IT-SICHERHEIT IM KLEINEN MITTELSTAND DER REGION WESER-EMS

Befunde aus 30 IT-Basisschutz-Erstbegehungen bei Betrieben mit 5 bis 25 Arbeitsplätzen. Erhebungszeitraum Januar 2024 bis Dezember 2025, eingeordnet in die Studienlage von BSI, Bitkom, GDV, Sophos und Verizon nach dem Stand Juli 2026.

83 %	**77 %**	**73 %**	**27/30**
25 VON 30 OHNE SCHRIFTLICHEN IT-NOTFALLPLAN	23 VON 30 IM IST-ZUSTAND NICHT VERSICHERBAR	22 VON 30 OHNE DOKUMENTIERTEN RESTORE-TEST	BETRIEBE MIT DREI ODER MEHR KRITISCHEN BEFUNDEN

HERAUSGEBER

Lisser IT-Systemhaus · Patrick Lisser
Auf der Nordheide 12, 27798 Hude
info@lisser-it.de · Tel. 04408-9999999

Alle in diesem Report zitierten Fremdstudien sind mit Erhebungsjahr, Stichprobe und Quellenangabe im Quellenverzeichnis nachgewiesen. Wo eine Studie größere Unternehmen befragt als die hier untersuchten, ist der Bezugsrahmen im Text genannt.

VORWORT

Cyberangriffe sind in der breiten Wahrnehmung deutscher Unternehmen angekommen. Die jährlichen Lageberichte des Bundesamts für Sicherheit in der Informationstechnik (BSI), die Wirtschaftsschutzstudien des Branchenverbands Bitkom und das Allianz Risk Barometer kommen seit Jahren zu konsistenten Befunden: Cybervorfälle sind das größte Geschäftsrisiko in Deutschland, der wirtschaftliche Schaden steigt, und kleine Unternehmen sind überproportional häufig betroffen. Laut Bitkom-Wirtschaftsschutzstudie 2025 waren 87 Prozent der befragten Unternehmen in den vorangegangenen zwölf Monaten von Datendiebstahl, Spionage oder Sabotage betroffen (Vorjahr: 81 Prozent), der Gesamtschaden für die deutsche Wirtschaft wird auf 289,2 Mrd. € beziffert — davon 202,4 Mrd. € durch Cyberangriffe.

Was in diesen Studien fehlt, ist die Perspektive der wirklich kleinen Betriebe. Die meisten Erhebungen beginnen bei Unternehmen ab zehn Beschäftigten und einem Jahresumsatz von mindestens einer Million Euro; die Sophos-Studien zur Ransomware-Lage berücksichtigen ausschließlich Organisationen ab einhundert Mitarbeitenden. Die Realität in der Region Weser-Ems sieht anders aus. Handwerksbetriebe, Steuerkanzleien, Arztpraxen, Ingenieurbüros, Speditionen oder Maschinenbau-Zulieferer mit 5 bis 25 Arbeitsplätzen sind das Rückgrat der regionalen Wirtschaft. Sie tauchen in der amtlichen Statistik selten auf und werden in Branchenstudien selten gezielt befragt.

Der vorliegende Report schließt diese Lücke punktuell. Er fasst Befunde aus 30 IT-Basisschutz-Erstbegehungen zusammen, die Lisser IT-Systemhaus zwischen Januar 2024 und Dezember 2025 bei Kleinunternehmen im Raum Oldenburg, Bremen und Weser-Ems durchgeführt hat, und ordnet sie in den Kontext der aktuellen Studien von BSI, Bitkom, GDV, Sophos und Verizon ein.

Der Bericht versteht sich als sachlicher Beitrag zur Lagebeurteilung, nicht als Werbeschrift. Er richtet sich an Inhaber und Geschäftsführungen kleiner Unternehmen sowie an deren Steuerberater, Versicherungsmakler, Kammervertreter und Wirtschaftsverbände, die in der Beratung dieser Betriebe eine Multiplikatorrolle einnehmen.

