischer Drei-Zonen-Aufbau

Ein klassischer Aufbau besteht aus drei Zonen:

```
WAN
DMZ
LAN
```

WAN:

```
externes Netz oder Internet
```

DMZ:

```
öffentliche Dienste
```

LAN:

```
internes Unternehmensnetz
```

Merksatz:

> Drei-Zonen-Aufbau = WAN, DMZ, LAN.

Beispielaufbau

Vereinfacht:

```
Internet
   |
 Firewall
 /    \
DMZ    LAN
Web    Clients
Mail   interne Server
```

Die Firewall kontrolliert, welche Zone mit welcher Zone kommunizieren darf.

Merksatz:

> Die Firewall ist der kontrollierte Übergang zwischen den Zonen.

Regelidee Internet zur DMZ

Vom Internet zur DMZ sollte nur erlaubt sein, was wirklich öffentlich erreichbar sein muss.

Beispiele:

Quelle	Ziel	Dienst	Aktion
Internet	Reverse Proxy DMZ	HTTPS TCP 443	erlauben
Internet	Mailgateway DMZ	SMTP TCP 25	erlauben
Internet	VPN-Gateway DMZ	VPN-Port	erlauben
Internet	DMZ-Server	SSH TCP 22	blockieren
Internet	interne Server	any	blockieren

Merksatz:

> Internet darf nur notwendige öffentliche Dienste in der DMZ erreichen.

Regelidee DMZ zum LAN

Von der DMZ ins LAN sollte sehr wenig erlaubt sein.

Beispiele:

Quelle	Ziel	Dienst	Aktion
Reverse Proxy DMZ	interner Webdienst	TCP 8080	erlauben
Webserver DMZ	Datenbankserver	TCP 5432	nur wenn nötig
Mailgateway DMZ	interner Mailserver	SMTP	nur gezielt
DMZ allgemein	LAN allgemein	any	blockieren

Wichtig:

```
DMZ darf keine freie Brücke ins interne Netz sein.
```

Merksatz:

```
Von DMZ ins LAN nur das zwingend Notwendige erlauben.
```

Regelidee LAN zur DMZ

Das interne LAN darf je nach Bedarf Dienste in der DMZ erreichen.

Beispiele:

```
interne Clients → DMZ-Webserver HTTPS

Admin-Netz → DMZ-Server SSH

Monitoring → DMZ-Systeme SNMP
```

Aber auch hier gilt:

```
nicht alles für jeden erlauben.
```

Merksatz:

```
Auch LAN zur DMZ sollte gezielt geregelt werden.
```

Regelidee Management zur DMZ

Administration sollte nicht aus beliebigen Netzen erlaubt sein.

Besser:

```
Managementnetz
oder
Bastion Host
oder
VPN-Adminzugang
```

Beispiel:

```
Managementnetz → DMZ-Server SSH TCP 22 erlauben
```

Aber nicht:

```
gesamtes LAN → DMZ-Server SSH erlauben
```

Und erst recht nicht:

```
Internet → DMZ-Server SSH erlauben
```

Merksatz:

```
Administration nur aus kontrollierten Managementbereichen erlauben.
```

DMZ und Reverse Proxy

Ein Reverse Proxy steht häufig in der DMZ.

Er nimmt externe HTTPS-Anfragen entgegen und leitet sie an interne Dienste weiter.

Beispiel:

```
Internet → Reverse Proxy DMZ → interner Wiki-Server
```

Vorteile:

```
- zentrale TLS-Verwaltung
- weniger direkte Veröffentlichung interner Server
- mehrere Dienste über eine öffentliche IP
- Zugriffskontrolle
- bessere Protokollierung
- Trennung zwischen extern und intern
```

Merksatz:

```
Reverse Proxy in der DMZ schützt interne Webdienste besser als direkte Freigabe.
```

DMZ und Webserver

Ein Webserver in der DMZ kann öffentliche Webseiten bereitstellen.

