

Informationen zur aktuelle Lage

Die IT-Sicherheitslage ist von dynamischen Entwicklungen geprägt. Neue Angriffsmethoden, Sicherheitslücken und die wachsende Professionalisierung von Cyberkriminalität stellen Unternehmen und Privatnutzer gleichermaßen vor erhebliche Herausforderungen. Gleichzeitig entstehen durch technologische Innovationen neue Angriffspunkte, die klassische Schutzmaßnahmen häufig überfordern. Dieses Kapitel gibt einen Überblick über aktuelle Bedrohungen, bewertet deren Auswirkungen und stellt Lösungsansätze vor, mit denen sich digitale Infrastrukturen wirksam absichern lassen.

Weitere Artikel zum Thema unter: gerds-blog.de

- [BSI - Bundesamt für Sicherheit in der Informationstechnologie](#)
 - [BSI - Grundschutz](#)
- [„VPN war gestern – Zero Trust ist heute: Sicherheit neu gedacht.“](#)

BSI - Bundesamt für Sicherheit in der Informationstechnologie

Die beste und erste Quelle wenn es um IT-Sicherheit geht: <https://www.bsi.bund.de>

BSI - Bundesamt für Sicherheit in der Informationstechnologie

BSI - Grundschutz

Der **BSI IT-Grundschutz** ist ein praxisnahes Konzept zur systematischen Absicherung von Informations- und Kommunikationstechnik in Unternehmen und Behörden. Er bietet methodische Vorgehensweisen, konkrete Sicherheitsmaßnahmen und umfangreiche Bausteine, um unterschiedliche IT-Systeme und Prozesse abzusichern. Ziel ist es, ein angemessenes und zugleich wirtschaftliches Schutzniveau zu erreichen, das sowohl für kleine Organisationen als auch für komplexe Infrastrukturen geeignet ist. Der Grundschutz unterstützt zudem bei der Umsetzung von ISO 27001-Zertifizierungen auf Basis von IT-Grundschutz. Er gilt in Deutschland als zentraler Standard für Informationssicherheit und wird regelmäßig vom BSI aktualisiert.

☐ [BSI IT-Grundschutz](#)

„VPN war gestern – Zero Trust ist heute: Sicherheit neu gedacht.“

Risiken klassischer VPN-Verbindungen

- **Unkontrollierter Netzwerkzugriff:** Nach erfolgreicher Anmeldung erhält der Nutzer meist weitreichenden Zugriff auf interne Systeme, unabhängig von seiner tatsächlichen Rolle.
- **Angriffsfläche durch kompromittierte Endgeräte:** Ein unsicherer Client-Rechner kann Schadsoftware ins interne Netz einschleusen.
- **Schwachstellen in VPN-Gateways:** Angreifer nutzen bekannte Sicherheitslücken in VPN-Software und Appliances gezielt aus.
- **Credential-Diebstahl:** Gestohlene Zugangsdaten ermöglichen unbemerkt einen vollwertigen Fernzugang.
- **Fehlende Segmentierung:** Klassische VPNs arbeiten oft nach dem „Alles-oder-Nichts“-Prinzip und erschweren eine granulare Zugriffskontrolle.
- **Skalierungsprobleme:** Mit zunehmender Zahl an Remote-Nutzern entstehen Performance-Engpässe und Sicherheitsrisiken durch unsaubere Erweiterungen.

Empfehlungen des BSI

Das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** empfiehlt im Rahmen des IT-Grundschutzes:

- **Starke Authentisierung** (z. B. Multi-Faktor-Authentifizierung) für alle VPN-Zugänge.
- **Härtung und regelmäßige Aktualisierung** der eingesetzten VPN-Gateways.
- **Strikte Zugriffsbeschränkung** nach dem Prinzip „Least Privilege“ statt pauschaler Netzzugriffe.
- **Netzsegmentierung** und Trennung kritischer Systeme, um Seitwärtsbewegungen einzuschränken.
- **Alternativen zu klassischen VPNs prüfen**, etwa Zero-Trust-Architekturen (ZTA) mit feingranularer Zugriffskontrolle.

