CYBER SECURITY

LEITFADEN 2027

Sicher aufgestellt ohne Konzern-Budget.

43 %
aller Angriffe treffen KMU

28 S.
Leitfaden mit Checklisten

NIS2
Compliance-Anforderungen

01 Bedrohungslage 2026 02 NIS2-Compliance 03 Zero Trust 04 Schutzmaßnahmen 05 Quick Wins

28 Seiten · PDF · 2026

KOSTENLOS

INHALT

01

BEDROHUNGSLAGE 2026

Cyberangriffe auf den Mittelstand haben sich seit 2023 verdreifacht. Die Angreifer werden professioneller, die Methoden raffinierter. Ein Überblick über die aktuelle Lage.

Ransomware

Verschlüsselungsangriffe bleiben die größte Bedrohung. Durchschnittliche Lösegeldforderung 2026: 1,2 Mio. Euro. Ausfallzeit im Schnitt: 23 Tage. Besonders betroffen: Fertigung, Gesundheitswesen, Logistik.

Phishing & Social Engineering

91 % aller erfolgreichen Angriffe beginnen mit einer Phishing-Mail. KI-generierte Nachrichten sind kaum noch von echten zu unterscheiden. Spear-Phishing auf C-Level nimmt stark zu.

Supply-Chain-Angriffe

Angreifer kompromittieren Zulieferer und Software-Dienstleister, um über deren Update-Mechanismen in Zielnetzwerke einzudringen. Jedes dritte KMU hat keine Übersicht über seine Software-Lieferkette.

+300 %
Anstieg der Angriffe auf KMU seit 2023

1,2 Mio.
durchschnittliche Lösegeldforderung

23 Tage
durchschnittliche Ausfallzeit

KEY TAKEAWAY

Die Frage ist nicht ob, sondern wann Ihr Unternehmen angegriffen wird. Vorbereitung ist keine Option mehr — sie ist Pflicht.

02

NIS2-COMPLIANCE

Die NIS2-Richtlinie erweitert den Kreis der betroffenen Unternehmen massiv. Ab Oktober 2024 gelten verschärfte Anforderungen — auch für viele Mittelständler, die bisher nicht reguliert waren.

Wer ist betroffen?

Unternehmen ab 50 Mitarbeitern oder 10 Mio. Euro Umsatz in 18 kritischen Sektoren: Energie, Transport, Gesundheit, digitale Infrastruktur, Fertigung, Lebensmittel, Chemie und weitere.

18
kritische Sektoren betroffen

Kernanforderungen

Risikomanagement und Sicherheitskonzepte

Meldepflicht bei Vorfällen (24h / 72h)

Supply-Chain-Sicherheit

Business Continuity Management

Verschlüsselung und Zugangskontrollen

Regelmäßige Audits und Schulungen

10 Mio.
Euro maximales Bußgeld

24 h
Erstmeldung bei Sicherheitsvorfällen

Bußgelder bei Verstößen

Wesentliche Einrichtungen: bis 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes. Wichtige Einrichtungen: bis 7 Mio. Euro oder 1,4 % des Umsatzes. Geschäftsführer haften persönlich.

KEY TAKEAWAY

NIS2 ist kein optionales Framework — es ist geltendes Recht mit empfindlichen Strafen. Starten Sie jetzt mit der Gap-Analyse.

03

ZERO TRUST GRUNDLAGEN

Zero Trust bedeutet: Vertraue niemandem, verifiziere alles. Dieses Prinzip lässt sich auch ohne Millionen-Budget umsetzen — mit den richtigen Prioritäten und schrittweiser Implementierung.

Identity & Access Management

Multi-Faktor-Authentifizierung für alle Zugänge. Least-Privilege-Prinzip konsequent umsetzen. Regelmäßige Access Reviews. Single Sign-On mit bedingtem Zugriff.

Netzwerk-Segmentierung

Mikrosegmentierung statt flacher Netzwerke. Laterale Bewegung von Angreifern wird drastisch erschwert. Software-Defined Perimeter für Remote-Zugriffe statt klassischem VPN.

Endpoint Security

Jedes Gerät wird als potenziell kompromittiert behandelt. Continuous Validation statt einmaliger Authentifizierung. Device Health Checks vor jedem Ressourcenzugriff.

85 %
weniger Breaches mit Zero Trust

MFA
blockiert 99,9 % aller Account-Angriffe

3 Stufen
zur vollständigen Implementierung

KEY TAKEAWAY

Zero Trust ist kein Produkt, sondern eine Strategie. Starten Sie mit MFA und Netzwerk-Segmentierung — das allein stoppt 90 % der Angriffe.

04

TECHNISCHE SCHUTZMASSNAHMEN

Technologie allein schützt nicht — aber ohne die richtigen Tools ist jede Strategie wirkungslos. Diese drei Säulen bilden das Fundament einer modernen Cyberabwehr im Mittelstand.