Wichtig:

```
Der Webserver sollte nur die internen Systeme erreichen,
die er wirklich braucht.
```

Beispiel:

```
Webserver braucht Datenbankzugriff.
```

Dann gilt:

```
Webserver DMZ → Datenbankserver TCP 5432 erlauben
```

Aber nicht:

```
Webserver DMZ → gesamtes LAN any erlauben
```

Merksatz:

```
Webserver in DMZ nur mit notwendigen Backend-Zugriffen ausstatten.
```

DMZ und Mailgateway

Ein Mailgateway in der DMZ kann E-Mails aus dem Internet annehmen.

Typische Aufgabe:

```
Internet → Mailgateway DMZ
Mailgateway prüft Spam und Malware
Mailgateway leitet an internen Mailserver weiter
```

Vorteil:

```
Der interne Mailserver steht nicht direkt im Internet.
```

Merksatz:

```
Mailgateway in der DMZ schützt interne Mailserver.
```

DMZ und VPN-Gateway

Ein VPN-Gateway kann in der DMZ stehen.

Ablauf:

```
externer Benutzer verbindet sich zum VPN-Gateway

nach erfolgreicher Anmeldung erhält er Zugriff auf erlaubte interne Ressourcen
```

Wichtig:

```
VPN-Zugriff darf nicht automatisch das gesamte LAN erlauben.
```

Besser:

```
VPN-Benutzer in eigene Zone einordnen
und gezielte Regeln setzen.
```

Merksatz:

```
VPN-Gateway kann in der DMZ stehen,
aber VPN-Rechte müssen begrenzt werden.
```

DMZ und öffentlicher DNS

Ein öffentlicher DNS-Server kann in einer DMZ stehen, wenn eine Organisation eigene öffentliche DNS-Zonen bereitstellt.

Wichtig:

```
öffentlicher DNS sollte nur öffentliche Informationen enthalten.
```

Interne Servernamen sollten nicht öffentlich sichtbar sein.

Merksatz:

```
Öffentlicher DNS darf keine internen Strukturen verraten.
```

DMZ und Bastion Host

Ein Bastion Host ist ein besonders abgesicherter Sprungserver.

Er kann genutzt werden, um administrative Zugriffe auf DMZ-Systeme zu bündeln.

Ablauf:

```
Admin → VPN oder Managementnetz → Bastion Host → DMZ-System
```

Vorteile:

```
- zentrale Kontrolle
- bessere Protokollierung
- weniger direkte Adminzugänge
```

- zusätzliche Sicherheitsprüfung

Merksatz:

Bastion Host bündelt und kontrolliert Adminzugriffe.

Bastion Host ist besonders kritisch

Ein Bastion Host hat oft Zugriff auf wichtige Systeme.

Deshalb muss er besonders geschützt werden.

Maßnahmen:

- MFA
- starke Authentifizierung
- nur Admins erlauben
- Protokollierung
- regelmäßige Updates
- keine unnötigen Dienste
- harte Firewall-Regeln
- Monitoring
- getrennte Admin-Konten

Merksatz:

Bastion Host stark absichern,
weil er ein zentraler Zugangspunkt ist.

DMZ und Datenbankserver

Datenbankserver sollten normalerweise nicht direkt in der öffentlichen DMZ stehen.

Besser:

Datenbank im internen Servernetz
und nur gezielter Zugriff vom Webserver oder Anwendungsserver

Beispiel:

```
Webserver DMZ → Datenbankserver TCP 5432
```

Wichtig:

```
kein allgemeiner Zugriff von Internet oder DMZ auf Datenbank.
```

Merksatz:

```
Datenbanken nicht öffentlich platzieren.
```

DMZ und interne Daten

DMZ-Systeme sollten möglichst wenig interne Daten enthalten.

Warum?

```
Sie sind stärker exponiert.
```

Wenn sensible Daten in der DMZ liegen, ist das Risiko bei einem Angriff höher.

