SUPPORA
GMBH

IT-SECURITY-LEITFADEN

2025/2026

Einleitung

Die Digitalisierung verändert nicht nur Geschäftsmodelle, sondern auch die Risikolandschaft. Während Unternehmen zunehmend auf vernetzte Systeme, Cloud-Services und digitale Prozesse setzen, nehmen auch Cyberbedrohungen rasant zu. Ransomware, Phishing, Datendiebstahl und Systemausfälle sind längst nicht mehr die Ausnahme – sie gehören zum Alltag. Besonders betroffen: kleine und mittlere Unternehmen (KMUs), die oft nicht über eigene IT-Sicherheitsabteilungen verfügen und sich im Ernstfall auf externe Unterstützung verlassen müssen.

Die alarmierenden Zahlen

Im Jahr 2024 belief sich der durch Cyberangriffe verursachte wirtschaftliche Schaden allein in Deutschland auf 178,3 Milliarden Euro. Gleichzeitig scheitern rund 70 % der Unternehmen beim ersten Versuch, IT-Audits oder gesetzliche Prüfungen wie zur NIS2-Richtlinie zu bestehen. Die Ursachen sind meist dieselben:

Die Ursachen sind meist dieselben:

- Veraltete Systeme
- Mangelnde Awareness im Team
- Fehlende Prozesse
- Unklare Zuständigkeiten

Unser Ziel

Mit diesem IT-Security-Leitfaden 2025/26 geben wir Ihnen einen kompakten, praxisorientierten Leitfaden an die Hand. Sie erfahren, wie Sie typische Schwachstellen erkennen, Sicherheitsmaßnahmen wirksam umsetzen, gesetzliche Anforderungen erfüllen und vor allem: wie Sie Ihr Unternehmen und Ihre Mitarbeitenden nachhaltig schützen – ohne übermäßigen Aufwand oder teure Großprojekte.

Zielgruppe: Geschäftsführung, IT-Verantwortliche oder Compliance-Beauftragte – dieser Leitfaden ist für alle, die Verantwortung tragen.

Nutzen Sie dieses Wissen, um die Sicherheit in Ihrem Unternehmen zu stärken – bevor es zu spät ist.

Unternehmensprofil

Suppora GmbH – Ihr Partner für IT-Sicherheit, Support, ERP & Automatisierung

Die Suppora GmbH ist ein inhabergeführtes IT-Dienstleistungsunternehmen mit Sitz in Worms. Wir unterstützen kleine und mittlere Unternehmen (KMUs) dabei, ihre IT-Infrastruktur sicher, effizient und zukunftsorientiert aufzustellen.

Unser Leistungsspektrum

Bereich	Beschreibung
IT-Support	Modulare Supportpakete für stabile Betriebsabläufe
IT-Sicherheit	Passgenaue Schutzkonzepte und NIS2-Begleitung
ERP-Services	Oracle JD Edwards EnterpriseOne Spezialisierung
Automatisierung	Prozessoptimierung und Effizienzsteigerung

Unser Anspruch

IT für Unternehmen verständlich, zuverlässig und leistungsfähig zu gestalten. Dabei stehen Sicherheit, Stabilität und Skalierbarkeit ebenso im Fokus wie eine praxisnahe Umsetzung.

Was wir tun – und für wen

Suppora GmbH unterstützt kleine und mittlere Unternehmen dabei, ihre IT sicher, stabil und effizient zu gestalten. Wir bieten IT-Support, IT-Security-Lösungen und ERP-Services – **modular, verständlich und praxisnah**.

Unser Ziel: IT, die funktioniert, schützt und mitwächst.

Unser Ansatz

Ganzheitlicher Management Approach basierend auf einem praxisorientierten, klar strukturierten und anpassungsfähigen Vorgehen, das auf Transparenz, Qualität und kontinuierlicher Verbesserung ausgelegt ist.

