Cyber-Resilienz-Report 2026 — Risiken erkennen, bewerten, priorisieren

Ein analytischer Lagebericht für Geschäftsführung und IT-Verantwortliche im deutschen Mittelstand · Ausgabe 2026

Cyber-Risiken sind längst kein reines IT-Thema mehr, sondern eine **unternehmerische Kernfrage**. Dieser Report übersetzt die abstrakte Bedrohungslage in konkrete, bewertbare Risiken — und zeigt, wo im Mittelstand die größten Lücken klaffen und welche Maßnahmen den größten Hebel haben. Statt langer Texte sprechen hier die **Daten**: Reifegrade, Risikomatrizen, Schadenskosten und Prioritäten auf einen Blick.

Inhalt

MANAGEMENT SUMMARY — DAS WICHTIGSTE IN KÜRZE

- **Mehr als jedes zweite mittelständische Unternehmen** war in den letzten zwei Jahren von mindestens einem sicherheitsrelevanten Vorfall betroffen — Tendenz steigend. - Der typische **Cyber-Reifegrad im Mittelstand liegt bei rund 54 von 100 Punkten** — solide Technik, aber deutliche Schwächen bei Organisation, Awareness und Notfallmanagement. - **Schäden entstehen selten durch das Lösegeld allein**: Betriebsausfall, Wiederherstellung und Reputationsverlust machen den Großteil der Gesamtkosten aus. - Die wirkungsvollsten Maßnahmen sind **nicht die teuersten**: MFA, getestete Backups und Awareness-Schulungen senken das Risiko überproportional.

1 · Die Bedrohungslage 2026

Wie sich Angriffe entwickeln — und wen sie treffen

Die Professionalisierung der Angreifer schreitet voran. **Ransomware-as-a-Service**, automatisierte Schwachstellen-Scans und KI-gestütztes Phishing senken die Einstiegshürde für Kriminelle — während der Mittelstand als lohnendes Ziel zunehmend in den Fokus rückt. Die folgenden Kennzahlen ordnen die Lage in seriösen Größenordnungen ein.

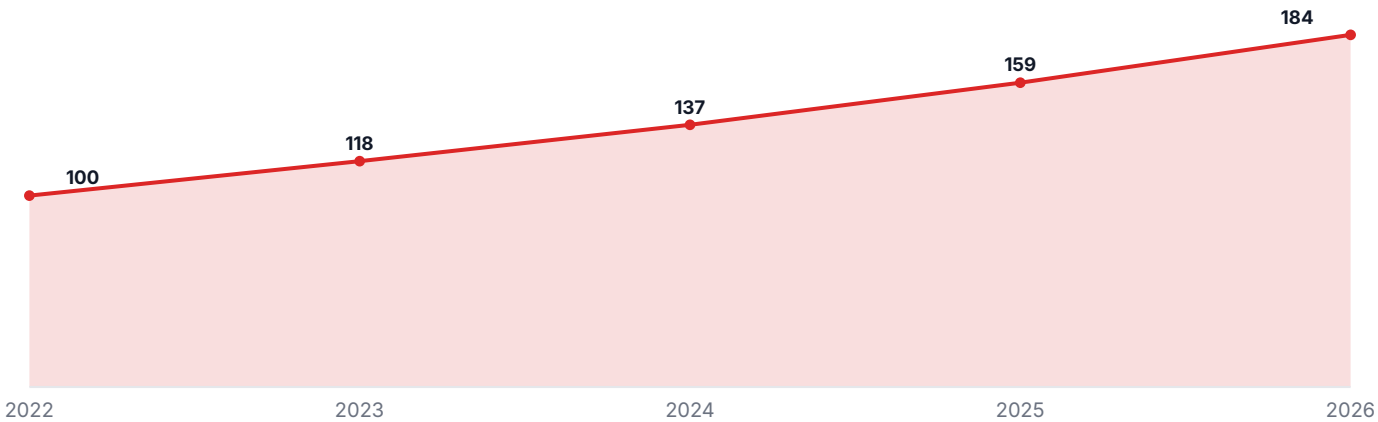
~58 %
der mittelständischen Unternehmen mit Vorfall (24 Monate)
ggü. 2024