Besser:

```
DMZ-Systeme nur mit notwendigen Daten ausstatten
und interne Datenbanken geschützt halten.
```

Merksatz:

```
In der DMZ nur Daten,
die dort wirklich benötigt werden.
```

DMZ und Protokollierung

DMZ-Systeme sollten gut protokolliert werden.

Wichtige Logs:

- Firewall-Logs
- Webserver-Logs
- Reverse-Proxy-Logs
- Authentifizierungslogs
- Systemlogs
- IDS/IPS-Logs
- VPN-Logs
- Mailgateway-Logs

Logs helfen bei:

- Angriffserkennung
- Fehlersuche
- Nachvollziehbarkeit
- Sicherheitsanalyse

Merksatz:

DMZ-Systeme brauchen gute Logs.

DMZ und Monitoring

DMZ-Systeme sollten überwacht werden.

Typische Prüfwerte:

- Erreichbarkeit
- CPU
- RAM
- Speicherplatz
- Dienste
- Zertifikate
- Loggröße
- ungewöhnliche Verbindungen
- fehlgeschlagene Logins
- Updates
- offene Ports

Merksatz:

```
DMZ-Systeme müssen aktiv überwacht werden.
```

DMZ und IDS/IPS

IDS steht für:

```
Intrusion Detection System
```

IPS steht für:

```
Intrusion Prevention System
```

IDS erkennt verdächtigen Verkehr.

IPS kann verdächtigen Verkehr zusätzlich blockieren.

In einer DMZ können IDS/IPS-Systeme helfen, Angriffe auf öffentliche Dienste zu erkennen.

Merksatz:

```
IDS erkennt.
IPS blockiert zusätzlich.
```

DMZ und WAF

WAF steht für:

```
Web Application Firewall
```

Eine WAF schützt Webanwendungen auf Anwendungsebene.

Sie prüft zum Beispiel HTTP-Anfragen auf:

```
- SQL-Injection
- Cross-Site Scripting
- ungewöhnliche Muster
```

```
- bekannte Angriffsversuche
- fehlerhafte Requests
```

Eine WAF ersetzt keine sichere Anwendung, kann aber zusätzlichen Schutz bieten.

Merksatz:

```
WAF schützt Webanwendungen auf Schicht 7.
```

DMZ und TLS

Öffentliche Dienste in der DMZ nutzen häufig TLS.

Beispiele:

```
HTTPS
SMTPS
IMAPS
LDAPS
VPN mit Zertifikaten
```

Wichtig:

```
Zertifikate aktuell halten
private Schlüssel schützen
TLS-Versionen sicher konfigurieren
Zertifikatskette vollständig liefern
```

Merksatz:

```
Öffentliche Dienste brauchen saubere TLS-Konfiguration.
```

TLS-Terminierung in der DMZ

TLS-Terminierung bedeutet:

```
TLS endet am Reverse Proxy oder Load Balancer.
```

Ablauf:

```
Client → HTTPS → Reverse Proxy DMZ
Reverse Proxy → HTTP oder HTTPS → Backend
```

Vorteile:

```
- zentrale Zertifikatsverwaltung
- Entlastung der Backendserver
- bessere Kontrolle
- einheitliche Sicherheitsrichtlinien
```

Wichtig:

```
Die interne Verbindung sollte je nach Schutzbedarf ebenfalls gesichert werden.
```

Merksatz:

```
TLS-Terminierung beendet TLS an einem zentralen Punkt.
```

TLS Passthrough

TLS Passthrough bedeutet:

```
Die TLS-Verbindung wird durchgereicht,
ohne am Proxy entschlüsselt zu werden.
```

Ablauf:

```
Client → TLS → Proxy → TLS → Backend
```

Vorteil:

```
Ende der TLS-Verbindung liegt am Backend.
```

Nachteil:

Proxy kann Inhalte weniger gut prüfen oder steuern.

