business.ewe.de/it-security

EWE

Jenseits des öffentlichen Internets: So machen Sie Ihr Netzwerk unverwundbar

Warum sichere Konnektivität der Schlüssel zu resilienten IT-Strukturen ist – und wie Sie diese Schritt für Schritt aufbauen.

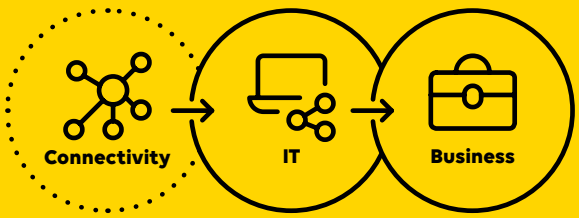
Inhalt

Einleitung

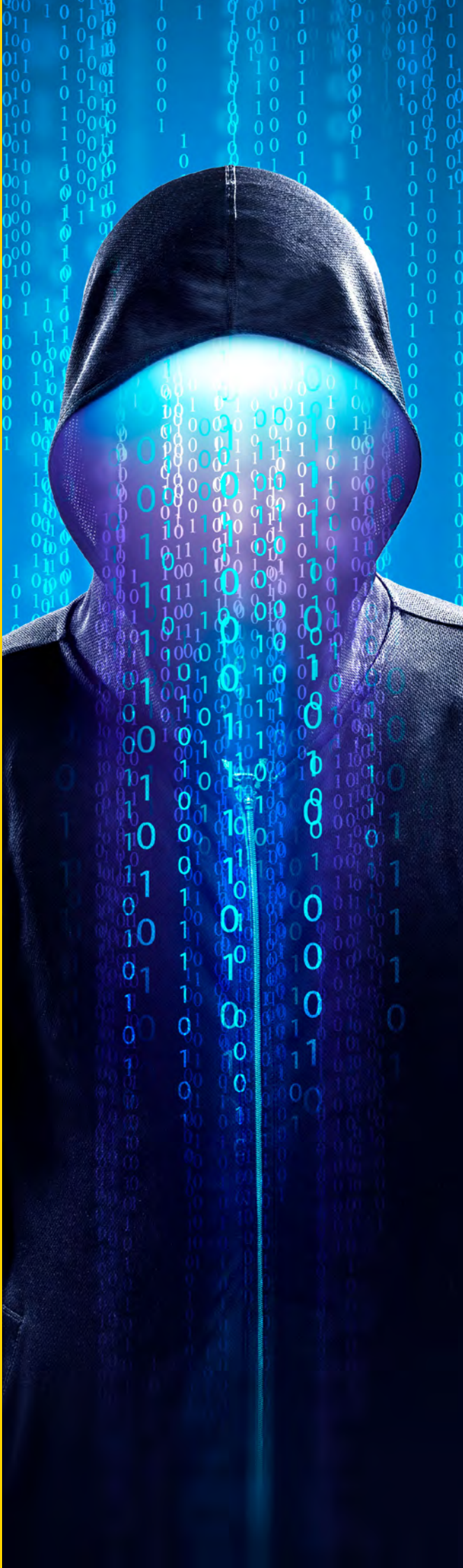
Die digitale Transformation ist längst Realität – besonders für mittelständische Unternehmen. Geschäftsmodelle basieren zunehmend auf Cloud-Anwendungen, Datenanalysen in Echtzeit, vernetzten Produktionsprozessen und hybriden Arbeitsmodellen. All diese Entwicklungen sind massiv von stabilen und sicheren Netzwerken abhängig.

Gleichzeitig steigt die Bedrohungslage: Cyberkriminelle nutzen gezielt die wachsende Komplexität moderner IT-Landschaften aus. Phishing, Ransomware und gezielte Angriffe auf Lieferketten treffen Unternehmen immer häufiger – und das mit oft existenzbedrohenden Folgen.

