Fox Romeo

IT-Sicherheit im Mittelstand

Risikobasiert, praktikabel, gesetzeskonform – ohne Paranoia

Inhalt

Management Summary

Die Cybersicherheitslage für den deutschen Mittelstand ist angespannt – und wird es auf absehbare Zeit bleiben. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt die Lage der IT-Sicherheit in Deutschland 2024 als „besorgniserregend“, mit einer weiter steigenden Professionalisierung der Angreifer und täglich hunderttausenden neuen Malware-Varianten.

Laut Bitkom entsteht der deutschen Wirtschaft jährlich ein Schaden von rund **200+ Milliarden Euro** durch Datendiebstahl, Spionage und Sabotage – zum dritten Mal in Folge liegt der Wert über dieser Marke. Ein erheblicher Teil dieser Schäden entsteht in kleinen und mittleren Unternehmen (KMU).

Gleichzeitig sind Sicherheitskonzepte im Mittelstand oft von zwei Extremen geprägt:

- **Angstmacherei**: überteuerte, überdimensionierte Lösungen, getrieben von Security-Marketing statt von Risikobewertung.
- **Ignoranz**: „Wir sind zu klein, um interessant zu sein“, minimale Schutzmaßnahmen, Compliance als lästiges Anhängsel.

Dieses Whitepaper zeigt einen Weg dazwischen: **IT-Sicherheit als nüchternes Risikomanagement**. Statt maximaler Sicherheit um jeden Preis geht es um **angemessenen Schutz** auf Basis von realistischen Bedrohungen, wirtschaftlicher Vernunft und regulatorischen Mindeststandards (DSGVO, NIS2 & Co.).

Kernbotschaften:

1. **Die meisten Angriffe sind opportunistisch und automatisiert** – kein James-Bond-Hacker, sondern Massenangriffe, die dort zuschlagen, wo die Abwehr am schwächsten ist.
2. **Ransomware & Social Engineering** sind die dominierenden Bedrohungen, verstärkt durch professionelle RaaS-Ökosysteme (Ransomware-as-a-Service) und KI-gestützte Phishing-Kampagnen.
3. **Compliance ist Pflicht, aber kein Sicherheitskonzept** – DSGVO, NIS2 und branchenspezifische Vorgaben definieren Mindeststandards, ersetzen aber keine Risikosteuerung.
4. **Ein dreistufiges Sicherheits-Reifegradmodell** ermöglicht Mittelständlern, ihren Status zu bestimmen und zielgerichtet das passende Schutzniveau anzusteuern – ohne die Organisation zu überfordern.
5. **Pragmatische Security gewinnt**: Passwort-Manager statt absurder Passwort-Policies, sinnvolle Cloud-Governance statt Schatten-IT, Rollen- und Rechtekonzepte statt „alles für alle“.

Das Ergebnis: Ein **umsetzbarer Fahrplan** für mittelständische Unternehmen, die ihre IT-Sicherheit professionalisieren wollen, ohne sich in Paranoia oder Theorie zu verlieren.

1. Ausgangslage: Warum IT-Sicherheit im Mittelstand jetzt Chefsache ist

1.1 Wirtschaftlicher Schaden und Bedrohungsentwicklung

Die Zahlen sprechen eine klare Sprache:

- Die deutsche Wirtschaft verzeichnet jährlich rund **206 Milliarden Euro Schaden** durch Diebstahl von IT-Ausrüstung und Daten, Spionage und Sabotage.
- Die Schäden liegen seit mehreren Jahren stabil über 200 Milliarden Euro – ein dauerhaft hohes Niveau, kein Ausreißer.
- Bitkom-Studien zeigen, dass in vielen Fällen organisierte Kriminalität hinter den Angriffen steht; KMU werden zunehmend zum primären Ziel, weil sie als leichter angreifbar gelten.

Der BSI-Lagebericht 2024 weist darauf hin, dass die **Bedrohungslage angespannt bleibt** und Angreifer dort zuschlagen, wo sie **am wenigsten Gegenwehr** erwarten – also häufig bei mittelständischen Unternehmen mit unzureichenden Sicherheitsmaßnahmen.