Patrick Lisser

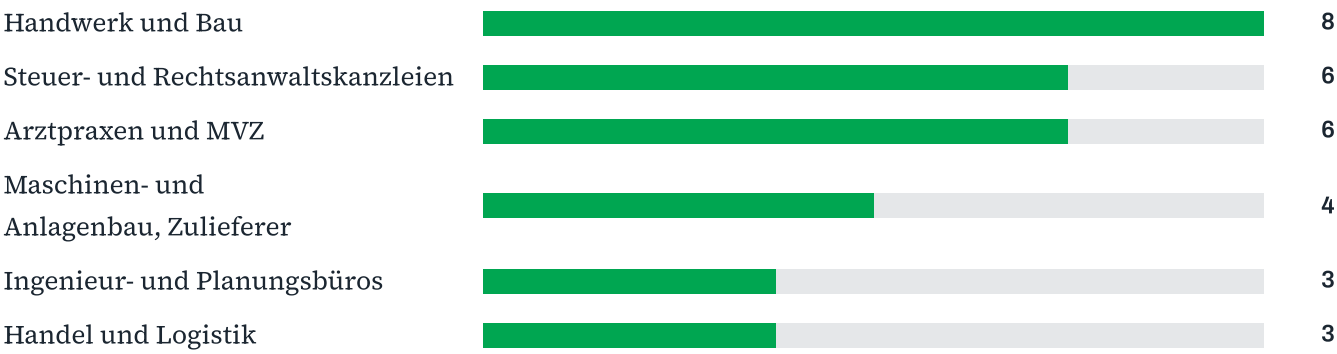
Inhaber, Lisser IT-Systemhaus

1 METHODIK

1.1 UNTERSUCHUNGSGEGENSTAND

Der Erhebung liegt eine Anlassstichprobe von 30 Erstbegehungen zugrunde, die Lisser IT-Systemhaus zwischen dem 1. Januar 2024 und dem 31. Dezember 2025 als IT-Basisschutz-Audit bei Unternehmen mit 5 bis 25 Arbeitsplätzen durchgeführt hat. Sämtliche Unternehmen sind ansässig in den Landkreisen Oldenburg, Wesermarsch, Ammerland, Cloppenburg, Vechta und Friesland sowie in den Städten Oldenburg, Bremen und Delmenhorst. Erfasst sind ausschließlich Erstbegehungen, also Audits vor Beginn einer Betreuung, um eine Verzerrung durch bereits umgesetzte Maßnahmen auszuschließen.

BRANCHENVERTEILUNG DER STICHPROBE (N = 30)



1.2 VORGEHEN

Das Audit orientiert sich an der **DIN SPEC 27076** „IT-Sicherheitsberatung für Klein- und Kleinstunternehmen“, veröffentlicht im Mai 2023 durch das Deutsche Institut für Normung im Konsortium mit BSI und Bundesverband mittelständische Wirtschaft. Sie ist der zurzeit einzige standardisierte Beratungs- und Prüfprozess in Deutschland, der speziell für Unternehmen mit bis zu 50 Beschäftigten entwickelt wurde, und umfasst 27 Anforderungen in sechs Themenbereichen, die in einem strukturierten Interview von ein bis zwei Stunden geprüft werden: Organisation und Sensibilisierung, Identitäts- und Berechtigungsmanagement, Datensicherung, Patch- und Änderungsmanagement, Schutz vor Schadprogrammen sowie IT-Systeme und Netzwerke.

Lisser IT-Systemhaus hat das Verfahren um eine technische Begehung ergänzt. In jedem Audit wurden zusätzlich erfasst:

- Bestandsaufnahme der Endgeräte (Workstations, Server, Notebooks, mobile Geräte) inklusive Alter und Betriebssystemstand;
- Konfiguration der Firewall, Prüfung offener Ports von außen;
- stichprobenartige Wiederherstellung aus dem aktuellen Backup;

- Prüfung der Berechtigungen im Active Directory beziehungsweise Microsoft 365 (verwaiste Konten, ausgeschiedene Mitarbeitende, Administrationsrechte);
- Sichtung der Verträge zur Auftragsverarbeitung gemäß Artikel 28 DSGVO;
- Sichtung vorhandener Dokumentation (Netzwerkplan, Passwortrichtlinie, Notfallplan, Verzeichnis von Verarbeitungstätigkeiten).