Merksatz:

TLS Passthrough reicht verschlüsselten Verkehr weiter.

DMZ und Updates

DMZ-Systeme sind oft exponiert.

Deshalb sind Updates besonders wichtig.

Betroffen sind:

- Betriebssystem
- Webserver
- Reverse Proxy
- Anwendung
- Frameworks
- Bibliotheken
- VPN-Software
- Mailgateway
- TLS-Komponenten

Merksatz:

Exponierte Systeme müssen besonders konsequent aktualisiert werden.

DMZ und Härtung

Härtung bedeutet:

Systeme sicher konfigurieren und unnötige Angriffsflächen reduzieren.

Maßnahmen:

- unnötige Dienste deaktivieren
- Standardpasswörter ändern
- Adminzugänge beschränken
- Updates einspielen
- Dateirechte prüfen
- sichere TLS-Konfiguration
- Logging aktivieren
- nur notwendige Ports öffnen
- Dienstkonten begrenzen

Merksatz:

Härtung reduziert Angriffsfläche.

DMZ und Least Privilege

Auch in der DMZ gilt:

nur notwendige Rechte vergeben.

Beispiele:

Webdienstkonto braucht keinen Domain-Admin.
Reverse Proxy braucht nur Zugriff auf definierte Backends.
Monitoring braucht nur Leserechte.
Adminzugriff nur für Admins.

Merksatz:

Least Privilege gilt auch für Dienste und Server.

DMZ und Netzwerksegmentierung

Netzwerksegmentierung bedeutet:

Netzbereiche werden getrennt,
damit nicht alle Systeme frei miteinander kommunizieren können.

Die DMZ ist ein Beispiel für Segmentierung.

Weitere Segmentierung:

- Servernetz
- Datenbanknetz
- Managementnetz
- Backupnetz
- Gastnetz
- IoT-Netz

Merksatz:

Segmentierung begrenzt Bewegungsfreiheit bei Angriffen.

Laterale Bewegung

Laterale Bewegung bedeutet:

Ein Angreifer bewegt sich nach einem ersten Einbruch weiter im Netzwerk.

Beispiel:

Angriff auf Webserver in DMZ.
Danach Versuch,
interne Server oder Datenbanken zu erreichen.

Segmentierung und Firewall-Regeln sollen das erschweren.

Merksatz:

DMZ soll laterale Bewegung ins LAN erschweren.

DMZ und Zero Trust

Zero Trust bedeutet vereinfacht:

```
keinem Zugriff automatisch vertrauen.
```

Auch DMZ-Systeme werden nicht automatisch als sicher betrachtet.

Prinzipien:

```
- Identität prüfen
- Zugriff begrenzen
- Verbindungen protokollieren
- nur notwendige Dienste erlauben
- Systeme überwachen
- Rechte regelmäßig prüfen
```

Merksatz:

```
Auch innerhalb des Netzes nicht blind vertrauen.
```

DMZ und Hochverfügbarkeit

Öffentliche Dienste sollen oft zuverlässig erreichbar sein.

Möglichkeiten:

```
- zwei Firewalls
- zwei Reverse Proxys
- Load Balancer
- redundante Internetanschlüsse
- mehrere Server
- Monitoring
- automatischer Failover
- regelmäßige Backups
```

Merksatz:

```
DMZ-Dienste brauchen je nach Kritikalität Verfügbarkeit und Redundanz.
```

DMZ und Backup

DMZ-Systeme brauchen Backups, aber Backups dürfen nicht unsicher erreichbar sein.

Wichtig:

- Backupzugriff einschränken
- Backupdaten schützen
- keine Schreibrechte aus DMZ auf zentrale Backups ohne Kontrolle
- Wiederherstellung testen
- Ransomware-Risiko beachten

Merksatz:

DMZ-Systeme sichern,
aber Backup-Infrastruktur schützen.

