ITK BERATUNG ▪ PLANUNG

Kommunikations-infrastruktur als kritischer Erfolgsfaktor

Die 10 häufigsten Schwachstellen und wie Sie diese strukturiert adressieren

STRATEGISCHE MANAGEMENTBERATUNG

Kommunikationsinfrastruktur ist eine zentrale Führungsaufgabe

Sicherheit ist Teil der Unternehmenssteuerung.

Betrieb & Stabilität

Absicherung von Stabilität und Betrieb.

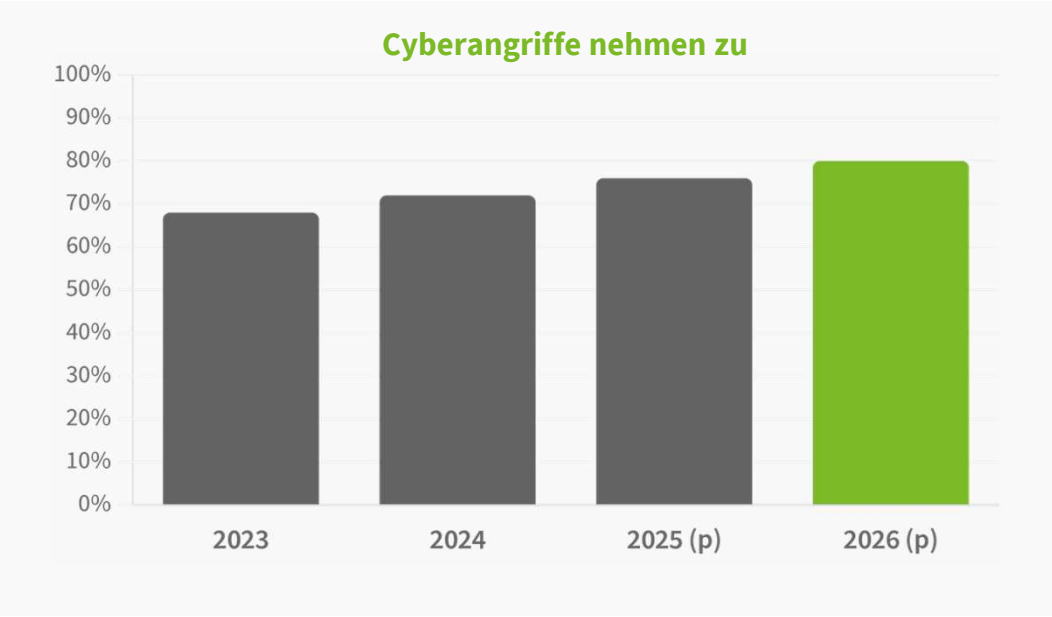
Compliance

Erfüllung regulatorischer Anforderungen (NIS-2 / DORA / KRITIS etc.).

Marktposition

Schutz von Marktposition und Reputation.

Entwicklung der Bedrohungslage in Deutschland



Kommunikationssysteme zunehmend im Fokus.

Remote-Zugriffe als Eintrittspunkt.

Steuerbarkeit wird entscheidend.