Jedes Audit wurde nach demselben Schema in einem schriftlichen Ergebnisbericht dokumentiert. Die Daten für den vorliegenden Report wurden aus diesen Berichten extrahiert und anonymisiert. Personenbezogene Daten der Unternehmen, ihrer Inhaber oder Mitarbeitenden werden nicht offengelegt.

1.3 LIMITATIONEN

Die Stichprobe ist eine Anlassstichprobe, kein Zufallssample: Die untersuchten Unternehmen haben sich aus eigenem Antrieb für ein Audit entschieden. Das spricht für ein überdurchschnittliches Problembewusstsein. Tatsächlich dürfte die Lage bei Unternehmen, die kein Audit beauftragen, schlechter sein, nicht besser. Die hier berichteten Befunde sind insofern als *untere Schranke* der Versäumnisse zu lesen, nicht als statistisch repräsentativer Querschnitt.

Die Fallzahl von 30 Unternehmen erlaubt keine belastbaren Subgruppen-Analysen nach Branche oder Größenklasse. Anteilswerte sind daher auf volle Prozentpunkte gerundet und mit absoluten Häufigkeiten angegeben. Die Befunde werden, wo möglich, mit den großen Erhebungen von BSI, Bitkom, GDV, Sophos und Verizon abgeglichen; deren Bezugsgruppen sind jeweils genannt, weil sie fast immer größere Unternehmen erfassen als die hier untersuchten.

2 KERNBEFUNDE IM ÜBERBLICK

Die Tabelle fasst die zwölf wichtigsten Befunde zusammen. Die Spalte „Lisser IT Stichprobe“ gibt den Anteil der 30 untersuchten Unternehmen wieder, bei denen der genannte Mangel vorlag. Die Spalte „Vergleichswert“ verweist auf eine größere Erhebung mit ähnlichem Gegenstand — mit dem Vorbehalt, dass diese in der Regel größere Unternehmen befragt.

THEMENFELD	BEFUND	LISSER IT STICHPROBE	VERGLEICHSWERT
Backup	Kein dokumentierter Wiederherstellungstest in den letzten zwölf Monaten	**22 von 30 · 73 %**	Sophos 2024 (global): bei 94 % der Ransomware-Opfer Angriffe auf die Backups, in 63 % erfolgreich
Backup	Backups ausschließlich online und in derselben Domäne erreichbar	**17 von 30 · 57 %**	—
MFA	MFA nicht für alle externen Zugänge aktiv (VPN, RDP, M365-Administration)	**21 von 30 · 70 %**	Baobab 2026: 53 % der Betriebe unter 5 Mio. € Umsatz ohne MFA
Patch-Management	Kein dokumentierter Patch-Prozess für Server, Clients und Netzwerkgeräte	**19 von 30 · 63 %**	GDV/forsa: 69 % der befragten Mittelständler erfüllen nicht alle Basisanforderungen
Endpoint	Veraltete oder nur Bordmittel-basierte Schutzsoftware ohne zentrales Management	**14 von 30 · 47 %**	—
Berechtigungen	Ausgeschiedene Mitarbeitende mit noch aktiven Zugängen	**18 von 30 · 60 %**	—
Berechtigungen	Tägliche Arbeit mit lokalen Administrationsrechten am Endgerät	**11 von 30 · 37 %**	—
Firewall / Netz	Firewall End-of-Life, ohne Signaturpflege oder mit unkontrollierten Portfreigaben	**12 von 30 · 40 %**	Verizon DBIR 2025: Angriffe auf Edge-Geräte und VPN von 3 % auf 22 % gestiegen
Server-Hardware	Mindestens ein produktiver Server älter als sechs Jahre oder ohne Herstellersupport	**13 von 30 · 43 %**	—
Dokumentation	Kein schriftlicher IT-Notfallplan vorhanden	**25 von 30 · 83 %**	GDV/forsa: 48 % der KMU ohne jeden Notfallplan
DSGVO	Kein vollständiger Vertrag zur Auftragsverarbeitung mit dem IT-Dienstleister	**16 von 30 · 53 %**	—
Versicherbarkeit	Im Ist-Zustand voraussichtlich nicht versicherbar (Mindestanforderungen nicht erfüllt)	**23 von 30 · 77 %**	—

MÄNGEL TRETEN NICHT ISOLIERT AUF

27 von 30

Betrieben wiesen drei oder mehr der oben genannten kritischen Befunde gleichzeitig auf. Ein einzelner Mangel ist die Ausnahme, das Bündel die Regel.