»Konnektivität ist nicht nur die technische Basis von IT – sie ist der zentrale Hebel für Sicherheit, Resilienz und Geschäftserfolg.«



Die größte Schwachstelle dabei sind oft nicht die Endgeräte oder die Software, sondern die Vernetzung selbst. Ohne eine ganzheitlich gedachte Konnektivitätsstrategie bleibt jede andere Sicherheitsmaßnahme lückenhaft. Es reicht nicht, Firewalls oder Antivirenprogramme isoliert einzusetzen. Unternehmen müssen ihr Netzwerk als strategischen Erfolgsfaktor begreifen – und genau hier setzt das Connectivity-Framework an.



Das Connectivity-Framework – vier Ebenen sicherer Vernetzung

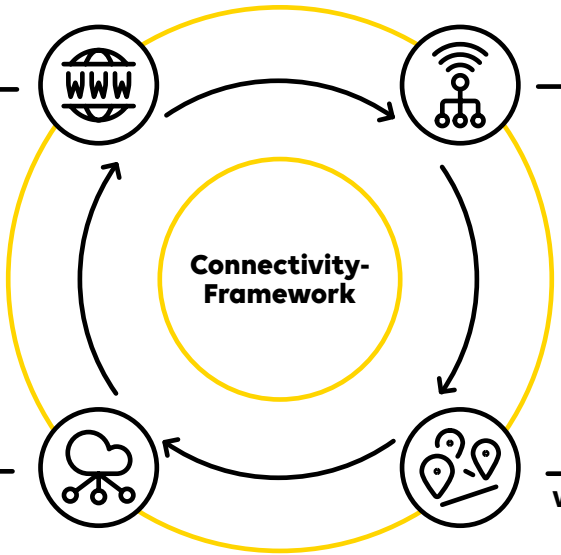
Um Netzwerke wirklich sicher und zukunftsfähig zu gestalten, brauchen Unternehmen ein klares Konzept. Das Connectivity-Framework bietet genau diesen strategischen Blick: Es zeigt, wie sich die unterschiedlichen Netzwerkebenen zusammensetzen und wie sie nahtlos ineinandergreifen müssen, um Angriffe zu verhindern und gleichzeitig Stabilität und Agilität zu gewährleisten.

Das Framework umfasst vier zentrale Ebenen:

Diese Ebenen sind untrennbar miteinander verbunden. Eine Schwachstelle in nur einer Ebene kann die gesamte Sicherheitsarchitektur kompromittieren. Deshalb müssen sie als Ganzes geplant und abgesichert werden, nicht als isolierte Einzelprojekte.

Internet-Anbindung
Die äußere Verbindung zur digitalen Welt

LAN/WLAN
Die interne Vernetzung innerhalb von Gebäuden und Geländen



Cloud- & Partner-Vernetzung
Die Schnittstellen zu externen Plattformen und Geschäftspartnern

WAN/Standortvernetzung
Die Verbindung verteilter Niederlassungen und Rechenzentren

Warum das relevant ist:

Unternehmen, die ihre Netzwerke so organisieren, gewinnen nicht nur ein höheres Sicherheitsniveau, sondern auch mehr **Transparenz und Kontrolle** über alle Datenflüsse. Sie können Störungen schneller erkennen und beheben, Compliance-Anforderungen besser erfüllen und neue digitale Geschäftsmodelle mit weniger Risiko umsetzen.

Internet-Anbindung – die äußere Basis

Die Internet-Anbindung ist das Tor zur digitalen Welt – und der erste Prüfstein für eine sichere IT-Infrastruktur. Dennoch wird dieser Aspekt in vielen Unternehmen unterschätzt. Geteilte Internetanschlüsse („Shared Services") sind zwar kostengünstig, verursachen jedoch häufig Leistungsschwankungen, bieten keine garantierte Verfügbarkeit und bergen Sicherheitsrisiken.