~95.000 €
durchschnittliche Schadenshöhe je Vorfall (KMU)
ggü. 2024

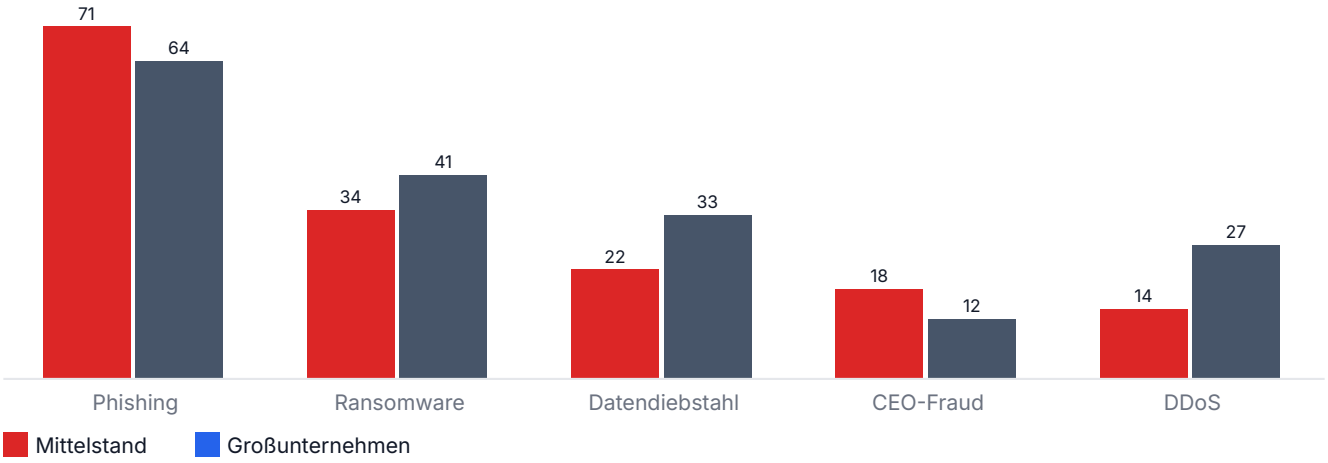
~7 Tage
durchschnittliche Ausfalldauer bis zur Wiederherstellung
ggü. 2024

< 24 Std.
typische Zeit bis zum Erstangriff auf neu exponierte Systeme
ggü. 2024

Bedrohungsindex Mittelstand 2022 → 2026 (Index, 2022 = 100)



Häufigste Angriffsarten: Mittelstand vs. Großunternehmen (Anteil betroffener Unternehmen, %)