Liste / Übersicht Cyberangriffe auf Unternehmen & Kommunen in D

Datum	Unternehmen	Art des Vorfalls
10. März 2026	Paass Logistik	Ransomware
9. März 2026	Centro-Einkaufszentrum	Datendiebstahl
9. März 2026	Westfield-Einkaufszentrum	Datendiebstahl
6. März 2026	ASB Saarland	unberechtigter Zugriff
6. März 2026	Suchthilfe direkt	unberechtigter Zugriff
6. März 2026	WAG Funktion Design	Ransomware
5. März 2026	Nopa Industriearmaturen	n/a
4. März 2026	BKA Group	Ransomware
3. März 2026	Elo	Ransomware
2. März 2026	Cabka Group	Ransomware
1. März 2026	LKE	Ransomware
24. Februar 2026	Westwing	n/a
24. Februar 2026	Wachendorff	n/a
24. Februar 2026	Westiform	Ransomware
19. Februar 2026	Ausgewählt Vertrieb	Ransomware
19. Februar 2026	Hegelmann	unberechtigter Zugriff
18. Februar 2026	Dinnebier Gruppe	Ransomware
18. Februar 2026	Thallos	n/a
18. Februar 2026	KFZ Sauter	Ransomware
17. Februar 2026	Deutsche Bahn	DDoS
16. Februar 2026	Franz Sales Haus	Datendiebstahl
16. Februar 2026	Moldtech	Ransomware
15. Februar 2026	Business Information Technology Solutions	n/a
14. Februar 2026	Spir Star	Ransomware
12. Februar 2026	Lohmann Tapes	n/a
10. Februar 2026	Wagner Metall Concept	Ransomware
9. Februar 2026	Renafan	Datendiebstahl
1. Februar 2026	Sigma Processing Group	Ransomware
31. Januar 2026	Röben Tonbaustoffe	Ransomware
29. Januar 2026	Clatronic	Ransomware
28. Januar 2026	Infocom	Ransomware
28. Januar 2026	Krüss	Ransomware
26. Januar 2026	Centrotherm International	Ransomware
24. Januar 2026	Hansemerkur International	Ransomware
24. Januar 2026	Harte-Bavendamm Rechtsanwälte	Ransomware
19. Januar 2026	Wohnverbund St. Gertrud	Ransomware
19. Januar 2026	Meissner Bolte	Ransomware
16. Januar 2026	Microprecision	Ransomware
15. Januar 2026	Elabs	Ransomware
15. Januar 2026	Aero-Coating	Ransomware
14. Januar 2026	Rameder	n/a
12. Januar 2026	Brockhaus Fertigungstechnik	Ransomware
8. Januar 2026	Stesad	Ransomware
7. Januar 2026	Buhlmann-Gruppe	Ransomware
5. Januar 2026	Gebrüder Bagusat	Ransomware
5. Januar 2026	KSL Ingenieure	Ransomware
5. Januar 2026	Desy	n/a
2. Januar 2026	Röben Tonbaustoffe	Ransomware

Hinweis: Nicht alle der in dieser Liste genannten Cyberangriffe sind bestätigt. Bei einigen handelt es sich um Mutmaßungen. Die Redaktion des Security-Insiders wird diese Liste laufend aktualisieren. Allerdings erhebt sie keinen Anspruch auf Vollständigkeit. (Stand 10.3.26)

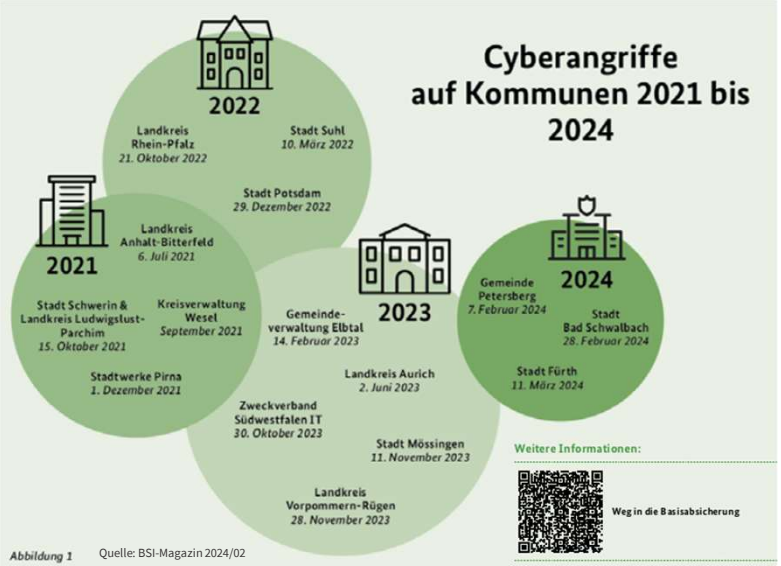


Abbildung 1 Quelle: BSI-Magazin 2024/02

Cyberangriffe verursachten 2025 massive wirtschaftliche Schäden:

- **202 Mrd. € Schäden durch Cyberangriffe auf Unternehmen in D** (Quelle: Bitkom)
- **298 Ransomware-Angriffe auf Organisationen in D** (Quelle: BSI, unter Berufung auf Leak-Seiten

Fehlende Transparenz als eigentliche Risikowurzel

Unklare Kommunikationsbeziehungen

Mangelnde Sichtbarkeit komplexer Kommunikations-beziehungen zwischen Systemen und Standorten.