Ein Beispiel: Wenn sich mehrere Kunden denselben logischen Übergabepunkt teilen, steigt die Gefahr unbeabsichtigter Datenlecks oder gezielter Angriffe über Schwachstellen auf Providerebene.

» Die Internetanbindung ist keine Commodity – sie ist kritische Infrastruktur. «

Ein dedizierter Zugang (DIA – Dedicated Internet Access) hingegen bietet exklusive Bandbreite, gleichbleibende Leistung und höhere Sicherheit. In Verbindung mit redundanten Leitungswegen entsteht ein hoch verfügbares Fundament für moderne Anwendungen wie Cloud Services, Remote Work oder IoT-Systeme.

Merkmale sicherer Internetanbindungen:

- Garantierte Bandbreite, unabhängig von Tageszeit und Auslastung
- Symmetrische Performance (Up- und Download gleich schnell)
- SLAs mit hoher Verfügbarkeit und schneller Störungsbeseitigung
- Redundanz durch physisch getrennte Leitungswege (Dual-Homing)

Praxisbeispiel

Ein Fertigungsbetrieb leidet unter Verbindungsabbrüchen beim Zugriff auf seine Cloud-Steuerung. Die IT wechselt zu einem DIA-Modell mit doppelter Anbindung – seither läuft der Betrieb ohne Unterbrechungen, auch bei Wartungen oder Störungen einzelner Leitungen.

Eine sichere Internetanbindung ist keine Nebensache, sondern Grundlage für alles Weitere – von der Firewall bis zum Datenverkehr in die Cloud. Sie ist das erste Glied in der Sicherheitskette – und eines der wichtigsten.

LAN/WLAN – Sicherheit und Stabilität im Herzen des Unternehmens

Während die Internet-Anbindung das äußere Tor zum Unternehmensnetzwerk bildet, ist das **LAN (Local Area Network)** das Herzstück der internen Kommunikation – und das **WLAN** die Schnittstelle, die Mitarbeitende, Gäste und IoT-Geräte drahtlos einbindet. Beide Komponenten sind unverzichtbar für den täglichen Betrieb, gleichzeitig aber häufig unterschätzte Angriffsziele.

Alte Switches ohne Monitoring-Funktion, fehlende Segmentierung oder Geräte, die ohne Autorisierung im Netz auftauchen, öffnen Angreifern Tür und Tor. Auch ungesicherte oder schlecht konfigurierte WLANs sind häufige Einfallstore – besonders bei hybriden Arbeitsmodellen mit mobilen Geräten und Gästen im Unternehmen.

Moderne LAN- und WLAN-Architekturen als Lösung:

Um die internen Netze zukunftsfähig zu machen, müssen Unternehmen in aktuelle Technologien und ein stringentes Sicherheitskonzept investieren:

1. **Aktuelle Hardware einsetzen**
   Moderne Switches & Router bieten nicht nur höhere Leistung, sondern auch integrierte Sicherheitsfunktionen wie Access Control Lists (ACLs), Verschlüsselung & automatisiertes Patch-Management.

2. **Netzwerksegmentierung umsetzen**
   Kritische Systeme (z. B. Produktionsanlagen oder Finanzsysteme) müssen in separaten Netzbereichen isoliert werden. Dasselbe gilt für IoT-Geräte und Gastzugänge.

3. **Rollenbasierte Zugriffskontrolle**
   Nutzer und Geräte erhalten nur die Zugriffsrechte, die sie wirklich benötigen.

4. **WLAN mit aktuellen Standards sichern**
   WPA3, Multi-Faktor-Authentifizierung (MFA) und die Trennung von Gast- und Unternehmensnetzwerken sind heute Pflicht.

5. **Transparenz schaffen**
   Zentrale Managementplattformen liefern in Echtzeit Einblicke in alle verbundenen Geräte und helfen, Auffälligkeiten frühzeitig zu erkennen. Ein modernes, sicheres LAN/WLAN ist mehr als nur „Infrastruktur im Hintergrund". Es ist der Knotenpunkt, an dem sich alle Datenströme treffen und verteilt werden. Wenn hier verlässliche Strukturen, Transparenz und klare Sicherheitsmechanismen fehlen, können sich selbst kleine Sicherheitsvorfälle zu großen Krisen entwickeln.