Parallel dazu identifiziert die EU-Agentur ENISA in ihrem **Threat Landscape 2024** Ransomware, Angriffe auf Verfügbarkeit (z. B. DDoS) und Angriffe auf Daten als zentrale Bedrohungen in Europa.

1.2 Mittelstand als bevorzugtes Ziel

Für professionelle Angreifer sind Mittelständler attraktiv:

- **Genug Geld**, um interessante Lösegeldsummen zahlen zu können
- **Genug Komplexität**, um Fehler und Sicherheitslücken zu produzieren
- **Zu wenig spezialisierte Security-Ressourcen**, um eine professionelle Verteidigung aufzubauen

Ransomware-as-a-Service (RaaS) hat die Professionalisierung der Angriffe massiv beschleunigt: Organisierte Gruppen stellen fertige Angriffswerkzeuge, Leak-Seiten und Zahlungsabwicklung bereit; „Affiliates“ führen die Angriffe aus. Schon grundlegende Schutzdefizite – ungepatchte VPNs, schwache Passwörter, fehlende Multi-Faktor-Authentifizierung – reichen, um Opfer zu werden.

2. Wie IT-Sicherheit im Mittelstand oft falsch verstanden wird

In vielen Unternehmen begegnet man zwei Extremen, die beide nicht funktionieren.

2.1 Extrem 1: Angstmacherei und Produktfetischismus

- Fokus auf „Next-Gen“-Produkte statt auf Risiken
- komplexe, teure Lösungen, die niemand vollständig versteht

- Security als Marketing-Schlachtfeld, nicht als Managementaufgabe

Folge:

- überdimensionierte Architekturen
- frustrierte Anwender
- hohe Kosten bei fragwürdiger Wirksamkeit

2.2 Extrem 2: Ignoranz und Minimallösungen

Typische Sätze:

- „Uns hackt niemand, wir sind zu klein."
- „Wir haben doch Antivirus und eine Firewall."
- „DSGVO machen wir später."

Folge:

- Datenschutzverstöße und Bußgelder
- Geschäftsunterbrechungen durch Ransomware
- persönliche Haftungsrisiken für Geschäftsführung und Vorstand

2.3 Der Weg dazwischen: Sicherheit als Risikomanagement

Die Wahrheit liegt in der Mitte:

Es geht nicht um maximale Sicherheit, sondern um **angemessenen Schutz** – abhängig von Branche, Unternehmensgröße, Schutzbedarfen und Risikobereitschaft.

Kernfragen:

- Welche Daten sind wirklich geschäftskritisch oder besonders schützenswert?
- Welche Systeme verursachen im Ausfall den größten Schaden?
- Welche Bedrohungen sind für unsere Branche realistisch?
- Welche **Versicherungs- und Compliance-Anforderungen** müssen wir mindestens erfüllen?

3. Risikobasiertes Sicherheitsmodell für KMU

3.1 Schritt 1: Schutzbedarfe identifizieren

Statt alle Systeme „gleich sicher" zu machen, sollten Mittelständler Schutzbedarfe definieren, z. B.:

- **Vertraulichkeit**: Kunden- und Mitarbeiterdaten, Konstruktionsunterlagen, Preislisten
- **Integrität**: ERP-/Warenwirtschaftsdaten, Produktionsrezepte, Dokumentenmanagement

- **Verfügbarkeit**: Produktionsanlagen, E-Mail, Telefonie, Cloud-Dienste

Typische Kategorien:

- **hochkritisch**: Stillstand > 24h bedroht die Existenz / führt zu hohen Konventionalstrafen
- **kritisch**: Stillstand > 1–3 Tage verursacht spürbare Schäden
- **unkritisch**: Stillstand über mehrere Tage tolerierbar

3.2 Schritt 2: Bedrohungen und Schwachstellen analysieren

Praxisnahe Fragen:

- Wo können Angreifer von außen „anlanden“? (VPN, RDP, Mail, Web-Anwendungen, Lieferanten-Zugänge)
- Gibt es bekannte Sicherheitslücken in exponierten Systemen? (Patch-Management, Schwachstellenscans)
- Wie leicht lassen sich Mitarbeitende über Phishing angreifen?
- Welche externen Dienstleister haben weitreichende Zugriffsrechte?