7-SCHRITTE-BASIC-SECURITY-ANLEITUNG

So wenden Sie die 7 Schritte an

Starten Sie mit einer Bestandsaufnahme Ihrer Systeme und Risiken. Optimieren Sie anschließend Ihre Netzwerksicherheit, führen Sie ein regelmäßiges Patchmanagement ein und sorgen Sie für aktiven Virenschutz mit Monitoring. Schützen Sie Ihre Daten durch eine klare Backup-Strategie und sichern Sie Zugriffe mit MFA und Rollenrechten ab. Abschließend fördern Sie durch Schulungen und Awareness-Maßnahmen das Sicherheitsbewusstsein im Team.

1 | Bestandsaufnahme & Risikoanalyse

Ein grundlegendes Verständnis der eigenen IT-Landschaft ist die Basis jeder Sicherheitsstrategie. Unternehmen sollten systematisch erfassen:

- Welche IT-Systeme im Einsatz sind
- Welche davon kritisch für den Betrieb sind
- Wo sich sensible Daten befinden
- Dokumentation von Zugriffsrechten

Kernfrage: Wer hat Zugriff auf welche Daten und Systeme?

Nur mit einer klaren Übersicht lassen sich Risiken gezielt bewerten und priorisieren.

2 | Netzwerksicherheit verbessern

Das interne Netzwerk ist die Lebensader eines Unternehmens. Umso wichtiger ist es, dieses vor unbefugtem Zugriff zu schützen.

Wichtige Maßnahmen:

- Firewalls → Kontrolle des Datenverkehrs
- VLANs → Logische Trennung verschiedener Netzbereiche
- Segmentierung → Verhindert ungehinderte Ausbreitung von Angriffen

Beispiel-Segmente: Gastnetz | Büro | Produktion

3 | Patchmanagement & Updates

Veraltete Software zählt zu den häufigstenBEinfallstoren für Angriffe.

Regelmäßige Updates erforderlich für:

- Betriebssysteme
- Anwendungen
- Netzwerkkomponenten

Zentrale Verwaltung durch:

- WSUS
- MDM-Systeme
- Endpoint-Lösungen

Zusätzlich: Regelmäßige Schwachstellen-Scans durchführen

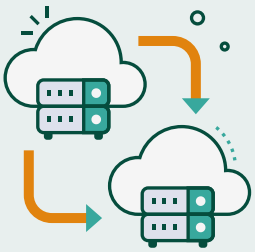
4 | Virenschutz & Monitoring

Ein aktueller und zentral verwalteter Virenschutz ist Pflicht.

Moderne Endpoint-Protection kombiniert:

- Signaturbasierten Schutz + KI-gestützte Verhaltensanalyse
- Echtzeit-Monitoring für sofortige Erkennung
- Automatisierte Benachrichtigungen bei verdächtigem Verhalten

5 | Datensicherung lokal & extern



Datenverlust kann entstehen durch:

- Betriebssysteme
- Anwendungen
- Netzwerkkomponenten

Die 3-2-1-Backup-Regel:

- 3 Kopien der Daten
- 2 verschiedene Medien
- 1 externe Sicherung

Zusätzlich: Regelmäßige Schwachstellen-Scans durchführen

6 | Zugriffsmanagement & Passwortrichtlinien

Zentrale Sicherheitsmaßnahmen:

- **Rollenbasierte Rechtevergabe** mit regelmäßiger Überprüfung
- **Multi-Faktor-Authentifizierung (MFA)** für alle kritischen Anwendungen
- **Keine gemeinsamen Accounts** → Sicherheitsrisiko vermeiden
- **Automatisiertes Offboarding** → Ehemalige Mitarbeitende ausschließen

4 | Awareness & IT-Training

Der Mensch bleibt das größte Einfallstor für Angriffe.

Regelmäßige Schulungen (mindestens 2x jährlich):

- Phishing-Erkennung
- Social Engineering
- Sichere Passwortnutzung

Bewusstseinsschärfung durch:

- Interne Kampagnen
- Poster & Infografiken
- Simulierte Phishing-Angriffe

ANTI-PHISHING-CHECKLISTE

(FÜR MITARBEITENDE)

Phishing-Angriffe gehören zu den häufigsten Einfallstoren für Cyberkriminalität – insbesondere in KMUs. Sie zielen darauf ab, Mitarbeitende zu täuschen und so an vertrauliche Daten oder Zugangsdaten zu gelangen.