Unzureichend dokumentierte Zugänge

Schatten-IT und historisch gewachsene Fernwartungszugänge ohne zentrale Kontrolle.

Fehlende Sicht auf Abhängigkeiten

Fehlendes Verständnis für kritische Abhängigkeiten innerhalb der Infrastruktur-Architektur.

Zentrale Erkenntnis: Ohne vollständige Transparenz keine Steuerbarkeit.

Überblick häufigste 10 Schwachstellen unsicherer Infrastrukturen

UCC / UCaaS / Contact Center

1. Sicherheitslücken in UC- / Collaboration-Tools
2. Ungeschützte Schnittstellen nach / von außen & nicht klar definiertes Change Management
3. Fehlende Verschlüsselung der Sprachdaten & unzureichender Schutz vor Schadcode

Cloud-, On-Prem- & Hybrid-Systeme

4. Fehlkonfigurationen in Cloud-Tenants
5. Sicherheits- & Verfügbarkeitsgefälle zwischen On-Prem & Cloud / kein BCM
6. Mangelnde Transparenz über Datenflüsse und fehlende Redundanzen

Netzwerke (LAN, WAN, SIP)

7. Veraltete Protokolle in der Infrastruktur
8. Mangelnde Absicherung von SIP-Trunks (ESBC & Firewall) und fehlendes Monitoring
9. Fehlende Segmentierung / Containerisierung kritischer Bereiche & Systeme

10. **Fehlende Awareness seitens der Nutzer**

Sicherung von Zugriffen und Identitäten

Unsicherer Remote-Zugriff

- Unzureichend gesicherter Remote-Zugriff
- Risiken externer unpersonalisierter Wartungszugänge

Fehlende MFA

- Fehlende oder unvollständige MFA
- Schwache Passwort-Policies

Unklare Berechtigungen

- Unklare / nicht definierte Berechtigungsstrukturen
- Fehlendes Least-Privilege-Prinzip

Zugriffskontrolle bestimmt das Gesamtrisiko maßgeblich.

Infrastruktur-Design und Netzwerkarchitektur

Fehlende Segmentierung

- Vermeidung flacher Netzstrukturen
- Isolierung kritischer Kommunikationswege

Unsichere Cloud-Konfigurationen

- Härtung von Cloud-Konfigurationen / Absicherung BCM
- Absicherung hybrider Schnittstellen

Kein Zero Trust

- "Never trust, always verify" Prinzip
- Identitätsbasierte Zugriffskontrolle

Die Architektur bestimmt die schnelle Ausbreitung von Sicherheitsvorfällen und Effektivität von Schutzmaßnahmen.

Sicherheit in Betrieb und Prozessen gewährleisten

Patch-Management unzureichend

Systematische Schließung von Sicherheitslücken durch zeitnahe Aktualisierung aller Infrastrukturkomponenten.

Monitoring & Logging fehlt

Lückenlose Überwachung & Protokollierung zur frühzeitigen Erkennung von Anomalien, Angriffsmustern & kritischer Incidents.

BCM & Notfallpläne unklar

Etablierung belastbarer Prozesse zur Aufrechterhaltung des Betriebs und schnellen Wiederherstellung im Not- / Krisenfall.

Operativer Betrieb entscheidet über die Reaktionsfähigkeit Ihrer Organisation.

Governance und Compliance zur Risikoreduktion

Fehlendes Risikomanagement

- Systematische Identifikation von Risiken
- Bewertung und Priorisierung von Maßnahmen

Unklare Verantwortlichkeiten

- Klare Definition von Rollen und Aufgaben
- Etablierung von Eskalationspfaden

Schwache Compliance-Strukturen

- Durchgängige Einhaltung von Richtlinien
- Nachweisbarkeit für Audits und Behörden fehlt

Governance reduziert Unsicherheit systematisch und schafft verlässlichen Handlungsrahmen.

Betriebswirtschaftliche Auswirkungen von Sicherheitsvorfällen

Betriebsunterbrechungen

Stillstand kritischer Kommunikationswege führt zu unmittelbaren Produktivitätsverlusten und Prozessstörungen.

