WEMACON

IT-WHITEPAPER Q3 2025

INFORMATIONSSICHERHEIT IN KMU
STRATEGIEN, RISIKEN UND LÖSUNGEN

Für ISB, IT-Leiter und Geschäftsführer

Inkl. Expertentipps für KMU

Klar bewerten, sicher schützen:
Dieses Whitepaper liefert Ihnen das notwendige Wissen und praxisnahe Ansätze, um die Informationssicherheit in Ihrem Unternehmen ganzheitlich zu bewerten und gezielt zu stärken. Mit klar strukturierten Checklisten, Risikoanalysen und Entscheidungshilfen gewinnen Sie die nötige Sicherheit, um Bedrohungspotenziale zu erkennen und Ihre Schutzmaßnahmen nachhaltig und zukunftssicher auszurichten.

QUALITÄT,
IT-SICHERHEIT &
DATENSCHUTZ
MADE IN GERMANY

VORWORT

Das aktuelle Whitepaper zur Informationssicherheit 2025 zeigt deutlich: Unternehmen stehen heute mehr denn je unter Druck, ihre digitale Resilienz auszubauen. Cyberangriffe, regulatorische Vorgaben und der zunehmende Fachkräftemangel machen deutlich, dass Informationssicherheit längst kein „IT-Thema“ mehr ist, sondern zu den entscheidenden Erfolgsfaktoren für die Wettbewerbsfähigkeit gehört.

Besonders erfreulich ist, dass immer mehr Unternehmen ihre Sicherheitsstrategie professionalisieren. Der Anteil der Organisationen, die sich als „sicherheitsbewusst und digital fortschrittlich“ bezeichnen, steigt kontinuierlich an. 2020 war das noch eine Minderheit, heute liegt der Wert bereits bei über 80 %. Die Entwicklung verdeutlicht uns: Informationssicherheit ist kein Hemmschuh, sondern Voraussetzung für Digitalisierung, Innovationsfähigkeit und nachhaltiges Wachstum.

In diesem Sinne wünsche ich Ihnen viele neue Impulse und viel Spaß beim Lesen.

Ganz herzlich

Maximilian Weil B.A.
Inhaber WEMACON
Experte für Datenschutz & Informationssicherheit

INHALT

1. MANAGEMENT SUMMARY

Mehr Maßnahmen – aber nicht mehr Sicherheit?

Die Absicherung von IT-Systemen und sensiblen Informationen beansprucht erhebliche Ressourcen – und bleibt dennoch oft unvollständig. Laut dem Microsoft Digital Defense Report 2024 gehen rund 90 % aller erfolgreichen Ransomware-Angriffe auf unzureichend geschützte Endgeräte zurück. Für kleine und mittelständische Unternehmen (KMU) bedeutet das: Der digitale Arbeitsplatz bleibt ein zentrales Einfallstor für Cyberangriffe.

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt regelmäßig vor der zunehmenden Professionalisierung von Angreifern und der besonderen Gefährdungslage für mittelständische Unternehmen. In seinem Lagebericht zur IT-Sicherheit in Deutschland 2024 hebt das BSI hervor, dass insbesondere unzureichend umgesetzte Basismaßnahmen, wie Patchmanagement oder Zugriffsschutz, häufige Schwachstellen darstellen.

Trotz wachsender Investitionen in Security-Lösungen und intensiver Bemühungen um Fachkräfte bleibt bei vielen Unternehmen das ungute Gefühl: Mehr Aufwand bedeutet nicht automatisch mehr Sicherheit.

Kernfrage: Wie lässt sich IT-Sicherheit heute wirtschaftlich, wirksam und gesetzeskonform umsetzen?

Unter zunehmendem Druck – etwa durch das IT-Sicherheitsgesetz, die EU-Richtlinie NIS2, die DSGVO oder branchenspezifische Standards – müssen Geschäftsführende, CIOs und CISOs Strategien entwickeln, die sowohl Schutz als auch Nachweisbarkeit gewährleisten. Dabei wird Informationssicherheit mehr und mehr zur unternehmerischen Pflicht – mit konkreter Haftung für Versäumnisse.