3.3 Schritt 3: Risiko bewerten (Eintrittswahrscheinlichkeit × Schadenshöhe)

Eine einfache Risikomatrix (z. B. niedrig, mittel, hoch) reicht in der Praxis oft aus:

- *Wahrscheinlichkeit hoch, Schaden hoch* → **Priorität A**
- *Wahrscheinlichkeit niedrig, Schaden hoch* → **Priorität B**
- *Wahrscheinlichkeit hoch, Schaden niedrig* → **Priorität C**

3.4 Schritt 4: Maßnahmen nach Wirtschaftlichkeit priorisieren

Für jedes priorisierte Risiko:

- Welche Maßnahmen reduzieren das Risiko **substanziell**?
- Was kostet die Maßnahme im Vergleich zum potenziellen Schaden?
- Welche Maßnahmen sind ohnehin für **Compliance oder Versicherer** erforderlich?

Beispiele:

- MFA für alle externen Zugänge → geringe Kosten, sehr hoher Effekt
- Immutable Backups und Notfallplan → mittlere Kosten, extrem hoher Effekt bei Ransomware
- Einführung eines Passwort-Managers → geringer Aufwand, deutliche Reduzierung von Passwort-Risiken

4. Rechts- und Compliance-Rahmen: Mindeststandards, keine Kür

4.1 DSGVO – Datenschutz als Pflichtprogramm

Die DSGVO ist seit 2018 wirksam und längst gelebte Realität: Aufsichtsbehörden verhängen regelmäßig spürbare Bußgelder, und zwar auch gegen mittelständische Unternehmen. Reports und Übersichten zeigen, dass die **durchschnittliche Höhe der DSGVO-Strafen seit 2019 deutlich angestiegen ist** – inzwischen im Schnitt im Millionenbereich pro Verstoß (getrieben u. a. durch große Verfahren, aber mit Signalwirkung für alle).

Für die Praxis im Mittelstand bedeutet das:

- **Verzeichnis von Verarbeitungstätigkeiten** ist Pflicht.
- **Technische und organisatorische Maßnahmen (TOM)** müssen dokumentiert und nachweisbar sein.
- **Auftragsverarbeitungsverträge** mit allen IT-Dienstleistern und Cloud-Anbietern sind zwingend.
- **Meldepflicht für Datenpannen** innerhalb von 72 Stunden.

Sicherheit ohne DSGVO-Compliance ist riskant – allein schon wegen Bußgeldern, Haftung und Reputationsschäden.

4.2 NIS2 – Neue Pflichten für viele Mittelständler

Die EU-Richtlinie **NIS2** erweitert den Kreis der regulierten Unternehmen deutlich. In Deutschland werden durch die nationale Umsetzung (NIS2UmsuCG) erstmals auch viele mittelständische Unternehmen als „wichtige“ oder „besonders wichtige Einrichtungen“ eingestuft, z. B. in Bereichen wie Produktion, Energie, Transport, digitale Infrastruktur oder Gesundheitswesen.

Pflichten für betroffene Unternehmen:

- Einführung eines **Informationssicherheits-Managementsystems (ISMS)**
- regelmäßige **Risikobewertungen** und **Sicherheitsmaßnahmen** entlang definierter Anforderungen
- strengere **Meldepflichten** bei Sicherheitsvorfällen
- persönliche Verantwortlichkeit der Unternehmensleitung

Auch Unternehmen, die **formal nicht unter NIS2 fallen**, sollten sich an den dort geforderten Mindeststandards orientieren – sie sind ein sinnvoller Referenzrahmen für professionelles Sicherheitsmanagement.

4.3 Weitere Rahmenwerke

- **ISO/IEC 27001** – international anerkannter Standard für Informationssicherheits-Managementsysteme

- **BSI-IT-Grundschutz** – deutsches Rahmenwerk, das auch für KMU wertvolle Bausteine enthält
- branchenspezifische Standards (z. B. **TISAX** im Automotive-Bereich, **KRITIS-Vorgaben** für kritische Infrastrukturen)

5. Reifegradmodell: Wo steht Ihr Unternehmen?

Ein Reifegradmodell hilft, das aktuelle Sicherheitsniveau einzuschätzen und passende Ziele zu definieren. Angelehnt an das Modell auf eurer IT-Sicherheitsseite lassen sich drei pragmatische Level unterscheiden.