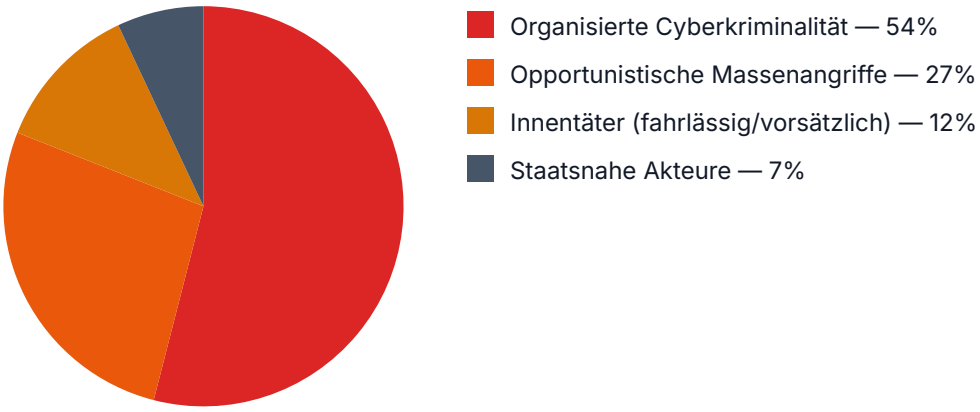
Größe schützt nicht

Der verbreitete Irrglaube „Wir sind zu klein, um interessant zu sein" ist gefährlich. Gerade **automatisierte, ungezielte Angriffe** treffen kleine und mittlere Unternehmen härter — weil dort Schutzmaßnahmen und Notfallpläne häufiger fehlen.

Wer hinter den Angriffen steckt

Die wenigsten Angriffe sind gezielte Aktionen gegen ein bestimmtes Unternehmen. Der Großteil entsteht durch **organisierte, arbeitsteilige Cyberkriminalität** und breit gestreute Massenangriffe, die jede erreichbare Schwachstelle ausnutzen.

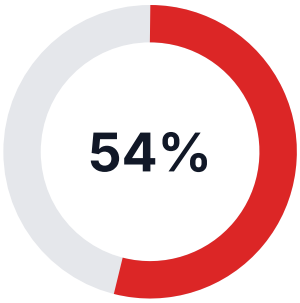
Bedrohungsakteure — Anteil an den Vorfällen (%)



2 · Ihr Cyber-Reifegrad

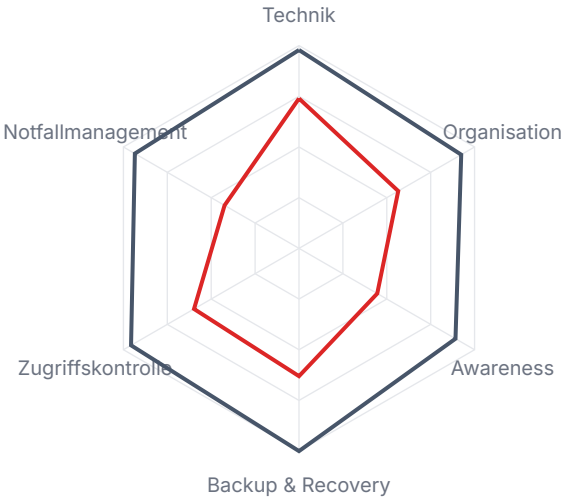
Wo der Mittelstand heute steht

Cyber-Resilienz ist mehr als Technik. Der folgende Reifegrad bewertet sechs Dimensionen auf einer Skala von 0 bis 100. Der typische Mittelstand erreicht solide Grundwerte bei Technik, fällt aber bei **Awareness und Notfallmanagement** deutlich ab — genau dort, wo im Ernstfall über Schaden oder Schadensbegrenzung entschieden wird.



Typischer Cyber-Resilienz-Score im Mittelstand

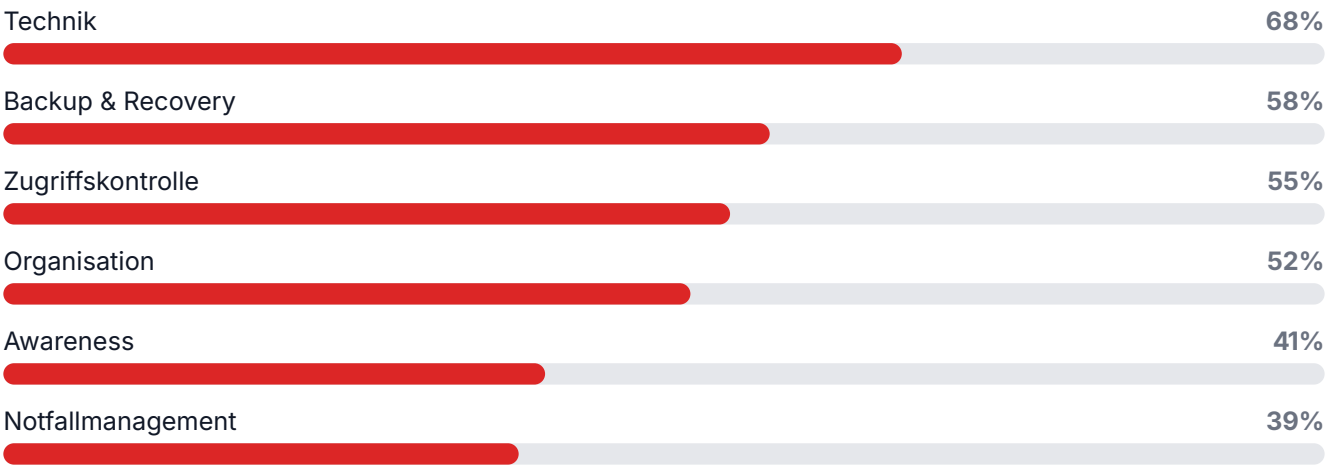
Reifegrad nach Dimension: Mittelstand Ø vs. Best Practice