WAN/Standortvernetzung – Sicherheit über Unternehmensgrenzen hinaus

Sobald ein Unternehmen mehrere Standorte betreibt, wird die Vernetzung zwischen diesen zu einer zentralen Frage für Sicherheit und Performance. Klassische Punkt-zu-Punkt-Verbindungen oder reine VPN-Lösungen geraten schnell an ihre Grenzen – besonders, wenn Cloud-Anwendungen, Remote-Arbeit und verteilte Teams zum Alltag gehören.

Moderne WAN-Architekturen setzen auf SD-WAN oder Multiprotocol Label Switching (MPLS), um sichere, performante und zentral steuerbare Verbindungen zu schaffen. Ziel ist es, Datenflüsse zwischen Standorten, Rechenzentren und Cloud-Diensten so zu lenken, dass Performance und Sicherheit Hand in Hand gehen.

Wichtige Sicherheits- und Leistungsaspekte im WAN:

Integrierte Security Policies: Firewalls und Verschlüsselung direkt ins WAN integriert, statt nur am Perimeter.

Zero-Trust-Ansatz: Jeder Standort und jede Verbindung wird kontinuierlich authentifiziert und autorisiert.

Priorisierung kritischer Anwendungen: QoS (Quality of Service) sorgt dafür, dass z. B. VoIP- oder ERP-Daten Vorrang vor weniger zeitkritischem Traffic haben.

Hohe Verfügbarkeit: Redundante Verbindungswege und automatisches Failover sichern den Betrieb.

Praxisbeispiel

Ein Logistikunternehmen mit Hubs in mehreren europäischen Ländern ersetzt seine alte VPN-Struktur durch ein SD-WAN. Ergebnis: 30 % schnellere ERP-Zugriffe, deutlich reduzierte Latenzzeiten für Tracking-Systeme und zentrale Kontrolle aller Security Policies.

Das WAN ist das Rückgrat für die Zusammenarbeit über Standorte hinweg. Moderne Technologien wie SD-WAN verbinden Sicherheit, Verfügbarkeit und Performance – flexibel skalierbar und zukunftssicher.

Cloud- & Partner-Vernetzung – externe Schnittstellen absichern

Um Netzwerke wirklich sicher und zukunftsfähig zu gestalten, brauchen Unternehmen ein klares Konzept. Das Connectivity-Framework bietet genau diesen strategischen Blick: Es zeigt, wie sich die unterschiedlichen Netzwerkebenen zusammensetzen und wie sie nahtlos ineinandergreifen müssen, um Angriffe zu verhindern und gleichzeitig Stabilität und Agilität zu gewährleisten.

Ein typisches Risiko ist unkontrollierter Datenverkehr über das öffentliche Internet. Ohne transparente Wege und Überwachung weiß die IT oft nicht, welche Daten wohin fließen. Schwachstellen in APIs werden gezielt ausgenutzt, und veraltete Sicherheitsstandards bei Partnern können selbst ein gut geschütztes eigenes Netz gefährden. Fehlende oder zu großzügige Zugriffsrechte erhöhen das Risiko zusätzlich.

Sichere Anbindung beginnt mit dem Grundsatz, Cloud- und Partnerverbindungen wie eigene Standorte zu behandeln: segmentiert, überwacht und mit klar definierten Zugriffsrichtlinien. Direkte Peerings zu großen Cloud-Plattformen – etwa AWS, Azure oder Microsoft 365 – über private Leitungen umgehen das öffentliche Internet und verbessern so Sicherheit und Performance. Ergänzend sorgt eine DMZ-Architektur dafür, dass interne Netze strikt von externen getrennt bleiben, während API-Sicherheitsmechanismen und Cloud Access Security Broker (CASB) Missbrauch verhindern.

