

WHITEPAPER · IT-SICHERHEIT

IT-Grundschutz für KMU – Praktischer Einstieg

Wie kleine und mittlere Unternehmen BSI IT-Grundschutz und CIS Controls in einen umsetzbaren 90-Tage-Plan übersetzen.

DAS ERHALTEN SIE

- Einordnung: BSI IT-Grundschutz, CIS Controls, NIS2
- Die acht Basismaßnahmen mit dem größten Effekt
- Priorisierungsmatrix nach Wirkung und Aufwand
- 30/60/90-Tage-Plan und Prüfcheckliste

AUF EINEN BLICK

Für	**Unternehmen mit 5–50 Mitarbeitenden**
Zeitbedarf	**ca. 2 Stunden Lesen & Bewerten**
Stand	**16. November 2026**
Version	**2.0**

Unverbindliche Praxishilfe – keine Rechtsberatung, kein Audit

1 Worum es geht

> IT-Sicherheit ist kein Produkt und kein einmaliges Projekt, sondern ein wiederholbarer Ablauf: Transparenz schaffen, Risiken priorisieren, Maßnahmen umsetzen, Wirksamkeit prüfen.

Kleine und mittlere Unternehmen haben selten eine eigene Sicherheitsabteilung. Gleichzeitig zielen die meisten Angriffe nicht auf Spezialwissen, sondern auf bekannte Lücken: fehlende Mehr-Faktor-Authentisierung, ungepatchte Systeme, zu weit gefasste Administratorrechte und Backups, die im Ernstfall nicht wiederherstellbar sind. Dieser Leitfaden konzentriert sich deshalb auf Maßnahmen mit hoher Wirkung und überschaubarem Aufwand.

Welches Rahmenwerk passt?

Rahmenwerk	Charakter	Geeignet, wenn …
BSI IT-Grundschutz (BSI-Standards 200-1 bis 200-4, IT-Grundschutz-Kompendium)	Umfassende deutsche Methodik mit Bausteinen und Anforderungen; Vorgehensweisen Basis-, Standard- und Kern-Absicherung	… Sie strukturiert nach deutschem Standard vorgehen oder später eine Zertifizierung (ISO 27001 auf Basis von IT-Grundschutz) erwägen
CIS Controls (Implementation Group 1)	Priorisierte, technische Maßnahmenliste; IG1 beschreibt eine grundlegende „Cyber-Hygiene“	… Sie schnell mit einer kompakten, technisch konkreten Liste starten möchten
ISO/IEC 27001	Internationale Norm für ein Informationssicherheits-Managementsystem (ISMS)	… Kunden oder Lieferketten einen formalen Nachweis verlangen

Die Rahmenwerke schließen sich nicht aus. Ein pragmatischer Weg für KMU: mit den Basismaßnahmen dieses Leitfadens beginnen, sie an der **Basis-Absicherung** des BSI oder an **CIS IG1** spiegeln und später gezielt vertiefen.

Betrifft Sie NIS2?
Mit dem deutschen NIS2-Umsetzungsgesetz gelten Cybersicherheitspflichten (Risikomanagement, Meldepflichten, Registrierung beim BSI, Verantwortung der Geschäftsleitung) für deutlich mehr Unternehmen – in bestimmten Sektoren in der Regel ab 50 Beschäftigten oder mehr als 10 Mio. € Jahresumsatz und Bilanzsumme. Prüfen Sie Ihre Betroffenheit, z. B. mit der NIS-2-Betroffenheitsprüfung des BSI. Auch nicht direkt betroffene Unternehmen spüren NIS2 häufig als Anforderung ihrer Kunden in der Lieferkette.

2 Ausgangslage: Schutzbedarf und Bestand

Sicherheit beginnt mit der Frage, was geschützt werden muss. Gehen Sie von den Geschäftsprozessen aus – nicht von der Technik.

Schritt	Leitfrage	Ergebnis
1. Prozesse benennen	Welche Abläufe halten das Unternehmen am Laufen (Auftragsannahme, Buchhaltung, Produktion, Kundenservice)?	Liste der 5–10 kritischen Prozesse

Schritt	Leitfrage	Ergebnis
2. Schutzbedarf einschätzen	Was passiert bei Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit? Wie lange ist ein Ausfall tragbar?	Kategorie **normal / hoch / sehr hoch** je Prozess
3. Bestand erfassen	Welche Server, Clients, Netzwerkgeräte, Cloud-Dienste, Konten und Dienstleister stützen diese Prozesse?	Asset-Inventar mit Eigentümer und Kritikalität
4. Abhängigkeiten zeichnen	Was fällt mit, wenn Identität, Internet, DNS oder ein zentraler Server ausfällt?	Einfache Abhängigkeitsskizze