Zero Trust als zukunftsweisender Ansatz

Im Gegensatz zum klassischen VPN verfolgt **Zero Trust** das Prinzip „**Never trust, always verify**“:

- **Jeder Zugriff wird einzeln geprüft**, unabhängig vom Standort des Nutzers.
- **Identität und Kontext** (z. B. Gerät, Standort, Uhrzeit) fließen in die Entscheidung ein.
- **Granulare Freigaben:** Nutzer erhalten nur Zugriff auf die Ressourcen, die sie wirklich benötigen.
- **Kontinuierliche Überprüfung:** Auch nach erfolgreicher Anmeldung bleibt die Verbindung nicht unbegrenzt gültig, sondern wird regelmäßig neu bewertet.
- **Verbesserte Transparenz:** Sicherheitsereignisse lassen sich feiner nachverfolgen, wodurch Angriffe schneller erkannt werden.

Das BSI sieht Zero-Trust-Architekturen als wichtigen Baustein für die Zukunft moderner IT-Sicherheitsstrategien, insbesondere in verteilten Infrastrukturen und hybriden Arbeitsumgebungen.

[BSI – Zero Trust: Grundlagen und Empfehlungen](#)

? Vergleich: Zugangsmodelle für externe Partner & interne Nutzer

Technologie / Modell	Funktionsweise	Sicherheit bei externen Geräten	Transparenz / Logging	Typische Eignung	Vorteile	Nachteile

Klassisches VPN	Tunnel ins interne Netz, Gerät wird wie „intern“ behandelt	☐ Sehr hoch riskant (unkontrollierte Endgeräte können Malware einschleppen)	Basis-Logs, oft nur Verbindungsdaten	interne Mitarbeiter	Einfach, etabliert	Alles-oder-nichts Zugriff, keine Gerätekontrolle
Bastion Host / Jump Host	Externe melden sich an einem zentralen Host in DMZ, von dort Zugriff auf Zielsysteme	☐ Gut: Endgeräte haben keinen direkten Netzzugang, Risiko isoliert	☐ Sehr gut: Sitzungen können überwacht, aufgezeichnet werden	Wartungsfirmen, externe Admins	Starke Kontrolle, Isolation	Etwas mehr Infrastruktur nötig
Terminalserver / Remote Desktop in DMZ	Partner arbeiten auf Terminalserver, nur Bildschirm/Keyboard übertragen	☐ Sehr gut: Keine Daten direkt auf Partner-Gerät	☐ Logs & Session Recording möglich	Externe Agenturen, Dienstleister	Einfaches Handling, kein Datentransfer	Lizenz-/Serverkosten, evtl. Performance
ZTNA (Zero Trust Network Access)	Zugriff auf bestimmte Apps/Dienste , nicht aufs Netz	☐ Sehr gut: Granularer Zugriff pro Anwendung, MFA verpflichtend	☐ Sehr detailliert, pro App	Wartungsfirmen, Agenturen, Homeoffice	Modern, granular, Cloud-ready	Teilweise neue Infrastruktur, Schulung nötig
PAM (Privileged Access Management)	Externe nutzen zentrale Plattform, erhalten temporäre Adminrechte/Accounts	☐ Sehr gut: Keine festen Passwörter, temporär & nachvollziehbar	☐ Sehr gut: Jeder Admin-Befehl protokollierbar	Wartungsfirmen, Admin-Dienstleister	Kontrolle über privilegierte Zugriffe, Compliance	Komplexe Einführung, meist Enterprise-Lösung
Device Health Check (klassisch im VPN)	Prüfung: Antivirus, Updates, Firewall → sonst kein Zugang	⚠ Nur bedingt wirksam (Partner können Anforderungen umgehen)	Mittel, abhängig von Lösung	Eigene Mitarbeiter, BYOD	Automatisierte Policy-Kontrolle	Bei externen Partnern oft nicht durchsetzbar

Empfehlung: Moderne Remote-Zugänge mit Headscale

Als sichere und flexible Alternative zu klassischen VPN-Lösungen empfiehlt sich der Einsatz von **Headscale** – einer Open-Source-Implementierung des Tailscale-Kontrollservers.