Sichere Cloud- und Partnerverbindungen sind keine Nebensache, sondern ein entscheidender Bestandteil moderner Unternehmensnetze. Sie schaffen eine kontrollierte, vertrauenswürdige Austauschumgebung – jenseits der Unsicherheiten des öffentlichen Internets.

» Sichere Cloud- und Partnerverbindungen sind keine Nebensache, sondern ein entscheidender Bestandteil moderner Unternehmensnetze. «

Sicherheitsprinzipien, die sich durch alle Ebenen ziehen

Jede der vier Ebenen des Connectivity-Frameworks sorgt für Stabilität und Kontrolle in einem Teilbereich der Vernetzung. Doch echte Sicherheit entsteht erst, wenn auf allen Ebenen dieselben Leitplanken gelten – verbindlich, konsequent und durchgängig.

Diese verbindlichen Leitplanken sind unsere Sicherheitsprinzipien. Sie durchziehen jede Verbindung – ob über das Internet, innerhalb des LANs, zwischen Standorten oder zu Cloud-Partnern. Erst wenn diese Prinzipien konsequent umgesetzt werden, wird aus der reinen Konnektivität ein sicherer, widerstandsfähiger Unternehmensverbund.

Zero Trust – Vertrauen ist kein Standardwert
Zero Trust geht davon aus, dass weder interne noch externe Akteure automatisch vertrauenswürdig sind. Jeder Zugriff wird einzeln authentifiziert und autorisiert, Identität und Gerätezustand kontinuierlich geprüft und Rechte streng nach dem „Need-to-know"-Prinzip vergeben.

Ende-zu-Ende-Verschlüsselung: Schutz vom Ursprung bis zum Ziel
Ob zwischen Standorten, bei Cloud-Zugriffen oder im Partnerdatenaustausch – Verschlüsselung muss lückenlos wirken. Moderne Protokolle wie TLS 1.3 oder IPsec sichern Daten und verhindern, dass Metadaten Rückschlüsse auf interne Strukturen zulassen.

Automatisiertes Monitoring und ein Security Operation Center (SOC)
Cyberangriffe werden immer komplexer und laufen oft über Wochen oder Monate hinweg unbemerkt. Deshalb reicht es nicht aus, nur auf Präventionsmaßnahmen zu setzen. Unternehmen brauchen eine kontinuierliche Überwachung ihres Netzwerks, idealerweise durch ein Security Operation Center (SOC). Das SOC analysiert den Datenverkehr in Echtzeit und erkennt ungewöhnliche Aktivitäten. Automatisierte Reaktionsmechanismen stoppen Angriffe sofort, bevor sie sich ausbreiten können. Zentrale Dashboards liefern Transparenz über alle vier Ebenen des Connectivity- Frameworks hinweg.

Gerade im Mittelstand sind IT-Teams oft zu klein, um die Sicherheit rund um die Uhr zu überwachen. Ein Managed SOC kann diese Lücke schließen und Bedrohungen abwehren, bevor sie Schaden anrichten. Einheitliche Sicherheitsprinzipien schaffen Konsistenz. Sie stellen sicher, dass jede Verbindung, jede:r Nutzer:in und jedes Gerät denselben hohen Standards unterliegt – egal, wo es sich befindet.

» Sicherheit ist kein statischer Zustand, sondern ein kontinuierlicher Prozess – in jeder Verbindung, auf jeder Ebene. «

Der Ausblick: Das eigene „Unternehmens-Internet“

Werden die vier Konnektivitäts-Ebenen mit diesen Prinzipien verknüpft, entsteht kein loses Netz aus Einzelmaßnahmen, sondern eine kontrollierte und geschützte Gesamtarchitektur.