- **Technik**
  Firewalls, Endpoint-Schutz, Patch-Management — meist vorhanden, aber nicht durchgängig aktuell.
- **Organisation**
  Verantwortlichkeiten, Richtlinien und dokumentierte Prozesse für IT-Sicherheit.
- **Awareness**
  Schulung und Sensibilisierung der Mitarbeitenden gegen Phishing und Social Engineering.
- **Backup & Recovery**
  Regelmäßige, getestete Datensicherungen mit definierter Wiederanlaufzeit.
- **Zugriffskontrolle**
  Berechtigungskonzepte, Mehr-Faktor-Authentifizierung und Least-Privilege-Prinzip.
- **Notfallmanagement**
  Geprobte Incident-Response-Pläne, Eskalationswege und Krisenkommunikation.

Reifegrad im Detail — wo der Hebel liegt

Reifegrad je Dimension (Mittelstand Ø, 0–100)



Der größte Hebel liegt nicht in der Technik

Die schwächsten Dimensionen sind **Awareness (41)** und **Notfallmanagement (39)** — zugleich die mit dem besten Aufwand-Wirkung-Verhältnis. Eine geprobte Notfallorganisation und sensibilisierte Mitarbeitende senken das Risiko stärker als jede weitere Investition in Technik.

3 · Risiken erkennen & bewerten

Von der Bauchentscheidung zur belastbaren Priorität

Risiko ist das Produkt aus **Eintrittswahrscheinlichkeit** und **Schadenshöhe**. Die Risikomatrix macht sichtbar, welche Szenarien zuerst Aufmerksamkeit verdienen. Die Heatmap ergänzt: Nicht jede Abteilung ist gleich exponiert.

Risikomatrix — Risikoscore (1 = gering, 25 = kritisch)

	Selten	Gelegentlich	Möglich	Häufig	Sehr häufig
Sehr hoch	5	10	15	20	25
Hoch	4	8	12	16	20
Mittel	3	6	9	12	15
Gering	2	4	6	8	10
Sehr gering	1	2	3	4	5

1 · Ransomware-Verschlüsselung	**Sehr hohe Schadenshöhe × möglich → kritisch (Score 15–20)**
2 · Phishing / Account-Übernahme	**Hohe Schadenshöhe × sehr häufig → kritisch (Score 16–20)**
3 · Datenabfluss / DSGVO-Verstoß	**Hohe Schadenshöhe × möglich → hoch (Score 12)**

4 · Ausfall durch fehlende Backups	**Sehr hohe Schadenshöhe × gelegentlich → hoch (Score 10)**
5 · Insider / Fehlkonfiguration	**Mittlere Schadenshöhe × häufig → erhöht (Score 12)**

Exposition: Bedrohung × Abteilung (1 = niedrig, 5 = sehr hoch)

	Geschäftsführung	Finanzen	Vertrieb	Produktion
Phishing	4	5	5	3
Ransomware	3	4	3	5
CEO-Fraud	5	5	2	1
Datendiebstahl	3	5	4	2
Schatten-IT	2	2	4	3

4 · Die Angriffskette verstehen

Vom ersten Klick bis zur Erpressung

Phishing-Funnel — was aus 1.000 versendeten E-Mails wird

Tag 0 — **Erstzugang**
Kompromittierte Zugangsdaten oder Phishing-Anhang verschaffen den Angreifern einen Fuß in der Tür.