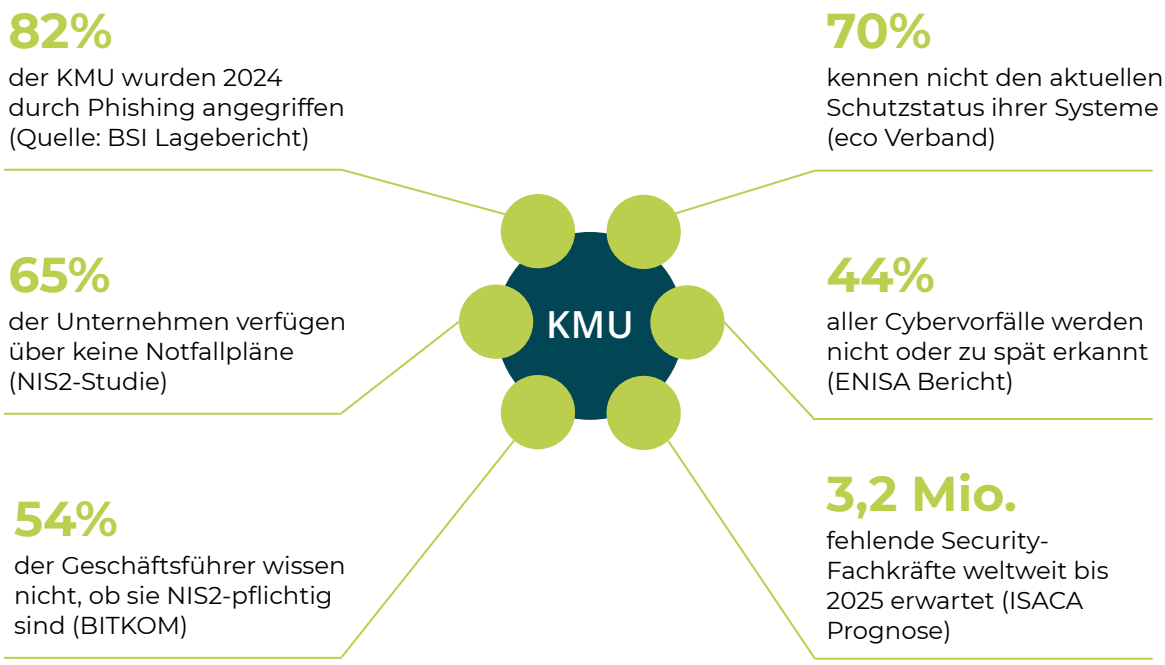
Dieses Whitepaper unterstützt Sie bei der strukturierten Analyse und Strategieentwicklung. Es benennt die wesentlichen Risiken, regulatorischen Anforderungen und Gestaltungsoptionen für eine belastbare Sicherheitsarchitektur im Mittelstand.

2. HERAUSFORDERUNG: INFORMATIONSSICHERHEIT IM MITTELSTAND

Informationssicherheit: Anforderungen & Einflussfaktoren

Viele kleine und mittelständische Unternehmen (KMU) stehen bei der Umsetzung einer wirksamen Informationssicherheit vor zunehmenden Herausforderungen:

Von der Risikobewertung über Zugriffskontrollen, Schwachstellenmanagement und Awareness-Trainings bis hin zu Compliance-Berichten und Nachweisen gegenüber Behörden – der Aufwand ist hoch und wächst kontinuierlich. Laut dem BSI-Lagebericht 2024 haben nur 28 % der KMU ein dokumentiertes Informationssicherheitsmanagement (ISMS) implementiert. Gleichzeitig sehen sich Unternehmen mit neuen regulatorischen Pflichten konfrontiert – wie z. B. durch die NIS2-Richtlinie, das IT-Sicherheitsgesetz 2.0 oder branchenspezifische Compliance-Anforderungen. Hinzu kommt der Mangel an qualifizierten IT-Sicherheitsfachkräften: Laut ISACA fehlen weltweit über 3 Mio. Cybersecurity-Experten – Tendenz steigend.



Unser Tipp:

Informationssicherheit pragmatisch angehen – mit dem BSI IT-Grundschutz-Kompendium
Das BSI IT-Grundschutz-Kompendium bietet eine praxisnahe und stufenweise umsetzbare Orientierung – speziell auch für kleinere Unternehmen. Das Kompendium des Bundesamts für Sicherheit in der Informationstechnik (BSI) enthält über 100 standardisierte Sicherheitsbausteine für typische IT-Systeme, Anwendungen und Prozesse. Es basiert auf national anerkannten Standards (u. a. ISO 27001) und hilft Ihnen, Schutzbedarf, Maßnahmen und Verantwortlichkeiten strukturiert zu erfassen – ohne direkt ein vollständiges ISMS implementieren zu müssen. Starten Sie schlank – und erweitern Sie Ihre Sicherheitsmaßnahmen schrittweise. So schaffen Sie schnell erste Verbesserungen und legen den Grundstein für langfristige Compliance und Resilienz.