Dieses Zusammenspiel ist der Schlüssel zum „Unternehmens-Internet“ – einer eigenen, vollständig kontrollierten Kommunikations- und Datenplattform, die die Vorteile des Internets bietet – ohne dessen Unsicherheiten. Ein solches Netzwerk verbindet **Standorte, Mitarbeitende, Anwendungen und Partnerunternehmen** so, dass Datenflüsse jederzeit nachvollziehbar, geschützt und optimiert sind.

Sicherheit, Performance, Transparenz und Agilität gehen Hand in Hand: Anwendungen laufen stabil mit geringen Latenzen, neue Partner oder Cloud-Plattformen lassen sich schnell integrieren, und die IT hat jederzeit den Überblick.

Ein inspirierendes Beispiel

Ein mittelständisches Unternehmen mit mehreren Niederlassungen, Produktionsstätten und hybriden Cloud-Workloads hat die Prinzipien des Connectivity-Frameworks Schritt für Schritt umgesetzt.

- ✓ Zuerst wurden dedizierte Internetzugänge mit Redundanz etabliert.
- ✓ Dann folgte die Modernisierung der LAN- und WLAN-Strukturen mit Segmentierung und zentralem Management.
- ✓ Über SD-WAN konnten alle Standorte flexibel angebunden und einheitliche Policies durchgesetzt werden.
- ✓ Abschließend wurden Cloud- Plattformen und Partnernetzwerke über private Peerings und DMZ-Zonen integriert.

Das Ergebnis:

Heute betreibt das Unternehmen ein eigenes „Unternehmens-Internet“, das vollkommen unter seiner Kontrolle steht.

Die IT kann jeden Zugriff nachvollziehen, Sicherheitsvorfälle werden in Echtzeit erkannt und abgewehrt, und die Geschäftsprozesse laufen stabil – selbst in Krisensituationen.

Warum jetzt der richtige Zeitpunkt ist:

Die Bedrohungslage wird sich in den nächsten Jahren weiter verschärfen. Gleichzeitig steigen die Anforderungen an Netzwerke durch Cloud-First-Strategien, Remote-Arbeit und IoT rasant an. Unternehmen, die ihre Konnektivität jetzt strategisch aufstellen, verschaffen sich nicht nur einen Sicherheitsvorsprung, sondern auch einen handfesten Wettbewerbsvorteil: Sie können schneller wachsen, innovativer arbeiten und Risiken besser kalkulieren.

Handlungsempfehlungen für IT-Entscheider:innen

Der Aufbau eines Unternehmens-Internets nach dem Connectivity-Framework klingt zunächst wie ein großes Transformationsprojekt. Und tatsächlich: Eine sichere, performante und zukunftsfähige Netzwerkarchitektur lässt sich nicht von heute auf morgen einführen. Die gute Nachricht ist: Unternehmen können sofort anfangen – mit klar priorisierten Schritten, die schnell Wirkung zeigen

1. Eine strategische Netzwerkanalyse durchführen
Bevor Sie einzelne Maßnahmen ergreifen, verschaffen Sie sich einen vollständigen Überblick. Identifizieren Sie Schwachstellen und Engpässe, um eine klare Roadmap erstellen zu können. Welche Verbindungen existieren aktuell (Internet, Standorte, Cloud, Partner)? Wo bestehen Redundanzen oder Engpässe? Welche Altlasten (veraltete Router, Switches, Access Points) gefährden die Stabilität und Sicherheit?

2. Sicherheit als integralen Bestandteil einplanen
Sicherheitsmaßnahmen dürfen nicht nachträglich „aufgesetzt" werden. Denken Sie Zero Trust, Verschlüsselung und Monitoring von Anfang an mit – auf jeder Ebene. So vermeiden Sie teure Nachbesserungen und schaffen eine konsistente Architektur.