Level 1 – Basis-Schutz (Minimum)

Zielgruppe: Unternehmen mit geringem IT-Reifegrad, hoher Risikobereitschaft, niedriger Abhängigkeit von IT

Typische Maßnahmen:

- Firewall & Antivirus / Endpoint-Security
- regelmäßige Backups (idealerweise offline / offlinekopiert)
- grundlegendes Patch-Management
- Passwortsicherheit + möglichst MFA für zentrale Zugänge
- rudimentäre Zugriffskontrolle
- grundlegende DSGVO-Basis (TOM, Verzeichnis, AV-Verträge)

Ziele:

- Vermeidung der schlimmsten Ausfälle
- Reduktion existenzbedrohender Fälle
- Erfüllung minimaler Anforderungen von Versicherern und Aufsichtsbehörden

Level 2 – Angemessener Schutz (Standard für die meisten Mittelständler)

Zielgruppe: typischer Mittelstand mit relevanter IT-Abhängigkeit, Kundenvorgaben, Lieferkettenanforderungen

Zusätzlich zu Level 1:

- **Endpoint Detection & Response (EDR)**
- **Security-Monitoring und Logging**
- **Phishing-Simulationen und regelmäßige Schulungen**
- **IT-Notfallplan** (inkl. Kommunikationsplan, Entscheidungswege)

- **Desaster-Recovery-Plan** mit RTO/RPO-Zielen
- **vollständige DSGVO- & GoBD-Compliance**

Ziele:

- angemessener Schutz gegen die häufigsten Bedrohungen
- deutliche Reduktion des Ransomware- und Phishing-Risikos
- weitgehende Ausfallsicherheit durch Notfallplanung
- Erfüllung typischer Audit-, Kunden- und Versicherungsanforderungen

Level 3 – Erhöhter Schutz (hochregulierte oder besonders schützenswerte Unternehmen)

Zielgruppe: regulierte Branchen, kritische Infrastrukturen, Unternehmen mit besonders schützenswertem geistigen Eigentum

Zusätzlich zu Level 2:

- **Zero-Trust-Architektur** (strenge Segmentierung, Identitätszentrierung)
- **SIEM mit Threat Intelligence**
- regelmäßige **Penetrationstests und Red-Teaming**
- **Zertifizierungen** (z. B. ISO 27001, TISAX)
- besondere Härtung und Überwachung hochkritischer Assets

Achtung: Für viele Mittelständler ist Level 3 **überdimensioniert** – sinnvoll ist es dort, wo regulatorische Vorgaben, kritische Geschäftsmodelle oder Kundenanforderungen dies verlangen.

6. Die fünf realistischsten Bedrohungen – und wie Sie sich schützen

Angelehnt an die Praxis und die Lageberichte von BSI und ENISA sind für den Mittelstand insbesondere fünf Bedrohungen relevant.

6.1 Phishing & Social Engineering

Schätzungen gehen davon aus, dass rund 80 % erfolgreicher Angriffe mit Phishing oder Social Engineering beginnen.

Typische Szenarien:

- gefälschte Paket- oder Rechnungs-E-Mails mit Schadsoftware
- „CEO-Fraud“ – angebliche Anweisungen der Geschäftsführung zur Überweisung
- Login-Seiten, die Passwörter abgreifen (Credential Harvesting)

Schutzmaßnahmen:

- verpflichtende **Awareness-Schulungen** für alle Mitarbeitenden
- regelmäßige **Phishing-Simulationen**
- durchgängige **Multi-Faktor-Authentifizierung**
- abgestimmtes **E-Mail-Filtering** und DMARC/SPF/DKIM

6.2 Ransomware & Ransomware-as-a-Service (RaaS)

Ransomware bleibt laut BSI und ENISA eine der größten Bedrohungen.BSI+2ENISA+2

Aktuelle Trends:

- **Doppelte Erpressung**: Daten werden vor der Verschlüsselung entwendet, anschließend drohen die Angreifer mit Veröffentlichung.
- **RaaS-Plattformen** senken die Einstiegshürden – Angriffe können quasi „gebucht" werden.