3. BEDROHUNGSLAGE 2025 - CYBERRISIKEN IM WANDEL

Was KMU heute bedroht – und was das für die Informationssicherheit bedeutet

Cyberkriminelle agieren längst nicht mehr isoliert oder amateurhaft – sie nutzen skalierbare Angriffsplattformen, KI-gestützte Automatisierung und ausgeklügelte Täuschungsstrategien. Besonders kleine und mittelständische Unternehmen (KMU) gelten als leichtes Ziel, da sie häufig über keine dedizierten Sicherheitsstrukturen oder nur eingeschränkte Ressourcen verfügen.

Laut dem BSI steigen sowohl die Anzahl als auch die Qualität der Angriffe – mit einem starken Fokus auf Endgeräte, E-Mail-Systeme und schlecht abgesicherte Anwendungen. Auch menschliche Faktoren wie ungeschulte Mitarbeitende oder fehlende Awareness tragen wesentlich zum Risiko bei.

4. TYPISCHE GEFAHRENQUELLEN & IHRE AUSWIRKUNGEN

94%

aller Sicherheitsvorfälle beginnen mit menschlichem oder organisatorischem Versagen.

(Quelle: ENISA Threat Landscape Report 2024)

”Die größte Schwachstelle bleibt der Mensch.”

Unternehmen müssen technische Schutzmaßnahmen mit Awareness-Trainings und klaren Prozessen kombinieren, um Sicherheitsvorfälle wirksam zu verhindern.

Gefahrenquelle:	Folgen für KMU:
Ransomware & Phishing (z. B. gefälschte E-Mails, Links, Anhänge)	Systemausfälle, Datenverlust, Erpressung und Reputationsschäden
Schwachstellen in Drittsoftware (nicht gepatchte Tools, Plugins, SaaS)	Unkontrollierter Zugriff auf interne Systeme durch externe Angriffsvektoren
Fehlkonfigurationen (Shadow IT) (nicht autorisierte Geräte oder Dienste)	Sicherheitslücken durch unüberwachte Systeme, keine zentrale Kontrolle
Menschliche Fehler (unzureichende Schulung, unsichere Passwörter, Social Engineering)	Unbeabsichtigte Datenlecks, Missbrauch von Zugängen, Nichteinhaltung von Compliance-Anforderungen

5. BAUSTEINE EINER ROBUSTEN INFORMATIONSSICHERHEITSSTRATEGIE

Informationssicherheit ganzheitlich denken – technisch, organisatorisch und menschlich

Eine moderne Sicherheitsstrategie ist mehr als nur ein Antivirenprogramm. Sie beruht auf mehreren, sich ergänzenden Säulen – und muss regelmäßig überprüft, angepasst und weiterentwickelt werden. Gerade in KMU ist es wichtig, pragmatisch zu starten, ohne dabei die Gesamtverantwortung aus den Augen zu verlieren.

Grundlage schaffen: Die vier Säulen der Informationssicherheit

1. Technische Maßnahmen

Eine moderne Sicherheitsarchitektur beginnt bei der Technik: Firewall, Virenschutz, Patchmanagement, Endpoint Protection und Netzwerksegmentierung bilden die technische Basis. Ergänzend sorgen SIEM-Systeme oder EDR-Lösungen für Transparenz über Angriffe.

2. Organisatorische Maßnahmen

Ohne klare Regeln bleibt Sicherheit ein Zufallsprodukt. Ein ISMS nach ISO/IEC 27001, Rollenverteilung, Dokumentation und Notfallmanagement helfen, Prozesse sicher und nachvollziehbar zu gestalten – intern wie extern.

3. Menschliche Komponente

Ob Phishing, Social Engineering oder Fehlbedienung – Menschen bleiben das größte Risiko. Regelmäßige Awareness-Trainings, klare IT-Richtlinien und simulierte Angriffe erhöhen das Sicherheitsbewusstsein im Alltag.

4. Kontinuierliche Verbesserung

Cybersicherheit ist kein Einmalprojekt. Regelmäßige Audits, Penetrationstests und ein aktives Schwachstellenmanagement helfen, Sicherheitslücken frühzeitig zu erkennen und die Abwehr permanent zu verbessern.

Unser Tipp:

Fangen Sie pragmatisch an – mit den Top 5 CIS Controls.
Gerade KMU profitieren von einem fokussierten Einstieg in die Sicherheitsarbeit. Die ersten fünf CIS Controls bieten einen konkreten, praxiserprobten Ansatz – z. B. für die Geräte- und Software-Inventarisierung, Zugriffskontrollen und Schwachstellenbeseitigung. So schaffen Sie mit überschaubarem Aufwand ein belastbares Sicherheitsfundament.

OUTSOURCING, TOOLS ODER INHOUSE?