Tag 1–3 — **Persistenz & Aufklärung**
Hintertüren werden eingerichtet, das Netzwerk wird kartiert, Backups und Domänen-Controller identifiziert.

Tag 4–10 — **Rechte-Ausweitung**
Über Privilege Escalation erlangen die Angreifer Administratorrechte und bewegen sich seitlich durchs Netz.

Tag 11–18 — **Datenabfluss**
Sensible Daten werden exfiltriert — Grundlage für die spätere doppelte Erpressung (Double Extortion).

Tag 19–20 — **Sabotage der Backups**
Sicherungen werden gelöscht oder verschlüsselt, um die Wiederherstellung zu verhindern.

Tag 21 — **Verschlüsselung & Erpressung**
Die eigentliche Ransomware wird ausgelöst; parallel folgt die Lösegeldforderung mit Veröffentlichungsdrohung.

> **Die Stunde Null liegt früher als gedacht**
>
> Zwischen Erstzugang und sichtbarer Verschlüsselung liegen oft **mehrere Wochen**. In diesem Zeitfenster lassen sich Angriffe mit guter Überwachung (EDR, Log-Auswertung) erkennen und stoppen — bevor der eigentliche Schaden entsteht.

Frühwarnsignale eines laufenden Angriffs

Diese Anzeichen sollten sofort Alarm auslösen

- [ ] **Anmeldungen zu ungewöhnlichen Zeiten oder aus unerwarteten Ländern**
  Besonders bei Admin- und Geschäftsführungskonten.
- [ ] **Virenschutz oder Sicherheits-Tools wurden unerwartet deaktiviert**
- [ ] **Neue, unbekannte Administrator- oder Dienstkonten tauchen auf**
- [ ] **Massenhaft umbenannte oder verschlüsselte Dateien auf Freigaben**
- [ ] **Ungewöhnlich hoher ausgehender Datenverkehr — vor allem nachts**
- [ ] **Backups schlagen plötzlich fehl oder wurden gelöscht**

5 · Was ein Vorfall kostet

Die wahren Kosten liegen jenseits des Lösegelds

Schadenskosten eines mittelschweren Ransomware-Vorfalls (kumulativ, €)

~121.000 €
typischer Gesamtschaden eines mittelschweren Ransomware-Vorfalls

~7 Tage
mittlere Ausfalldauer bis zum Normalbetrieb

~60 %
Anteil indirekter Kosten am Gesamtschaden

~1 von 4
betroffene Unternehmen mit Folgeschäden über Monate

Gut vorbereitet

- \+ Getestete Offline-Backups → Wiederanlauf in Stunden statt Tagen
- \+ Geprobter Notfallplan → klare Rollen, ruhige Entscheidungen
- \+ Cyber-Versicherung & Incident-Response-Partner griffbereit
- \+ Transparente Krisenkommunikation erhält Kundenvertrauen

Unvorbereitet

- x Keine nutzbaren Backups → vollständiger Datenverlust droht
- x Chaos und Improvisation → längere Ausfälle, Fehlentscheidungen
- x Lösegeldzahlung ohne Garantie auf Entschlüsselung
- x Vertrauensverlust bei Kunden, Partnern und Aufsichtsbehörden

Cyber-Versicherung — Schutz und Grenzen

Typisch gedeckt	**Betriebsunterbrechung, Forensik & Wiederherstellung, Rechts- und Beratungskosten, teils Lösegeld**