Schutzmaßnahmen:

- **Immutable Backups** (nicht durch Ransomware lösch- oder verschlüsselbar)
- **Netzwerksegmentierung**, damit Angreifer sich nicht frei im Netzwerk bewegen können
- **EDR-Lösungen** und Monitoring
- detaillierte **Notfall- und Wiederanlaufpläne** (inkl. Test-Wiederherstellungen)

6.3 Ungepatchte Schwachstellen

Automatisierte Scans finden weltweit Schwachstellen in exponierten Systemen – oft genügt eine alte VPN-Appliance oder ein nicht aktualisierter Mailserver, damit Angreifer eindringen können. BSI-Berichte zeigen regelmäßig, dass viele erfolgreiche Angriffe auf bekannte, längst gepatchte Lücken zurückgehen.

Schutzmaßnahmen:

- verbindliches **Patch-Management** mit klaren Fristen
- regelmäßige **Vulnerability-Scans**
- Minimierung der **Angriffsfläche** (nur notwendige Dienste ins Internet öffnen)

6.4 Insider-Bedrohungen

Nicht alle Vorfälle sind „böse Hacker":

- versehentliche Datenlecks durch falsche Freigaben
- vorsätzliche Sabotage durch frustrierte Mitarbeitende
- Datendiebstahl kurz vor oder nach Kündigung

Schutzmaßnahmen:

- **Least-Privilege-Prinzip** (jeder nur, was er wirklich braucht)

- sauberer **Joiner-Mover-Leaver-Prozess** (Onboarding, Rollenwechsel, Offboarding)
- Protokollierung und **Monitoring kritischer Zugriffe**

6.5 Supply-Chain-Angriffe

Angriffe über Zulieferer, IT-Dienstleister oder Softwarelieferketten nehmen zu:

- kompromittierte Fernwartungszugänge
- manipulierte Software-Updates
- Schwachstellen bei Cloud- oder SaaS-Anbietern

Schutzmaßnahmen:

- strukturiertes **Vendor-Management**
- Sicherheitsanforderungen und **Vertragspflichten** an Dienstleister
- MFA und Segmentierung für alle externen Zugriffe
- Notfallpläne für den Ausfall kritischer Dienstleister

7. Security vs. Usability: Sicherheit, die nicht nervt

Ein wesentlicher Erfolgsfaktor für Security im Mittelstand ist **Akzeptanz**. Sicherheitsmaßnahmen, die den Arbeitsalltag massiv behindern, werden umgangen – und schaffen so neue Risiken.Fox Romeo IT GmbH

Beispiele für praxistaugliche Lösungen:

- statt komplizierter Passwortregeln → **Passwort-Manager + MFA**
- statt pauschalem Verbot aller Cloud-Dienste → **freigegebene, gemanagte Cloud-Services** mit zentralem Identity-Management
- statt händisch beantragter, langwieriger Freigaben → **rollenbasierte Standardberechtigungen** plus Monitoring

Leitgedanke:

Die sichere Lösung muss **einfacher** sein als die unsichere Alternative.

8. Roadmap: In drei Stufen zu angemessener IT-Sicherheit

8.1 Phase 1 – 0 bis 3 Monate: Akute Risiken entschärfen

- Security-Assessment / Kurzanalyse der aktuellen Lage

- Härtung der wichtigsten externen Zugänge (VPN, M365, RDP) mit MFA
- Sicherstellung valider und getesteter Backups (inkl. Offline-/Immutable-Komponente)
- erste Awareness-Maßnahmen (Kurzschulung, Phishing-Simulation)
- Überprüfung der wichtigsten DSGVO-Basics (TOM, AV-Verträge, Meldeprozesse)

8.2 Phase 2 – 3 bis 12 Monate: Strukturen etablieren

- Einführung eines **einfachen ISMS-Light** (Richtlinien, Rollen, Prozesse)
- Aufbau eines **Logging- und Monitoring-Konzepts**
- regelmäßige Schwachstellenscans und strukturiertes Patch-Management
- formalisierter **IT-Notfallplan** und Durchführung mindestens eines Tests pro Jahr
- Berechtigungs-Review und Einführung von Rollenmodellen