Was Ihre Mitarbeitenden wissen müssen:

Prüfpunkt	Maßnahme
☑ Absender prüfen	Vertrauenswürdige Adresse? Domain korrekt? (nicht support@micros0ft.de)
☑ Anhänge meiden	Vorsicht bei .zip, .exe, .docm, .html-Formaten
☑ Dringlichkeit hinterfragen	"Letzte Mahnung", "Sofort handeln" → Emotionale Manipulation
☑ Linkziele prüfen	Maus über Link → URL mit Absender abgleichen
☑ Zugangsdaten schützen	Nie unaufgefordert Passwörter eingeben
☑ Melden bei Unklarheiten	IT-Abteilung informieren – lieber einmal zu viel fragen

Praxis-Tipp:

Richten Sie eine interne Meldeadresse ein – z.B. sicher@ihre-firma.de – und führen Sie regelmäßig simulierte Phishing-Angriffe durch, um die Aufmerksamkeit im Team hoch zu halten.

NIS2 REQUIREMENTS LIST

(KOMPAKT ERKLÄRT)

Wer ist betroffen?

Kriterien:

- Unternehmen mit > 50 Mitarbeitenden ODER
- > 10 Mio. € Jahresumsatz

Betroffene Sektoren:

- Energie, Transport, Gesundheit
- Digitale Dienste, IT-Dienstleister
- Produktion kritischer Güter
- u.v.m.

Was wird verlangt?

Bereich	Anforderung
Risikomanagement	Dokumentierte Prozesse zur Identifikation und Bewertung von IT-Risiken
Sicherheitsmaßnahmen	Firewalls, Backup-Strategien, Zugriffskontrolle, Awareness-Trainings
Notfallmanagement	Prozesse für Erkennung, Meldung und Reaktion bei IT-Vorfällen
Meldepflicht	Schwere Vorfälle innerhalb von 24 Stunden an zuständige Behörde

Was droht bei Nicht-Einhaltung?

- Bußgelder bis 10 Mio. € oder 2 % des Jahresumsatzes
- Persönliche Haftung von Geschäftsführung oder IT-Leitung
- Reputationsverlust bei öffentlich bekannt gewordenen Vorfällen

AWARENESS & SICHERHEITSKULTUR

Wichtiger Fakt: In über 70 % der Angriffe ist menschliches Fehlverhalten der Auslöser.

Phishing, schwache Passwörter und fehlende Aufmerksamkeit machen Unternehmen angreifbar. Deshalb ist eine starke Sicherheitskultur im Team entscheidend.

Ziel:

Die Belegschaft soll nicht als potenzielle Schwachstelle, sondern als aktive Verteidigungslinie wahrgenommen werden. Wer Risiken erkennt und richtig handelt, kann entscheidend dazu beitragen, Schäden zu vermeiden.

Wichtige Maßnahmen im Unternehmen:

Regelmäßige Schulungen

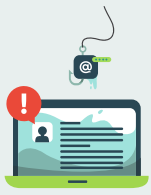
- **Häufigkeit:** Mindestens zweimal jährlich
- **Themen:** Social Engineering, Phishing, sichere Passwörter, Datenschutz
- **Format:** Digital oder vor Ort

Infografiken & Poster

Sichtbare Erinnerungen im Büro zu:

- Sicheren Passwörtern
- Verhalten bei verdächtigen E-Mails
- Bedeutung von Software-Updates

Simulierte Phishing-Angriffe



- Gezielte Phishing-Tests durchführen
- Schwachstellen identifizieren
- Gezielt nachschulen

Meldekultur etablieren

- Leichte Meldung ohne Konsequenzen
- Eigene Adresse: sicher@firmenname.de

Gamification-Ansätze

- · IT-Security-Quiz
- · Challenges
- · Security-Escape-Room

Verantwortung zuweisen

Jede Abteilung sollte eine:n Sicherheitsbeauftragte:n benennen als Ansprechperson und Multiplikator:in.