Minimal-Inventar – diese Felder genügen für den Start

- Bezeichnung, Typ (Server, Client, Netzwerk, Cloud-Dienst, Konto) und Standort bzw. Anbieter
- Verantwortliche Person (fachlich und technisch)
- Unterstützte Geschäftsprozesse und Schutzbedarf
- Betriebssystem/Version, Support-Ende und Patch-Verantwortung
- Erreichbarkeit aus dem Internet (ja/nein) und administrative Zugänge

Typische blinde Flecken

Private oder „vergessene" Geräte im Netz, alte Administrator- und Dienstkonten, Fernwartungszugänge von Dienstleistern, Cloud-Dienste, die eine Abteilung selbst gebucht hat, sowie Netzwerkgeräte, deren Firmware nie aktualisiert wurde.

3 Die acht Basismaßnahmen

Die folgenden Maßnahmen decken die häufigsten Angriffswege ab. Sie orientieren sich an der Basis-Absicherung des BSI und an CIS IG1.

1 · Identitäten & MFA

- MFA für E-Mail, Fernzugriff, Cloud-Dienste und alle Admin-Zugänge
- Getrennte Admin-Konten, keine Admin-Rechte im Alltag
- Konten beim Austritt sofort deaktivieren

2 · Patch-Management

- Feste Wartungsfenster für OS, Anwendungen, Firmware
- Internet-exponierte und aktiv ausgenutzte Lücken zuerst
- Systeme ohne Herstellersupport ersetzen oder isolieren

3 · Härtung

- Standardpasswörter ändern, unnötige Dienste abschalten
- Makros aus dem Internet blockieren
- Lokale Admin-Passwörter je Gerät verschieden (z. B. Windows LAPS)

4 · Endgeräteschutz

- Aktueller Malware-Schutz mit zentraler Übersicht
- Festplattenverschlüsselung auf Notebooks
- Bildschirmsperre und Geräteverwaltung

5 · Netzwerk

- Zonen für Clients, Server, Management, Gäste, IoT
- Firewall nach dem Prinzip „standardmäßig verweigern“
- Keine offenen Fernwartungsports (RDP/SMB) im Internet

6 · Backup & Wiederherstellung

- 3-2-1 mit mindestens einer offline/unveränderbaren Kopie
- Backup-Zugänge getrennt von der Domäne
- Regelmäßige, dokumentierte Restore-Tests

7 · Awareness

- Kurze, regelmäßige Schulungen statt Einmal-Termin
- Klarer Meldeweg für verdächtige E-Mails
- Kultur: Melden wird nie bestraft

8 · Notfallplan

- Rollen, Kontakte und Erstmaßnahmen offline verfügbar
- Wiederanlauf-Reihenfolge festgelegt
- Mindestens jährlich üben (Tabletop)

Ergänzend: zentrale Protokollierung der wichtigsten Systeme (Anmeldungen, Admin-Aktionen, Firewall) mit ausreichender Aufbewahrungsdauer – ohne Protokolle lässt sich ein Vorfall kaum aufklären.

4 Priorisierungsmatrix

Nicht alles gleichzeitig: Bewerten Sie jede offene Maßnahme nach **Risikoreduktion** und **Aufwand**. Die Einstufung unten ist ein typischer Ausgangspunkt für KMU und muss an Ihre Umgebung angepasst werden.

Maßnahme	Risikoreduktion	Aufwand	Priorität
MFA für E-Mail, Fernzugriff und Admins	sehr hoch	gering	**A – sofort**
Offene RDP/SMB-Ports im Internet schließen	sehr hoch	gering	**A – sofort**
Offline/unveränderbare Backup-Kopie + Restore-Test	sehr hoch	mittel	**A – sofort**
Getrennte Admin-Konten, Rechte bereinigen	hoch	gering	**A – sofort**
Patch-Prozess mit Wartungsfenster	hoch	mittel	**B – 60 Tage**
Netzwerksegmentierung (Gäste, IoT, Server)	hoch	mittel–hoch	**B – 60 Tage**
Festplattenverschlüsselung Notebooks	mittel	gering	**B – 60 Tage**
Zentrale Protokollierung	mittel	mittel	**C – 90 Tage**
Awareness-Programm und Meldeweg	mittel–hoch	gering	**C – 90 Tage**
Notfallübung (Tabletop)	mittel	gering	**C – 90 Tage**

Faustregel

Priorität A sind Maßnahmen, die einen häufigen Angriffsweg mit wenig Aufwand schließen. Dokumentieren Sie bewusst akzeptierte Restrisiken mit Begründung, Verantwortlichem und Ablaufdatum.