DMZ und Datenfluss

Bei einer DMZ muss man Datenflüsse genau kennen.

Fragen:

Wer spricht mit wem?
Welche Anwendung?
Welcher Port?
Welche Richtung?
Welche Daten?
Wie sensibel sind die Daten?
Wird verschlüsselt?
Wird protokolliert?
Ist der Zugriff notwendig?

Merksatz:

DMZ-Regeln entstehen aus klaren Datenflüssen.

Datenflussdiagramm für DMZ

Ein einfaches Datenflussdiagramm kann zeigen:

```
Internet → Reverse Proxy TCP 443

Reverse Proxy → interner Webdienst TCP 8080

interner Webdienst → Datenbank TCP 5432

Monitoring → Reverse Proxy SNMP oder Agent-Port

Admin-Netz → Reverse Proxy SSH
```

So erkennt man, welche Regeln wirklich nötig sind.

Merksatz:

```
Datenflüsse sichtbar machen,
bevor Regeln erstellt werden.
```

DMZ und Richtung der Verbindungen

Die Richtung der Verbindung ist wichtig.

Beispiel:

```
Internet startet Verbindung zum Reverse Proxy.

Reverse Proxy startet Verbindung zum Backend.

Backend sollte normalerweise nicht beliebig Verbindungen ins Internet starten.
```

Firewall-Regeln müssen nach der tatsächlichen Verbindungsrichtung erstellt werden.

Merksatz:

```
Regeln nach Verbindungsstart planen.
```

DMZ und ausgehender Verkehr

Auch ausgehender Verkehr aus der DMZ sollte kontrolliert werden.

Warum?

Ein kompromittiertes DMZ-System könnte versuchen:

- Schadsoftware nachzuladen
- Daten abzuziehen
- Verbindung zu Command-and-Control-Servern aufzubauen
- interne Systeme zu scannen
- Spam zu versenden

Merksatz:

DMZ outbound nicht blind erlauben.

DMZ und DNS

DMZ-Systeme brauchen oft DNS.

Aber:

Sie sollten möglichst definierte DNS-Resolver nutzen.

Regelidee:

DMZ-Systeme → interner oder DMZ-DNS UDP/TCP 53 erlauben

Nicht ideal:

DMZ-Systeme → beliebige externe DNS-Server erlauben

Merksatz:

DNS aus der DMZ kontrollieren.

DMZ und NTP

DMZ-Systeme brauchen korrekte Uhrzeit.

NTP ist wichtig für:

```
- Zertifikate
- Logs
- Authentifizierung
- Monitoring
- Fehlersuche
```

Regelidee:

```
DMZ-Systeme → freigegebener NTP-Server UDP 123
```

Merksatz:

```
DMZ-Systeme brauchen kontrollierte Zeitsynchronisation.
```

DMZ und Namenskonzept

Ein sauberes Namenskonzept hilft bei DMZ-Diensten.

Beispiele:

```
extern:
www.firma.de
vpn.firma.de
mail.firma.de

intern:
reverseproxy01.dmz.firma.local
mailgw01.dmz.firma.local
```

Wichtig:

```
öffentliche Namen,
interne Namen
und Zertifikate müssen zusammenpassen.
```

Merksatz:

```
DNS-Namen und Zertifikate sauber planen.
```

DMZ und interne Authentifizierung

Manchmal müssen DMZ-Dienste Benutzer gegen interne Verzeichnisdienste prüfen.

Beispiel:

```
Webanwendung in DMZ nutzt LDAP oder SSO.
```

Problem:

```
Direkter Zugriff aus DMZ auf interne Domain Controller kann riskant sein.
```

Mögliche Lösungen:

```
- gezielte LDAPS-Regeln
- Reverse Proxy mit Authentifizierung
- Federation / SSO
- getrennte Identitätsdienste
- Proxy-Dienst für Authentifizierung
```

Merksatz:

```
Authentifizierung aus der DMZ ins LAN nur gezielt und sicher erlauben.
```

DMZ und Datenbankzugriff

Wenn DMZ-Systeme Datenbankzugriff brauchen, sollte dieser stark begrenzt werden.