6. STRATEGIEN FÜR KMU

Wir helfen Unternehmen, die richtige Kombination für ein belastbares Sicherheitsniveau zu finden – effizient, skalierbar und praxistauglich

- **01. Managed Services & externe Partner**

  Ob MSSP oder SOCaaS: Dienstleister übernehmen die kontinuierliche Überwachung, Analyse und Reaktion auf Sicherheitsvorfälle. Ideal bei Personalmangel oder fehlendem Know-how.

- **02. Inhouse oder Hybridlösungen**

  Unternehmen mit eigenem IT-Team können Tools wie SIEM, EDR oder Schwachstellenmanagement intern betreiben – ggf. unterstützt durch externe Spezialisten oder Berater.

Nicht jede Organisation benötigt ein eigenes Security Operations Center – aber jedes Unternehmen braucht ein funktionierendes Sicherheitskonzept.
Die Wahl der richtigen Lösung hängt von Budget, IT-Reifegrad, Fachkräften und Compliance-Anforderungen ab.

Managed Security Services (MSSP) bieten einen schnellen Einstieg ohne große Vorlaufzeit. SOC-as-a-Service geht noch weiter: Hier übernehmen externe Experten auch die Analyse und Reaktion auf Vorfälle in Echtzeit. Für KMU, die intern Know-how aufbauen möchten, sind Hybridmodelle mit Tool-gestützter Eigenverantwortung sinnvoll – z. B. kombiniert mit regelmäßigen Audits und externer Beratung.
Wichtig ist: Es gibt nicht die eine Lösung – sondern nur die passende Kombination aus interner Verantwortung und externer Unterstützung.

Unser Tipp für Entscheider:
Beginnen Sie mit einer klaren Bestandsaufnahme: Welche Systeme haben wir? Wer ist verantwortlich? Welche Risiken bestehen konkret? Erst mit dieser Basis lässt sich entscheiden, ob Inhouse, Tools oder externe Partner die richtige Wahl sind.

7. PRO & CONTRA TYPISCHER SICHERHEITSANSÄTZE

Die richtige Strategie für Ihre IT-Sicherheit – was wirklich passt

Cyberbedrohungen treffen Unternehmen auf unterschiedlichste Weise – ebenso vielfältig sind die Schutzmaßnahmen. Doch nicht jedes Modell passt zu jedem Unternehmen. Entscheidend sind die individuellen Rahmenbedingungen: IT-Reifegrad, Ressourcenverfügbarkeit, rechtliche Anforderungen und nicht zuletzt das eigene Risikoprofil.

Die nachfolgende Übersicht zeigt, welche gängigen Ansätze KMU typischerweise wählen – und welche Stärken und Schwächen sie mitbringen:

Ansatz	Vorteile	Herausforderungen
MSSP (Managed Security Services Provider)	✓ 24/7-Monitoring durch externe Experten ✓ Keine eigene Security-Infrastruktur notwendig	✗ Abhängigkeit vom Anbieter ✗ Eingeschränkte Einflussmöglichkeiten
Interne Lösung	✓ Volle Kontrolle über Prozesse & Daten ✓ Langfristiger Know-how-Aufbau	✗ Hoher Personalbedarf & Fachkräftemangel ✗ Höhere Kosten für Betrieb & Weiterbildung
Security-Tools (EDR, SIEM, Patch-Management etc.)	✓ Schnelle Implementierung ✓ Hohe Skalierbarkeit & Automatisierung	✗ Technisch isolierte Lösung ohne Prozessanbindung ✗ Eingeschränkte Wirksamkeit ohne zentrale Steuerung
Hybridmodell (z. B. Toolbetrieb intern, MSSP für Monitoring)	✓ Flexible Kombination aus Eigenleistung & externer Expertise ✓ Gute Balance zwischen Kontrolle und Effizienz	✗ Erhöhter Koordinationsaufwand ✗ Klare Rollendefinitionen nötig

8. CHECKLISTE ZUR STRATEGISCHEN ENTSCHEIDUNGSFINDUNG

1. Analyse des Ist-Zustands
- Haben wir eine aktuelle Risikobewertung durchgeführt?
- Wie erfassen und melden wir Schwachstellen in Systemen oder Prozessen?
- Gibt es eine definierte Datenklassifikation (z. B. öffentlich, intern, vertraulich)?

2. Zielformulierung
- Welche Sicherheitsziele verfolgen wir kurz-, mittel- und langfristig?
- Welche gesetzlichen/regulatorischen Vorgaben (z. B. NIS2, DSGVO) betreffen uns?
- Wie fügen sich diese Maßnahmen in unsere Digitalstrategie ein?

