

Sicherheit

Angriffsfläche klein halten, Sicherheitsmeldungen richtig einordnen.

- [Was sollte von außen erreichbar sein?](#)
- [Sicherheitsmeldungen lesen: CVE, CVSS, EPSS, KEV](#)

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.

Sicherheitsmeldungen lesen: CVE, CVSS, EPSS, KEV

Jede Woche erscheinen hunderte neue Sicherheitslücken. Alles sofort zu patchen ist unmöglich. Diese vier Begriffe helfen beim Sortieren. Das [Sicherheitslagebild](#) zeigt sie für jede Lücke an.

CVE: die Kennung

`CVE-2024-3400` ist die weltweit eindeutige Nummer einer Lücke. Damit findest du Herstellerhinweise, Patches und Berichte. Die Nummer allein sagt nichts über die Gefahr.

CVSS: wie schlimm wäre es?

Der **CVSS-Wert** (0 bis 10) beschreibt die Schwere, falls die Lücke ausgenutzt wird:

Wert	Stufe
9,0 bis 10	kritisch
7,0 bis 8,9	hoch
4,0 bis 6,9	mittel
unter 4	niedrig

Wichtiger als die Zahl ist oft der **Vektor** dahinter, z. B. `AV:N/AC:L/PR:N/UI:N`: über das Netz (AV:N), einfach (AC:L), ohne Anmeldung (PR:N), ohne Zutun eines Nutzers (UI:N). Das ist der gefährlichste Fall. Das Lagebild übersetzt den Vektor in Klartext.

EPSS: wie wahrscheinlich ist ein Angriff?

EPSS schätzt die Wahrscheinlichkeit, dass eine Lücke in den nächsten 30 Tagen tatsächlich ausgenutzt wird. Die meisten Lücken liegen unter 1 %. Ein Wert von 10 % oder mehr ist ein deutliches Warnsignal, auch wenn der CVSS-Wert nur „mittel“ ist.

KEV: wird schon angegriffen

Der **KEV-Katalog** der US-Behörde CISA listet Lücken, die **nachweislich aktiv ausgenutzt** werden. Für Bundesbehörden gilt dort eine Frist zum Patchen, meist zwei bis drei Wochen. Für alle anderen gilt: KEV-Einträge zu eigenen Systemen haben Vorrang vor allem anderen.

Reihenfolge in der Praxis

1. **Betrifft es mich?** Produkt und Version prüfen. Die Merkliste im Lagebild mit Versionsangabe nimmt dir das ab.
2. **KEV oder hoher EPSS-Wert:** sofort patchen oder abschotten.
3. **Kritisch und aus dem Internet erreichbar:** innerhalb weniger Tage.
4. **Rest:** im normalen Update-Rhythmus.

Bei aktiv ausgenutzten Lücken nach dem Patch auch nach **Angriffsspuren** suchen. Wer schon drin war, bleibt es sonst trotz Update. Die Detailseite im Lagebild hat dafür eine Checkliste.