Prüfen:

```
Muss die Datenbank wirklich intern stehen?
Welche Quelle darf zugreifen?
Welcher Port?
```

```
Welches Konto?
Welche Rechte?
Ist TLS nötig?
Gibt es Protokollierung?
Gibt es Eingabevalidierung in der Anwendung?
```

Merksatz:

```
Datenbankzugriff aus der DMZ ist kritisch.
```

DMZ und direkte Internetzugriffe

Nicht jedes DMZ-System braucht freien Internetzugang.

Beispiele für notwendige ausgehende Verbindungen:

```
Updateserver
Zertifikatsprüfung
Paketquellen
Monitoring
externe API
```

Besser:

```
gezielte Ziele erlauben
oder
Proxy nutzen
```

Merksatz:

```
DMZ-Systeme nicht beliebig ins Internet lassen.
```

DMZ und öffentliche APIs

Öffentliche APIs sollten besonders geschützt werden.

Maßnahmen:

- HTTPS
- Authentifizierung
- Autorisierung
- Rate Limiting
- Eingabevalidierung
- Logging
- Monitoring
- WAF
- API-Gateway
- keine unnötigen Daten ausgeben

Merksatz:

Öffentliche API = stark exponierter Schicht-7-Dienst.

DMZ und Fehlersuche

Bei DMZ-Problemen prüft man systematisch:

1. DNS zeigt richtig?
2. öffentliche IP korrekt?
3. NAT oder Portweiterleitung korrekt?
4. Firewall-Regel WAN → DMZ korrekt?
5. Dienst in DMZ läuft?
6. Host-Firewall erlaubt Zugriff?
7. Zertifikat passt?
8. Proxy leitet korrekt weiter?
9. Regel DMZ → Backend korrekt?
10. Backend läuft?
11. Logs prüfen.

Merksatz:

DMZ-Fehlersuche braucht DNS,
NAT,
Firewall,
Dienst
und Backend.

Fehlerbild: Öffentlicher Webdienst nicht erreichbar

Mögliche Ursachen:

- DNS zeigt auf falsche öffentliche IP
- NAT-Regel fehlt
- Firewall-Regel fehlt
- Reverse Proxy down
- Webserver hört nicht auf Port
- Host-Firewall blockiert
- Zertifikatfehler
- falscher virtueller Host
- Backend nicht erreichbar
- Provider oder CGNAT-Problem

Merksatz:

Öffentlicher Webdienst braucht komplette Kette von DNS bis Backend.

Fehlerbild: Reverse Proxy zeigt 502

Mögliche Ursachen:

- Backend läuft nicht
- falscher Backend-Port
- falsches Protokoll HTTP/HTTPS
- Firewall DMZ → Backend blockiert
- Backend-DNS falsch
- Container-Name oder interner Hostname falsch
- Backend antwortet ungültig
- Timeout

Merksatz:

502 bedeutet oft:
Proxy erreicht Backend nicht sauber.

Fehlerbild: DMZ-Server erreicht LAN nicht

Mögliche Ursachen:

- Firewall-Regel fehlt
- falsche Richtung
- falsches Ziel
- falscher Port
- Route fehlt
- Rückweg fehlt
- Zielserver-Firewall blockiert
- DNS löst intern falsch auf
- Regel durch frühere Blockregel verdeckt

Merksatz:

DMZ zu LAN nur gezielt erlauben und sauber prüfen.

Fehlerbild: DMZ-Server kann Updates nicht laden

Mögliche Ursachen:

- kein ausgehender Internetzugang erlaubt
- DNS nicht erlaubt
- Proxy erforderlich
- Zertifikatsprüfung schlägt fehl
- NTP falsch und Zertifikat wirkt ungültig
- Paketquelle blockiert
- Firewall-Regel zu eng

Merksatz:

Auch ausgehender DMZ-Verkehr braucht passende Regeln.