Finanzielle Schäden

Hohe Kosten durch Incident Response, Systemwiederherstellung sowie potenzielle Bußgelder und Pönalen.

Haftungsrisiken

Rechtliche Konsequenzen bei Verletzung der Sorgfaltspflicht (NIS-2, DORA, DSGVO) für die Geschäftsführung.

Vertrauens- / Reputationsverlust

Nachhaltige Schädigung des Kundenvertrauens und der Marktposition durch öffentlich wirksame Vorfälle.

Ziel ist die systematische Risikoreduktion, nicht die reine Technikoptimierung.

Strategischer Ansatz

- Optimierung statt Austausch
- Bestehende Systeme durch gezielte Anpassung nutzen
- Einsparpotenziale realisieren
- Investitionen so weit als möglich vermeiden

Wirtschaftlichkeit im Fokus

Sicherheit und Wirtschaftlichkeit lassen sich durch intelligente Strategien verbinden.

ROI MAXIMIEREN

Beratungsansatz der ITD

Produktneutral & herstellerunabhängig

Objektive Beratung ohne Verkaufsinteressen für Hardware / Software / Services.

Zertifizierte Experten & individuelle Strategien

Langjährige Erfahrung bzgl. Individueller Absicherung regulierter / beaufsichtigter Organisationen.

ITIL®-Integration

Nachhaltige Verankerung der Sicherheit in Ihren Service-Prozessen.

Ihr Ziel: Fundierte Entscheidungen

Wir schaffen die Transparenz, die Sie für eine fundierte Steuerung Ihrer Kommunikationsinfrastruktur benötigen.

ZUKUNFTSSICHER & STEUERBAR

Kostenfreie Erstberatung: www.itd.de/kontakt/

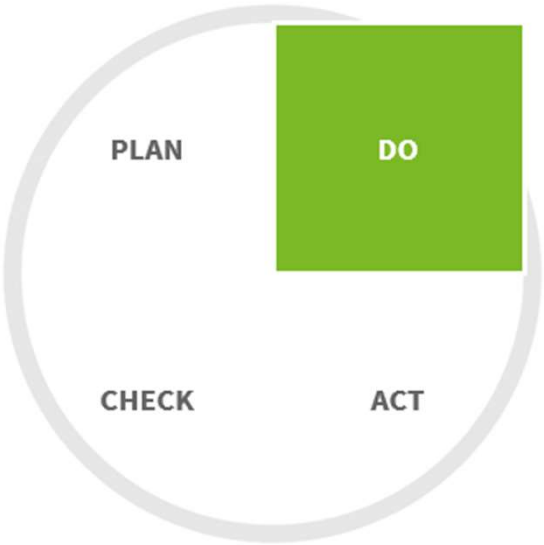
Methodik: Analyse → Bewertung → Maßnahmen im PDCA-Zyklus

01 Analyse der Kommunikationsinfrastruktur & der von ihr betroffenen Geschäftsprozesse

02 Schutzbedarfsanalyse & strukturierte Bewertung des Schutzbedarfs

03 Modellierung / Strukturanalyse, Definition Sicherheitsmaßnahmen & Soll-Ist-Vergleich)

04 Umsetzung der erforderlichern Sicherheitsmaßnahmen und ggf. Risikoanalyse



PDCA-Zyklus für Compliance

Nachhaltige Sicherheitsentwicklung & Auditfähigkeit

Ergebnisbild: Sicherheit wird plan- und steuerbar

Transparente Infrastruktur

Reduzierte Risiken

Klare Verantwortlichkeiten

Nachweisbare Compliance

Sichere & resiliente Kommunikationsinfrastruktur als belastbares Fundament für Ihr Business.

Ihr nächster Schritt

- **Klare Risikoeinschätzung**
- **Mehr Transparenz**
- **Fundierte Enscheidungsbasis**
- **Minimierung der Haftungsrisiken unter Berücksichtigung der Angemessenheit / Wirtschaftlichkeit**

Bereit für eine fundierte Entscheidung?

Sichern Sie sich jetzt Ihre erste strategische Einschätzung – fundiert, unabhängig und zielführend.

JETZT KOSTENFREIE ERSTBERATUNG SICHERN
www.itd.de/kontakt/