

Was sollte von außen erreichbar sein?

Jeder offene Port ist eine Tür. Die Frage ist nicht „was ist offen?“, sondern „was **muss** offen sein?“.

Prüfen: den eigenen Anschluss mit dem [Port-Check](#), eigene Server mit dem [Port-Scan](#) (Premium).

Typisch in Ordnung

Port	Dienst	Hinweis
80, 443	Webserver	80 nur zur Weiterleitung auf HTTPS
25	Mailserver (Empfang)	nur auf dem Mailserver selbst
465, 587	Mailversand für Nutzer	mit Anmeldung
993	IMAP mit TLS	statt 143 ohne TLS
51820/udp	WireGuard	VPN statt vieler einzelner Dienste

Nie direkt ins Internet

Port	Dienst	Warum
3389	Remotedesktop (RDP)	einer der häufigsten Einbruchswegen für Ransomware
445, 139	Windows-Freigaben (SMB)	Würmer wie WannaCry
5900	VNC	oft schwache oder keine Passwörter
3306, 5432, 1433, 27017, 6379	Datenbanken	Datenabfluss, oft ohne Anmeldung erreichbar
8006, 9090, ...	Verwaltungsoberflächen (Proxmox, Cockpit, Router)	Lücken in solchen Oberflächen werden gezielt gesucht

Für den Zugriff von außen: **VPN** (WireGuard, OpenVPN, IPsec) und die Dienste nur dahinter erreichbar machen.

SSH

Wenn SSH offen sein muss:

- nur **Schlüssel**, keine Passwörter (`PasswordAuthentication no`)
- kein direkter Root-Login (`PermitRootLogin no`)
- Fail2ban oder ähnliches gegen Durchprobieren
- wenn möglich nur von bekannten IPs erlauben

IPv6 nicht vergessen

Viele Router leiten IPv4 per Portfreigabe weiter, öffnen IPv6 aber über eine eigene Firewall-Regel. Ein Gerät kann also per IPv6 erreichbar sein, obwohl IPv4 dicht ist. Den Port-Check über ip6.ngosu-corp.de/ports laufen lassen.

Erstellt: 2026-10-16 12:02:55 CEST von cherry

Zuletzt aktualisiert: 2026-10-17 22:54:19 CEST von cherry