3. Schnell umsetzbare Quick Wins identifizieren
Einige Maßnahmen lassen sich kurzfristig realisieren und haben sofort einen positiven Effekt, wie beispielsweise die Umstellung auf dedizierte Internetanbindungen mit Redundanz, die WLAN-Modernisierung (WPA3, Segmentierung von Gast- und Firmennetzen) oder ein zentrales Monitoring der wichtigsten Datenflüsse.

4. Langfristige Roadmap definieren
Das Connectivity-Framework sollte nicht als „Projekt", sondern als kontinuierlicher Prozess verstanden werden. Planen Sie die nächsten 12 bis 24 Monate mit klaren Meilensteinen:

- ✓ Modernisierung der LAN/WLAN-Infrastruktur.
- ✓ Einführung einer SD-WAN-Architektur zur Standortvernetzung.
- ✓ Absicherung aller Cloud- und Partnerverbindungen durch Peerings, DMZ und CASB.

5. Externe Expertise einbinden
Gerade mittelständische IT-Abteilungen sind häufig zu klein, um ein solches Transformationsprojekt allein zu stemmen. Nutzen Sie die Unterstützung von Dienstleistern, die nicht nur Produkte liefern, sondern auch die Konzeption und Umsetzung begleiten können.

Tipp: Kommunizieren Sie diese Quick Wins sichtbar im Unternehmen – sie stärken das Vertrauen in die IT.

Die Checkliste – sofort umsetzbare Maßnahmen:

- [ ] Bestandsaufnahme aller Netzwerke und Sicherheitsmechanismen erstellen.
- [ ] Quick Wins priorisieren: z. B. dedizierte Internetanbindung und WLAN-Segmentierung.
- [ ] Zero Trust und Verschlüsselung auf jeder Ebene als Standard etablieren.
- [ ] Monitoring und automatisierte Bedrohungserkennung einführen.
- [ ] Eine Roadmap mit klaren Meilensteinen und Budgetrahmen entwickeln.

Über EWE

EWE ist ein führender Anbieter von Telekommunikations- und IT-Dienstleistungen in Deutschland und seit vielen Jahren ein verlässlicher Partner für mittelständische Unternehmen. Mit einem der größten Glasfasernetze in Norddeutschland, modernen Rechenzentren und einem starken Portfolio an Managed Security Services helfen wir Unternehmen, ihre Netzwerke sicher und zukunftsfähig zu gestalten.

Wir verstehen die besonderen Herausforderungen mittelständischer IT-Abteilungen: knappe Budgets, begrenzte Ressourcen und gleichzeitig hohe Erwartungen an Sicherheit und Verfügbarkeit. Deshalb bieten wir nicht nur Produkte, sondern ganzheitliche Lösungen, die sich an den individuellen Anforderungen unserer Kunden orientieren.

Unsere Stärken auf einen Blick:

Eigene Infrastruktur:
Wir betreiben ein leistungsfähiges Glasfasernetz mit Backbone-Anbindung und bieten direkte Peerings zu den wichtigsten Cloud-Providern.

Moderne Rechenzentren:
ISO-zertifizierte Rechenzentren mit höchsten Sicherheitsstandards.

Managed Security Services:
Von Zero Trust bis SOC – wir entlasten IT-Teams und sorgen dafür, dass Sicherheitsvorfälle in Echtzeit erkannt und abgewehrt werden.

Marktkenntnis Mittelstand:
Wir kennen die typischen Pain Points und entwickeln Lösungen, die pragmatisch und bezahlbar sind.

Der Aufbau eines Unternehmens-Internets ist ein strategischer Schritt, der langfristig Sicherheit und Stabilität schafft. Wir begleiten Sie gern – von der Bestandsaufnahme bis zur Umsetzung.

Sie möchten mehr darüber erfahren, wie Sie Ihr Unternehmensnetzwerk sicher, performant und zukunftsfähig gestalten können? Unsere Expert:innen beraten Sie gern individuell und unverbindlich.

Ihr persönlicher Ansprechpartner:
David Brieskorn
IT-Security-Experte
david.brieskorn@ewe.de
0162 1385546