EDR — Endpoint Detection & Response

Klassischer Virenschutz reicht nicht mehr. EDR-Lösungen erkennen verdächtiges Verhalten in Echtzeit, isolieren kompromittierte Endpunkte automatisch und liefern forensische Daten für die Analyse.

< 1 Min.
Reaktionszeit mit automatisiertem EDR

SIEM — Security Information & Event Management

Zentrale Korrelation aller Sicherheitsereignisse. Moderne SIEM-Systeme nutzen KI zur Anomalie-Erkennung und reduzieren False Positives um bis zu 80 %. Cloud-basierte Lösungen senken die Einstiegshürde.

80 %
weniger False Positives mit KI-SIEM

Backup & Disaster Recovery

Die 3-2-1-Regel: 3 Kopien, 2 verschiedene Medien, 1 offline. Immutable Backups verhindern Verschlüsselung durch Ransomware. Regelmäßige Recovery-Tests sind Pflicht — nicht optional.

3-2-1
Backup-Regel als Goldstandard

KEY TAKEAWAY

EDR + SIEM + immutable Backups: Diese Kombination stoppt Angriffe, erkennt Eindringlinge und sichert die Wiederherstellung — auch bei Totalverlust.

05

SOFORTMASSNAHMEN & CHECKLISTE

Sie müssen nicht alles auf einmal umsetzen. Diese 10 Quick Wins lassen sich sofort implementieren und reduzieren Ihr Risiko um bis zu 80 % — ohne großes Budget oder externe Berater.

Quick Wins 1–5

1. MFA für alle Admin-Zugänge aktivieren
2. Automatische Updates erzwingen
3. Backup-Strategie (3-2-1) implementieren
4. Phishing-Simulation für Mitarbeiter starten
5. Netzwerk-Segmentierung: IT von OT trennen

Quick Wins 6–10

6. Passwort-Manager unternehmensweit einführen
7. E-Mail-Authentifizierung (SPF, DKIM, DMARC)
8. Notfallplan erstellen und testen
9. Privilegierte Accounts inventarisieren
10. Security-Awareness-Training quartalsweise

80 %
Risikoreduktion durch Quick Wins

0 Euro
Investition für die ersten 5 Maßnahmen

1 Tag
Umsetzungszeit pro Quick Win

KEY TAKEAWAY

Perfekte Sicherheit gibt es nicht — aber 80 % Schutz mit 20 % Aufwand schon. Starten Sie heute mit Quick Win Nr. 1.

UNSERE LEISTUNGEN

CYBERSECURITY LEISTUNGEN

Als Cybersecurity-Partner schützen wir Ihr Unternehmen ganzheitlich — von der Analyse bis zur laufenden Überwachung. Unsere Leistungen:

- **Sicherheitsaudits & Penetrationtests**
  Schwachstellenanalyse, externe und interne Pentests, Social-Engineering-Tests und detaillierte Risikobewertung.
- **NIS2-Compliance & Beratung**
  Gap-Analyse, Maßnahmenplanung, Dokumentation und Begleitung bis zur vollständigen NIS2-Konformität.
- **SOC & Managed Detection**
  24/7-Überwachung, SIEM-Betrieb, Incident Response und Threat Intelligence für Ihr Unternehmen.
- **Zero-Trust-Architektur**
  Identity & Access Management, Netzwerk-Segmentierung und Endpoint-Security-Implementierung.
- **Security Awareness Training**
  Phishing-Simulationen, Schulungen und Awareness-Kampagnen für alle Mitarbeiterebenen.
- **Backup & Disaster Recovery**
  3-2-1-Backup-Strategie, Recovery-Tests, Notfallpläne und Business-Continuity-Konzepte.

500+
behobene Schwachstellen

< 4 h
Incident Response Reaktionszeit

99,9 %
Verfügbarkeit bei Managed-Kunden

PARTNER & REFERENZEN

VERTRAUEN & ZERTIFIZIERUNGEN

Unsere Partnerschaften und Zertifizierungen garantieren Ihnen höchste Qualitätsstandards in der Cybersecurity-Beratung.

Technologiepartner

Google Partner

Microsoft Partner

SOPHOS PLATFORM PARTNER

CROWDSTRIKE

databricks PARTNER

Referenzkunden

HITCHCOCK SINCE 1966

Über 60 mittelständische Unternehmen vertrauen auf unsere Cybersecurity-Expertise. Branchenübergreifend — von Maschinenbau bis Gesundheitswesen.

Deutsche Aidshilfe

HiScout

VI2VI We care about video solutions.

IHR PARTNER FÜR CYBERSECURITY

Webect Digital Group GmbH

Wir unterstützen mittelständische Unternehmen bei der Umsetzung moderner Cybersecurity-Strategien — pragmatisch, budgetbewusst und auf Augenhöhe.

Jetzt unverbindlich beraten lassen

+49 0 7195 9299770 // vertrieb@webect.de