Funktionsweise in Kürze:

- **Zero-Trust-Prinzip:** Headscale baut auf dem WireGuard-Protokoll auf und verbindet Endgeräte direkt miteinander, ohne zentralen Datenverkehr über ein VPN-Gateway.
- **Dezentrale Kommunikation:** Geräte authentifizieren sich gegenseitig und tauschen verschlüsselte Peer-to-Peer-Verbindungen aus.
- **Granulare Zugriffskontrolle:** Über Policy-Regeln lassen sich Zugriffsrechte sehr fein definieren – jedes Gerät erhält nur den Zugriff, der wirklich erforderlich ist.
- **Einfache Verwaltung:** Headscale läuft als selbst gehosteter Server und ersetzt den Tailscale-Cloud-Dienst, sodass volle Daten- und Sicherheitskontrolle bestehen bleibt.
- **Hohe Performance:** Da Verbindungen direkt zwischen den Endpunkten aufgebaut werden, entfallen Engpässe klassischer VPN-Gateways.

Mit Headscale lässt sich also eine **Zero-Trust-Netzwerkinfrastruktur** aufbauen, die die Vorteile von WireGuard (Sicherheit, Geschwindigkeit, Einfachheit) mit moderner Zugriffskontrolle und selbstbestimmtem Hosting kombiniert – und damit die Schwachstellen klassischer VPN-Architekturen effektiv vermeidet.

Kommerzielle Alternativen zu Headscale

Im Bereich **Remote Access und Zero-Trust-Netzwerke** gibt es verschiedene kommerzielle Anbieter, die ähnliche Funktionen wie Headscale bzw. Tailscale bereitstellen:

- **Tailscale** – Cloudbasierter Zero-Trust-VPN-Dienst (kommerziell, aber mit kostenloser Basisversion). Nutzt wie Headscale WireGuard, erfordert jedoch den proprietären Kontrollserver von Tailscale.
- **NordLayer (NordVPN Business)** – Kommerzielle VPN- und ZTNA-Plattform für Unternehmen mit zentralem Management, Identity-Integration und Support.
- **Perimeter 81** – Zero-Trust Network Access (ZTNA) mit Cloud-Management, Multi-Faktor-Authentifizierung und Role-Based Access Control.
- **Cisco Secure Connect / Cisco AnyConnect** – Etablierte Unternehmenslösung für VPN und Zero Trust, allerdings mit hoher Komplexität und Lizenzkosten.
- **Zscaler Private Access (ZPA)** – Cloud-native Zero-Trust-Plattform für sicheren Zugriff auf interne Anwendungen ohne klassische VPN-Tunnel.
- **Palo Alto Prisma Access** – Vollumfängliche SASE-/Zero-Trust-Lösung für größere Unternehmen mit globaler Infrastruktur.

Headscale als Alternative

- **Kosten:** Headscale ist Open Source und kostenlos, während die kommerziellen Systeme Lizenz- und Betriebskosten verursachen.
- **Kontrolle:** Mit Headscale behalten Organisationen die volle Datenhoheit, da der Server **selbst betrieben** wird – im Gegensatz zu cloudbasierten Diensten wie Tailscale, Zscaler oder Perimeter 81.
- **Flexibilität:** Anpassungen und Integrationen sind frei möglich, da Headscale quelloffen ist.
- **Sicherheit:** Baut wie die großen Anbieter auf **WireGuard** und Zero-Trust-Prinzipien auf, ohne zentrale Gateway-Schwachstellen klassischer VPNs.
- **Support:** Der Nachteil ist fehlender kommerzieller Herstellersupport – stattdessen ist die Community entscheidend. Für Unternehmen mit hohen Anforderungen an SLA kann das ein Ausschlusskriterium sein.