5 30/60/90-Tage-Plan

Zeitraum	Ziele	Nachweis
Tag 1–30 Transparenz & Sofortmaßnahmen	Kritische Prozesse und Inventar erfassen · MFA-Lücken schließen · Admin-Konten trennen · offene Fernzugänge schließen · Backup-Status prüfen	Inventarliste, MFA-Report, Liste der Admin-Konten, Restore-Protokoll
Tag 31–60 Grundlagen festigen	Patch-Prozess mit Wartungsfenster · Netzwerkzonen planen und erste Trennung (Gäste/IoT) · Verschlüsselung Notebooks · Ausnahmen mit Ablaufdatum dokumentieren	Patch-Kalender, Netzwerkplan, Ausnahmeliste
Tag 61–90 Wirksamkeit & Routine	Zentrale Protokollierung · Awareness-Start · Tabletop-Übung zum Notfallplan · Restrisiken bewerten · Plan für das nächste Quartal freigeben	Übungsprotokoll, Risikoliste, freigegebener Maßnahmenplan

Danach: Quartalsweise Überprüfung von Konten, Patch-Stand, Firewall-Regeln und Restore-Tests; jährliche Überprüfung von Schutzbedarf, Dienstleistern und Notfallplan.

Entscheidungsnotiz

Geltungsbereich _____

Verantwortlich (Geschäftsleitung) _____

Technische Umsetzung _____

Gewähltes Rahmenwerk _____

Nächste Überprüfung _____

6 Prüfcheckliste

Markieren Sie einen Punkt erst als erledigt, wenn ein nachvollziehbarer Nachweis vorliegt.

	Prüfpunkt	Verantwortlich	Termin / Nachweis
ORGANISATION			
☐	Kritische Prozesse und Schutzbedarf sind dokumentiert.	_____	_____
☐	Asset-Inventar hat Eigentümer und Kritikalität.	_____	_____
☐	NIS2-Betroffenheit ist geprüft und dokumentiert.	_____	_____
☐	Maßnahmen haben Verantwortliche und Termine.	_____	_____
TECHNIK			
☐	MFA ist für privilegierte, externe und Cloud-Zugriffe aktiv.	_____	_____
☐	Admin-Konten sind getrennt und nachvollziehbar.	_____	_____
☐	Patch-Prozess und Ausnahmefreigaben sind dokumentiert.	_____	_____
☐	Keine Fernwartungsports offen im Internet.	_____	_____
☐	Netzwerkzonen und Firewall-Regeln sind überprüft.	_____	_____
☐	Notebooks sind verschlüsselt.	_____	_____
WIEDERHERSTELLUNG & MENSCHEN			
☐	Backups sind getrennt/unveränderbar und Restore-getestet.	_____	_____
☐	Meldeweg für verdächtige E-Mails ist bekannt.	_____	_____
☐	Notfallkontakte sind aktuell und offline verfügbar.	_____	_____

Quellen & weiterführende Referenzen

- BSI: IT-Grundschutz – BSI-Standards 200-1, 200-2, 200-3 und 200-4 sowie IT-Grundschutz-Kompendium, bsi.bund.de
- BSI: NIS-2-Betroffenheitsprüfung und Informationen zum NIS2-Umsetzungsgesetz, bsi.bund.de
- Center for Internet Security: CIS Critical Security Controls v8.1, Implementation Group 1, cisecurity.org
- ISO/IEC 27001:2022 – Informationssicherheits-Managementsysteme
- KONTORIT Wissen: „IT-Notfallplan“, „Backup-Strategie 3-2-1“ und „Netzwerk-Design“ (kontorit.de/whitepaper)

Unterstützung gewünscht? KONTORIT begleitet kleine und mittlere Unternehmen in Hamburg bei Bestandsaufnahme, Umsetzung und Betrieb. Anfrage: **kontorit.de/kontakt** · E-Mail: **support@kontorit.de**

Dieses Dokument ist eine allgemeine, unverbindliche Orientierungshilfe. Es ersetzt keine individuelle Beratung, kein Sicherheitsaudit, keine Rechts- oder Steuerberatung und keinen Zertifizierungsnachweis. Produktfunktionen, Lizenzen und rechtliche Anforderungen ändern sich; prüfen Sie den aktuellen Stand anhand der genannten Quellen und Ihrer konkreten Umgebung. Genannte Marken gehören ihren jeweiligen Inhabern. © 2026 KONTORIT · Stand 16. November 2026 · Version 2.0