Häufig ausgeschlossen	**Grobe Fahrlässigkeit, fehlende Mindeststandards, Vorsatz, Krieg/Staatsangriffe**
Voraussetzung	**Nachweis von MFA, getesteten Backups, Patch-Management und Awareness-Maßnahmen**
Wichtig	**Eine Police ersetzt keine Prävention — sie senkt die finanzielle Folge, nicht die Eintrittswahrscheinlichkeit**

Versicherer verlangen Mindeststandards

Ohne nachgewiesene **Mehr-Faktor-Authentifizierung** und **getestete Backups** wird im Schadensfall die Leistung gekürzt oder verweigert. Die Versicherung ist also nur so gut wie die Prävention dahinter.

6 · Maßnahmen & Priorisierung

Der 30/60/90-Tage-Fahrplan

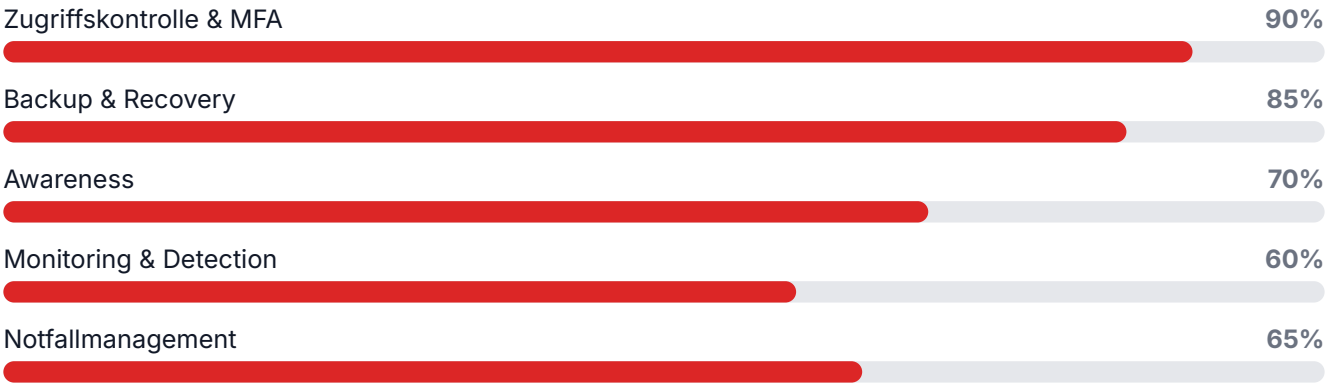
1. **0–30 Tage · Sofortmaßnahmen**
   MFA für alle Konten aktivieren, Backups prüfen und offline sichern, kritische Systeme patchen, exponierte Dienste schließen.
2. **30–60 Tage · Stabilisieren**
   Berechtigungen aufräumen (Least Privilege), Endpoint-Detection einführen, Awareness-Schulung starten, Notfallkontakte festlegen.
3. **60–90 Tage · Verankern**
   Incident-Response-Plan dokumentieren und proben, Monitoring ausbauen, Lieferketten-Risiken bewerten, Cyber-Versicherung prüfen.

Maßnahme	Aufwand	Wirkung
Mehr-Faktor-Authentifizierung (MFA)	Gering	Sehr hoch
Getestete Offline-/Air-Gap-Backups	Mittel	Sehr hoch
Awareness-Schulung der Mitarbeitenden	Gering	Hoch
Konsequentes Patch-Management	Mittel	Hoch
Endpoint Detection & Response (EDR)	Hoch	Hoch
Netzsegmentierung	Hoch	Mittel
Geprobter Incident-Response-Plan	Mittel	Hoch
Least-Privilege-Berechtigungen	Mittel	Hoch