3. Ressourcenbewertung
- Haben wir ausreichend Fachpersonal, Tools und Budget zur Verfügung?
- Gibt es Erfahrungen mit Dienstleistern (positiv/negativ)?
- Welche Tools oder Prozesse sind intern sinnvoll umsetzbar, welche nicht?

4. Entscheidungsmatrix
- Welche Risiken tragen wir aktuell bewusst oder unbewusst?
- Wo liegt der größte Hebel zur Verbesserung – intern oder extern?
- Welche Maßnahme ist strategisch sinnvoll, auch im Hinblick auf Skalierbarkeit und Zukunftsfähigkeit?

Unser Tipp:

Sicherheit beginnt mit Transparenz.
Ein ehrlicher Blick auf den Status quo, kombiniert mit realistischen Zielbildern, ist der Schlüssel zu jeder funktionierenden Sicherheitsstrategie. Nutzen Sie diese Checkliste regelmäßig – nicht nur vor Investitionen, sondern auch zur Fortschrittskontrolle.

9. AUSBLICK: NÄCHSTE SCHRITTE ZUR SICHERHEITSOPTIMIERUNG

Informationssicherheit ist kein Projekt mit Enddatum – sondern ein kontinuierlicher Prozess, der mit der richtigen Strategie zum echten Wettbewerbsvorteil wird. Unternehmen, die ihre Sicherheitsmaßnahmen systematisch aufbauen, gewinnen nicht nur Resilienz gegen Cyberbedrohungen, sondern erfüllen auch steigende regulatorische Anforderungen und stärken das Vertrauen von Kunden, Partnern und Mitarbeitenden.
Der Einstieg muss dabei nicht kompliziert sein: Schon mit einer einfachen Standortbestimmung lassen sich erste Handlungsfelder identifizieren und priorisieren.

Empfohlene nächste Schritte:

1. Durchführung eines Risk Assessments

Erfassen Sie systematisch Ihre IT-Risiken, Schwachstellen und Sicherheitslücken – und gewinnen Sie ein realistisches Bild Ihrer aktuellen Bedrohungslage.

2. ISMS-Kurz-Audit oder Selbstbewertung starten

Prüfen Sie, inwieweit Ihre Organisation bereits grundlegende Anforderungen an Informationssicherheit erfüllt – z. B. entlang der ISO/IEC 27001 oder der BSI-Standards.

3. Einführung der DIN SPEC 27076 als Einstieg in die Sicherheitsstruktur

Die DIN SPEC 27076 ist speziell auf KMU ausgerichtet und bietet ein niederschwelliges, klar strukturiertes Vorgehen zur Verbesserung der Informationssicherheit – ohne übermäßigen Aufwand oder Bürokratie.

4. Ableitung & Umsetzung konkreter Maßnahmen

Setzen Sie auf Quick-Wins bei besonders risikobehafteten Bereichen (z. B. Zugriffsmanagement, E-Mail-Sicherheit, Backup-Strategien) – intern oder mit externer Unterstützung.

Unser Tipp:

Die DIN SPEC 27076 ist ideal für den Mittelstand.
Sie ermöglicht einen pragmatischen Einstieg in das Thema Informationssicherheit – und ist gleichzeitig anschlussfähig an internationale Standards wie die ISO/IEC 27001. Besonders für Unternehmen ohne eigene Security-Abteilung ist sie ein wertvoller Leitfaden.

WEMACON

IT-WHITEPAPER Q3 2025

SO KÖNNEN WIR SIE UNTERSTÜTZEN

Ihre Informationssicherheit verdient einen klaren Plan – wir begleiten Sie auf diesem Weg

WEMACON, Inh. Maximilian Weil
Eschberger Weg 19
66121 Saarbrücken

Telefon: (+49) 0681 38 75 42 80
E-Mail: info@wemacon.de
Web: www.wemacon.de

Mit unserer Erfahrung aus zahlreichen Kundenprojekten im Mittelstand bieten wir Ihnen:

Analyse & Standortbestimmung
Schnelles Risk Assessment oder ISMS-Kurzcheck auf Basis von BSI und DIN SPEC 27076

Maßnahmenentwicklung & Umsetzung
Unterstützung bei konkreten Sicherheitsmaßnahmen – intern oder mit externen Partnern

Beratung zu Strategie, Tools & Dienstleistern
Unabhängige Empfehlungen zur Wahl zwischen MSSP, Inhouse, Hybrid oder Tool-gestützter Lösung

Workshops & Awareness-Trainings
Für Führungskräfte und Teams – gezielt auf Ihr Unternehmen abgestimmt