Fehlerbild: Zertifikat passt intern, extern aber nicht

Mögliche Ursachen:

```
- extern anderer Hostname
- Reverse Proxy liefert falsches Zertifikat
- DNS zeigt auf falsche IP
- Split DNS falsch
- Zertifikat enthält externen Namen nicht
- SNI-Konfiguration falsch
```

Merksatz:

```
Zertifikat muss zum tatsächlich aufgerufenen Namen passen.
```

SNI kurz erklärt

SNI steht für:

```
Server Name Indication
```

SNI ermöglicht, dass ein Server mehrere TLS-Zertifikate für verschiedene Hostnamen auf derselben IP anbieten kann.

Beispiel:

```
wiki.firma.de
cloud.firma.de
git.firma.de
```

alle über:

```
dieselbe öffentliche IP und TCP 443
```

Der Client teilt beim TLS-Aufbau den gewünschten Hostnamen mit.

Merksatz:

```
SNI hilft bei mehreren HTTPS-Diensten auf einer IP.
```

DMZ und Prüfungsdenken

In Prüfungsaufgaben wird oft erwartet, dass man erkennt:

Öffentliche Dienste gehören in die DMZ.

Interne Systeme gehören nicht direkt ins Internet.

DMZ-Systeme dürfen nur notwendige Verbindungen ins LAN aufbauen.

Firewall-Regeln müssen Quelle,
Ziel,
Dienst
und Richtung enthalten.

NAT und Firewall-Regeln müssen zusammenpassen.

Merksatz:

DMZ-Aufgaben immer mit Zonen und Datenflüssen lösen.

Was eine DMZ nicht macht

Eine DMZ macht nicht automatisch:

- Webserver sicher
- Software aktuell
- Passwörter stark
- TLS korrekt
- Anwendung fehlerfrei
- Datenbank geschützt
- Angriffe unmöglich
- Logs ausgewertet
- Backups vorhanden

Eine DMZ reduziert Risiken, ersetzt aber keine weiteren Sicherheitsmaßnahmen.

Merksatz:

DMZ ist Netztrennung,
kein vollständiges Sicherheitskonzept.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Wofür steht DMZ?
- Was ist der Zweck einer DMZ?
- Welche Systeme gehören typischerweise in eine DMZ?
- Warum stehen öffentliche Server besser in der DMZ als im LAN?
- Welche Regeln braucht ein Webserver in der DMZ?
- Warum sollte die DMZ nicht frei ins LAN dürfen?
- Was ist ein Reverse Proxy in der DMZ?
- Was ist ein Bastion Host?
- Was ist der Unterschied zwischen LAN, WAN und DMZ?
- Warum sind Sicherheitszonen sinnvoll?
- Was bedeutet Netzwerksegmentierung?
- Was ist laterale Bewegung?
- Welche Rolle spielen Firewall-Regeln zwischen Zonen?
- Warum muss auch ausgehender Verkehr aus der DMZ kontrolliert werden?
- Warum ist Monitoring in der DMZ wichtig?

Typische Prüfungsfallen

DMZ steht für Demilitarized Zone.

DMZ ist ein separates Netz.

DMZ ist nicht das interne LAN.

Öffentliche Dienste gehören besser in die DMZ.

DMZ schützt das LAN durch Trennung.

DMZ darf nicht ungefiltert ins LAN.

Internet darf nur notwendige DMZ-Dienste erreichen.

Adminzugriff auf DMZ nicht aus dem gesamten Internet erlauben.

Reverse Proxy kann in der DMZ stehen.

Mailgateway kann in der DMZ stehen.

VPN-Gateway kann in der DMZ stehen.

Datenbankserver normalerweise nicht öffentlich in die DMZ stellen.