12 Quick-Wins für die nächsten 90 Tage

- [ ] **MFA für E-Mail, VPN und Admin-Konten aktiviert**
- [ ] **Mindestens eine Backup-Kopie offline / unveränderlich gelagert**
- [ ] **Wiederherstellung aus Backup einmal real getestet**
- [ ] **Alle Systeme mit aktuellen Sicherheitsupdates versorgt**
- [ ] **Nicht benötigte Fernzugänge (RDP) aus dem Internet entfernt**
- [ ] **Admin-Rechte auf das notwendige Minimum reduziert**
- [ ] **Phishing-Awareness-Schulung durchgeführt**
- [ ] **Notfallkontakte und Eskalationsweg dokumentiert**
- [ ] **Endpoint-Schutz mit Verhaltenserkennung im Einsatz**
- [ ] **Passwort-Richtlinie und Passwort-Manager etabliert**
- [ ] **Lieferanten- und Dienstleister-Zugänge überprüft**
- [ ] **Cyber-Versicherung und Deckungsumfang geprüft**

Ziel-Umsetzungsgrad je Handlungsfeld (Zielwert nach 90 Tagen)



FAZIT

Cyber-Resilienz entsteht nicht durch ein einzelnes Produkt, sondern durch das **Zusammenspiel aus Technik, Organisation und Menschen**. Wer die größten Lücken zuerst schließt — MFA, getestete Backups, Awareness und ein geprobter Notfallplan — senkt sein Risiko mit überschaubarem Aufwand erheblich. Der entscheidende Schritt ist, **jetzt** zu beginnen und Fortschritt messbar zu machen.

Lohnt sich Cyber-Sicherheit für ein kleines Unternehmen überhaupt?

Ja. Gerade kleinere Unternehmen werden Ziel automatisierter Angriffe und haben seltener Schutzmaßnahmen. Die Grundabsicherung (MFA, Backups, Updates, Schulung) ist günstig und hochwirksam.

Sollten wir im Ernstfall Lösegeld zahlen?

Behörden und Sicherheitsexperten raten grundsätzlich davon ab. Eine Zahlung garantiert keine Entschlüsselung, finanziert die Täter und macht das Unternehmen zum erneuten Ziel. Getestete Backups sind die bessere Versicherung.

Wie oft sollten wir Backups testen?

Mindestens vierteljährlich sollte eine Wiederherstellung real geprobt werden — ein Backup, das sich nicht zurückspielen lässt, ist wertlos.

Was bedeutet NIS2 für unser Unternehmen?

Die NIS2-Richtlinie erweitert die Pflichten zur Cyber-Sicherheit auf deutlich mehr Unternehmen, auch im Mittelstand. Frühzeitige Bestandsaufnahme und Dokumentation schaffen Klarheit über die eigene Betroffenheit.

Reicht eine Firewall nicht aus?

Nein. Moderne Angriffe umgehen klassische Perimeter-Schutzmaßnahmen. Notwendig ist ein mehrschichtiger Ansatz mit Endpoint-Schutz, Berechtigungskonzepten, Überwachung und geschulten Mitarbeitenden.

Wo fangen wir mit begrenztem Budget an?

Bei den Quick-Wins mit dem besten Aufwand-Wirkung-Verhältnis: MFA aktivieren, Backups offline sichern und testen, Updates einspielen und Mitarbeitende schulen.

7 · NIS2 & rechtliche Pflichten

Was 2026 auf den Mittelstand zukommt

Mit der **NIS2-Richtlinie** weitet der Gesetzgeber den Kreis der regulierten Unternehmen erheblich aus. Betroffen sind nicht nur Betreiber kritischer Infrastruktur, sondern auch viele mittelständische Zulieferer und Dienstleister in wichtigen Sektoren. Neu ist vor allem: Die **Geschäftsleitung haftet persönlich** für ein angemessenes Risikomanagement.