📌 Fazit:

Headscale ist eine attraktive **Open-Source-Alternative zu kommerziellen Zero-Trust-Lösungen**, wenn **Kostenkontrolle, Datenhoheit und Flexibilität** im Vordergrund stehen. Kommerzielle Anbieter punkten hingegen mit **Enterprise-Support, globaler Infrastruktur und Zertifizierungen**.

Vergleich: Headscale vs. kommerzielle Anbieter

Kriterium	Headscale (Open Source)	Tailscale	Cloudflare Zero Trust	Enterprise-Anbieter (Cisco, Zscaler, Perimeter 81, Palo Alto)
Kosten	Kostenlos, Open Source	Abo-Modell (Basisversion gratis)	Abo-Modell (nach Nutzern/Traffic)	Teure Lizenz- und Servicekosten
Datenhoheit	Volle Kontrolle (Self-Hosting)	Metadaten über Tailscale-Cloud	Datenverkehr über Cloudflare-Edge	Abhängig vom Anbieter, oft Cloud
Protokoll	WireGuard	WireGuard	Proprietär (Zugriff pro App via mTLS/OAuth), kombiniert mit DNS/HTTP-Security	Unterschiedlich (IPsec, TLS, proprietäre Protokolle)
Zero Trust	Granulare Policies, rollenbasiert	App-/Geräte-Zugriff, Identity-Integration	Vollständige ZTNA-/SASE-Plattform, App-Zugriff statt Netzwerkeinwahl	Umfassende ZTNA-/SASE-Funktionalität
Skalierbarkeit	Abhängig von eigener Infrastruktur	Cloudbasiert, automatisch skalierend	Sehr hoch durch weltweites CDN/Edge-Netzwerk	Sehr hoch, für Enterprise-Infrastrukturen optimiert
Support	Community-basiert	Hersteller-Support	Hersteller-Support, global verfügbar	Hersteller-Support, SLAs, 24/7
Flexibilität	Sehr hoch, volle Anpassung	Mittel, abhängig von Tailscale-Funktionen	Mittel, stark an Cloudflare-Ökosystem gebunden	Eingeschränkt durch Anbieterarchitektur
Sicherheit	Peer-to-Peer, kein Gateway-Bottleneck	Peer-to-Peer via WireGuard, zentral verwaltet	Zugriff pro Anwendung, DLP, Malware-Schutz, globales Filtering	Umfassende Security-Stacks, zertifiziert (ISO/SOC2 etc.)
Implementierung	Eigeninstallation (Linux-Server)	Einfach via Cloud-Setup	Cloud-Service, kein eigener Server nötig	Komplex, meist Projekte mit Integratoren
Zielgruppe	KMU, Tech-affine Unternehmen, Selbsthoster	Start-ups, KMU, hybride Teams	Mittelstand bis Enterprise, Cloud-first-Strategien	Großunternehmen mit Compliance- & SLA-Anforderungen

☐ Kurzfazit:

- **Headscale** = ideal für **Selbsthoster und KMU**, die **Datenhoheit, Kostenkontrolle und Flexibilität** priorisieren.
- **Tailscale** = einfacher Einstieg in Zero Trust mit WireGuard, aber Cloud-gebunden.

- **Cloudflare Zero Trust** = attraktiv für **Cloud-first-Strategien**, global skalierbar, mit starkem Fokus auf **SASE und Security-Filtering**.
- **Enterprise-Anbieter** = umfangreiche Funktionen und Zertifizierungen, aber hohe Kosten und Komplexität.

☐ Zusammenfassung:

Headscale eignet sich ideal für Organisationen, die **Kosten sparen, Datenhoheit behalten** und **flexible Anpassungen** wünschen. **Kommerzielle Anbieter** sind sinnvoll für Unternehmen, die **Zertifizierungen, weltweite Skalierbarkeit und professionellen Support** benötigen.