DMZ

Inhaltsverzeichnis

Eine DMZ (Demilitarized Zone) ist ein Netzwerksegment zwischen dem unsicheren Internet und dem internen LAN. Öffentliche Dienste stehen dort isoliert, während das interne Netz zusätzlich geschützt bleibt.

1 Funktionsweise

Firewalls steuern den Traffic in drei Richtungen: Internet ? DMZ, DMZ ? LAN und möglichst restriktiv Internet ? LAN. In der DMZ liegen typischerweise Web-, Mail- oder VPN-Einstiegspunkte.

- **Isolation:** kompromittierte öffentliche Dienste treffen nicht direkt das LAN
- **Regelwerke:** nur benötigte Ports und Richtungen freigeben
- **Jump-/Proxy-Pfade:** Verwaltung aus dem LAN gezielt erlauben

2 Typische Einsatzbereiche

- Öffentliche Webserver und Reverse Proxies
- Mail-Gateways und Authentifizierungs-Frontends
- Partner- oder Gästezugänge mit begrenzten Rechten

3 Wichtige Hinweise

- Eine DMZ ohne strikte Firewall-Regeln ist nur ein weiteres flaches Netz.
- Backends im LAN sollten nie unnötig direkt aus der DMZ erreichbar sein.
- Monitoring und Patch-Management in der DMZ sind besonders wichtig.

4 Fazit

Die DMZ ist ein klassisches Segmentierungsmuster: öffentliche Dienste erreichbar machen, ohne das interne Netzwerk unnötig freizugeben.