NIS2-Pflichten im Überblick

- [ ] **Risikomanagement für IT-Sicherheit etablieren und dokumentieren**
- [ ] **Meldepflicht: Frühwarnung an die Behörde binnen 24 Stunden**
  Vollständige Meldung folgt innerhalb von 72 Stunden.
- [ ] **Sicherheit der Lieferkette bewerten und steuern**
- [ ] **Technische und organisatorische Mindestmaßnahmen umsetzen (u. a. MFA, Backups, Verschlüsselung)**
- [ ] **Nachweis- und Dokumentationspflichten erfüllen**
- [ ] **Leitungsebene schulen — die Verantwortung ist nicht delegierbar**

> **DSGVO-Fristen gelten zusätzlich**
>
> Unabhängig von NIS2 bleibt die **72-Stunden-Meldepflicht der DSGVO** bei Datenpannen bestehen. Wer beide Regime erfüllen muss, braucht einen integrierten Notfallplan — Details dazu im *DSGVO-Notfallhandbuch*.

Anhang

Glossar, Quellen und Kontakt

Glossar

Ransomware
Schadsoftware, die Daten verschlüsselt und für die Freigabe ein Lösegeld fordert.

Phishing
Täuschungsangriff, der über gefälschte Nachrichten an Zugangsdaten oder Geld gelangen will.

MFA (Mehr-Faktor-Authentifizierung)
Anmeldung mit mindestens zwei unabhängigen Faktoren, z. B. Passwort plus Einmalcode.

EDR (Endpoint Detection & Response)
Software, die verdächtiges Verhalten auf Endgeräten erkennt und automatisiert reagiert.

Zero Trust
Sicherheitsmodell nach dem Prinzip „niemals vertrauen, immer prüfen" — jeder Zugriff wird verifiziert.

RTO / RPO
Recovery Time Objective (zulässige Ausfallzeit) und Recovery Point Objective (zulässiger Datenverlust) definieren Backup-Ziele.

Air-Gap
Physische oder logische Trennung eines Backups vom Netzwerk, damit Angreifer es nicht erreichen.

Double Extortion
Doppelte Erpressung: Daten werden verschlüsselt und zusätzlich mit Veröffentlichung gedroht.

BSI
Bundesamt für Sicherheit in der Informationstechnik — zentrale deutsche Cyber-Sicherheitsbehörde.

NIS2
EU-Richtlinie zur Erhöhung der Cyber-Sicherheit, die erweiterte Pflichten für viele Unternehmen einführt.

Quellen & weiterführende Informationen

[1] BSI — Die Lage der IT-Sicherheit in Deutschland (jährlicher Lagebericht), Bundesamt für Sicherheit in der Informationstechnik.
[2] BSI — IT-Grundschutz-Kompendium und Empfehlungen für kleine und mittlere Unternehmen.
[3] ENISA Threat Landscape — European Union Agency for Cybersecurity, jährlicher Bedrohungslagebericht.
[4] Richtlinie (EU) 2022/2555 (NIS2) — Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der EU.
[5] Allianz für Cyber-Sicherheit — Handlungsempfehlungen und Lagebilder für die Wirtschaft.
[6] Verband der deutschen Wirtschaft — Studien zu Schäden durch Cyber-Kriminalität im Mittelstand.

ÜBER DEN AUTOR

SW Business Solutions

IT-Sicherheit & Beratung für den Mittelstand

Wir begleiten mittelständische Unternehmen praxisnah auf dem Weg zu belastbarer Cyber-Resilienz — von der Standortbestimmung über die Priorisierung bis zur Umsetzung. Unser Anspruch: **verständlich, herstellerneutral und an Ihrem tatsächlichen Risiko ausgerichtet**. Dieser Report fasst unsere Beratungserfahrung in einem datengetriebenen Lagebild zusammen.

IHR ANSPRECHPARTNER

SW Business Solutions

IT-Sicherheit & Beratung

info@sw-business-solutions.de

Wie resilient ist Ihr Unternehmen wirklich?

Machen Sie den kostenlosen IT-Sicherheits-Check und erhalten Sie eine erste Einschätzung Ihres Reifegrads — in wenigen Minuten.

https://www.sw-business-solutions.de/leadmagnete