DMZ-Systeme brauchen Updates und Härtung.

DMZ-Systeme brauchen Monitoring und Logs.

Firewall-Regeln zwischen Zonen müssen Richtung beachten.

DMZ outbound ebenfalls kontrollieren.

NAT-Regeln und Firewall-Regeln müssen zusammenpassen.

DMZ ersetzt keine sichere Anwendung.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
DMZ	separates Netz für öffentlich erreichbare Dienste
Sicherheitszone	Netzbereich mit eigenem Schutzbedarf
WAN	externes Netz oder Internet
LAN	internes Netz
Managementnetz	Netz für Administration
Gastnetz	separates Netz für Gäste
Reverse Proxy	nimmt Anfragen an und leitet an Backends weiter
Mailgateway	Mailserver-Schutz- oder Weiterleitungssystem
VPN-Gateway	Einstiegspunkt für VPN-Verbindungen
Bastion Host	abgesicherter Sprungserver

Begriff	Kurze Erklärung
Segmentierung	Aufteilung in getrennte Netzbereiche
laterale Bewegung	Bewegung eines Angreifers innerhalb des Netzes
IDS	erkennt Angriffe
IPS	erkennt und blockiert Angriffe
WAF	Web Application Firewall
TLS-Terminierung	TLS endet am Proxy oder Load Balancer
TLS Passthrough	TLS wird verschlüsselt weitergereicht
SNI	Hostname-Anzeige beim TLS-Aufbau
Härtung	sichere Konfiguration eines Systems

IHK-sichere Kurzformulierung

Eine DMZ, also Demilitarized Zone, ist ein separates Netzwerksegment für Dienste, die aus dem Internet erreichbar sein müssen. Typische Systeme in einer DMZ sind Webserver, Reverse Proxys, Mailgateways oder VPN-Gateways. Der Zweck einer DMZ besteht darin, öffentliche Dienste vom internen LAN zu trennen und dadurch das interne Netz besser zu schützen. Zwischen WAN, DMZ und LAN werden gezielte Firewall-Regeln eingerichtet. Aus dem Internet sollten nur notwendige Dienste in der DMZ erreichbar sein, und von der DMZ ins interne LAN sollten nur zwingend erforderliche Verbindungen erlaubt werden. Eine DMZ reduziert Risiken, ersetzt aber keine Updates, Härtung, sichere Anwendungen, Monitoring oder Protokollierung.

Merksätze

DMZ = Demilitarized Zone.

DMZ = separates Netz für öffentliche Dienste.

DMZ ist nicht LAN.

DMZ liegt zwischen Internet und internem Netz.

Öffentliche Dienste gehören besser in die DMZ.

DMZ schützt internes LAN durch Trennung.

Internet → DMZ nur notwendige Dienste erlauben.

Internet → LAN blockieren.

DMZ → LAN nur zwingend notwendige Verbindungen erlauben.

LAN → DMZ gezielt erlauben.

Adminzugriff nur aus Managementnetz oder über Bastion Host.

Reverse Proxy kann in der DMZ stehen.

Mailgateway kann in der DMZ stehen.

VPN-Gateway kann in der DMZ stehen.

Datenbanken nicht direkt öffentlich platzieren.

DMZ outbound kontrollieren.

DNS und NTP für DMZ gezielt erlauben.

DMZ-Systeme brauchen Updates.

DMZ-Systeme brauchen Härtung.

DMZ-Systeme brauchen Monitoring.

DMZ-Systeme brauchen Logs.

IDS erkennt Angriffe.

IPS blockiert zusätzlich.

WAF schützt Webanwendungen.

TLS-Terminierung endet am Proxy.

TLS Passthrough reicht TLS weiter.

SNI ermöglicht mehrere HTTPS-Namen auf einer IP.

Segmentierung begrenzt laterale Bewegung.

DMZ ersetzt kein vollständiges Sicherheitskonzept.