SELBSTCHECK: WIE SICHER IST IHRE IT?

Dieser Selbstcheck hilft Ihnen, schnell und einfach den Status Ihrer IT-Sicherheit einzuschätzen. Die folgenden Fragen decken zentrale Bereiche der IT-Sicherheitsstrategie ab.

Sicherheits-Fragebogen

Frage	Ja/Nein
Gibt es MFA für alle kritischen Systeme? Multi-Faktor-Authentifizierung verhindert unbefugten Zugriff auch bei kompromittierten Passwörtern.	
Werden Backups regelmäßig getestet? Nur getestete Backups bieten im Ernstfall Sicherheit und stellen den Geschäftsbetrieb wieder her.	
Haben alle Mitarbeitenden IT-Security-Schulungen absolviert? Geschultes Personal ist der wichtigste Schutz vor Phishing und Social Engineering.	
Gibt es eine Notfall- und Wiederanlaufplanung? Ein strukturierter Plan sichert die schnelle Reaktion im Ernstfall.	
Wird die Einhaltung von NIS2 geprüft? Nur wer regelmäßig prüft, bleibt konform und vermeidet Bußgelder.	

Bewertung:

Ergebnis	Status	Handlungsbedarf
5x Ja	Sehr gut aufgestellt	Weiter so!
3-4x Ja	Handlungsbedarf mittelfristig	Verbesserungen planen
5xNein	Sofort handeln	Dringender Handlungsbedarf

FAZIT & NÄCHSTE SCHRITTE

Die Herausforderung

Oft fehlt es an:

- Kapazitäten
- Übersicht
- Spezialisierten Fachkräften

Ihr Fahrplan

Mit diesem IT-Security-Leitfaden haben Sie einen praxisnahen Fahrplan an der Hand, um Schritt für Schritt mehr Sicherheit, Transparenz und Kontrolle in Ihre IT zu bringen. Von technischen Grundlagen über Mitarbeitersensibilisierung bis hin zu gesetzlichen Anforderungen zeigt dieser Leitfaden, worauf es ankommt.

Unser Angebot

Jede Organisation ist anders. Deshalb endet unser Leitfaden nicht mit einer Checkliste, sondern mit einem Angebot: Die Suppora GmbH unterstützt Sie dabei, den Weg zur sicheren IT aktiv zu gestalten – mit individuellen Assessments, praxisnahen Empfehlungen und einer partnerschaftlichen Begleitung auf Augenhöhe.

Unsere Empfehlung:

Nutzen Sie unser kostenfreies IT-Infrastruktur- & IT-Security-Assessment, um innerhalb von 30 Minuten zu erfahren:

- Wo Ihre größten Risiken liegen
- Ob Sie NIS2-relevant sind
- Welche Maßnahmen kurzfristig Wirkung zeigen
- Wie Sie mit überschaubarem Aufwand Ihre IT-Struktur absichern

KONTAKT

Sie möchten Ihre IT absichern, Ihre Infrastruktur modernisieren oder ein unverbindliches Security-Assessment durchführen?
Wir sind für Sie da – persönlich, verständlich und lösungsorientiert.

Suppora GmbH
IT-Sicherheit • IT-Support • Automatisierung • ERP (Oracle JDE)

Herrnsheimer Hauptstraße 1b 67550 Worms, Deutschland

+49 (0)6241 85 72 36 0 info@suppora.eu www.suppora.eu

Unsere Empfehlung:
Vereinbaren Sie jetzt ein kostenloses Erstgespräch oder fordern Sie unser IT-Sicherheits-Assessment an – kompakt, praxisnah und individuell.

Direkte Links:

Termin vereinbaren **Assessment anfordern**

Suppora GmbH – Ihr Partner für professionelle IT-Betreuung

Abschließender Hinweis:
Dieser Leitfaden ersetzt keine individuelle Sicherheitsberatung, bietet aber einen bewährten und sofort umsetzbaren Fahrplan für KMUs, um die IT-Sicherheit spürbar zu verbessern und gesetzliche Vorgaben wie NIS2 zu erfüllen.