8.3 Phase 3 – 12+ Monate: Professionalisierung und ggf. Zertifizierung

- Ausbau in Richtung Level 2 oder 3 des Reifegradmodells
- ggf. Vorbereitung auf Zertifizierungen (ISO 27001, TISAX etc.)
- vertiefende technische Maßnahmen (Zero Trust, SIEM, Threat Intelligence)
- Verbesserung der Integration mit Lieferanten und Kunden (Security-Anforderungen, Audits)

9. Rolle von Versicherungen, Dienstleistern und Outsourcing

9.1 Cyber-Versicherung: Kein Ersatz für Security

Cyber-Versicherungen können helfen, finanzielle Schäden abzufedern – sie ersetzen aber keine Sicherheitsmaßnahmen. Typischerweise verlangen Versicherer:

- Mindeststandards bei Backup, Patch-Management, MFA
- dokumentierte Prozesse für Incident Response
- regelmäßige Schulungen

Fehlt diese Basis, droht im Schadenfall eine **Leistungskürzung** oder -verweigerung.

9.2 Externe Dienstleister und Managed Security

Viele Mittelständler können kein eigenes, voll besetztes Security-Team aufbauen. Externe Dienstleister sind dann oft der einzige realistische Weg zu professioneller IT-Sicherheit – allerdings nur, wenn:

- Interessenkonflikte (z. B. Produktverkauf vs. Beratung) transparent adressiert werden

- Rollen klar verteilt sind (wer ist für was verantwortlich?)
- Reporting und Kennzahlen verständlich und Management-tauglich sind

10. Checkliste für Geschäftsführung und Vorstand

Zum Abschluss eine kompakte Checkliste – nicht vollständig, aber ein guter Start:

1. **Rolle & Verantwortung**
    - Gibt es einen klar benannten Verantwortlichen für Informationssicherheit?
    - Berichtet dieser regelmäßig an Geschäftsführung / Vorstand?
2. **Risikobild**
    - Liegt eine aktuelle Risikobewertung vor (kritische Systeme, Daten, Prozesse)?
    - Kennen wir unsere wichtigsten Bedrohungsszenarien (Ransomware, Phishing, Ausfall kritischer Systeme)?
3. **Technische Basis**
    - Sind alle externen Zugänge durch MFA geschützt?
    - Haben wir ein funktionierendes Patch-Management mit definierten Fristen?
    - Sind Backups regelmäßig getestet und vor Manipulation geschützt?
4. **Organisation & Prozesse**
    - Existiert ein IT-Notfallplan mit klaren Rollen und Kommunikationswegen?
    - Sind Joiner-Mover-Leaver-Prozesse definiert und dokumentiert?
    - Finden regelmäßige Berechtigungs-Reviews statt?
5. **Menschlicher Faktor**
    - Werden alle Mitarbeitenden mindestens jährlich zu Security-Themen geschult?
    - Setzen wir Phishing-Simulationen ein und werten diese aus?
6. **Compliance & Verträge**
    - Haben wir ein aktuelles Verzeichnis der Verarbeitungstätigkeiten?
    - Sind alle AV-Verträge mit Dienstleistern vorhanden und geprüft?
    - Wissen wir, ob und wie NIS2 uns betrifft – direkt oder indirekt über Kundenanforderungen?
7. **Externe Partner & Lieferkette**
    - Gibt es definierte Sicherheitsanforderungen an unsere wichtigsten Dienstleister?
    - Sind Zugriffe externer Partner klar geregelt, segmentiert und mit MFA abgesichert?

Quellenverzeichnis

- Bundesamt für Sicherheit in der Informationstechnik (BSI). *Die Lage der IT-Sicherheit in Deutschland 2024*. Bericht 2024.
- Bundesamt für Verfassungsschutz
- The ENISA Threat Landscape (ETL) report is the annual report of the European Union Agency for Cybersecurity, ENISA, on the state of the cybersecurity threat landscape.
- BSI – Lageberichte & -bilder. „IT-Sicherheitslage“ auf der BSI-Website.
- Datenschutz-Grundverordnung (DSGVO). Übersichten zu Bußgeldern und rechtlichen Anforderungen. z. B. „DSGVO-Bußgelder erreichen 2023 neues Rekordhoch“ (Statista-Infografik)