SELBSTEINSCHÄTZUNG UND LAGE

78 % → 38 %

In den Vorgesprächen bezeichneten zwei Drittel der Geschäftsführungen ihre IT-Sicherheit als „ausreichend“ oder „gut“. Dieselbe Verzerrung zeigt die GDV/forsa-Befragung: 78 % halten das Cyberrisiko für KMU allgemein für hoch, für den eigenen Betrieb nur 38 %.

3 DETAILBEFUNDE NACH THEMENFELDERN

3.1 DATENSICHERUNG

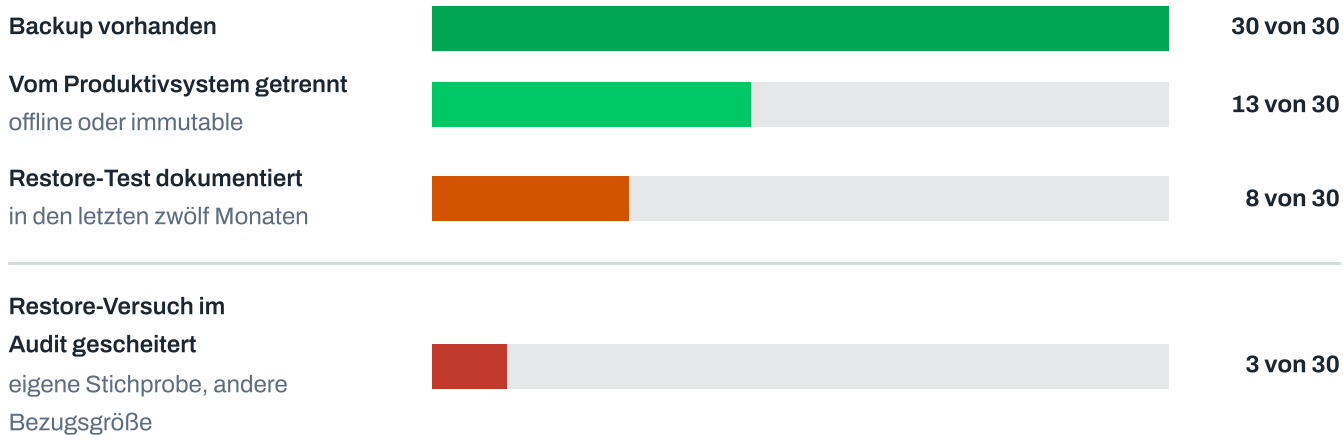
Die Datensicherung ist nach übereinstimmender Einschätzung der großen Studien die letzte Verteidigungslinie gegen Ransomware. Sophos berichtet in der Sonderauswertung „The impact of compromised backups on ransomware outcomes“ (2024, Befragung von 2.974 IT- und Sicherheitsverantwortlichen durch Vanson Bourne), dass Angreifer bei 94 Prozent der Ransomware-Vorfälle gezielt die Backups angriffen. Wer die Sicherungen verliert, zahlt: Betroffene mit kompromittierten Backups zahlten fast doppelt so häufig Lösegeld und trugen eine achtmal höhere Gesamtrechnung für die Wiederherstellung. *Beide Werte sind globale Durchschnitte über Organisationen mit 100 bis 5.000 Beschäftigten und auf Kleinbetriebe nicht unmittelbar übertragbar.*

In der Lisser IT Stichprobe hat jeder der 30 Betriebe nominell ein Backup. Bei der Detailprüfung relativiert sich dieser Befund deutlich. Bei 17 Betrieben sind die Backups ausschließlich online erreichbar, also auf einer NAS im selben Netz oder in einem Cloud-Speicher, der vom Produktivsystem aus mit denselben Zugangsdaten zugänglich ist. Ein Angreifer mit administrativen Rechten kann diese Sicherungen mitverschlüsseln oder löschen. Ein dediziertes Offline- oder immutables Backup, wie es Versicherer seit 2025 regelmäßig verlangen, fehlt in diesen Betrieben.

Wichtiger noch als das Vorhandensein eines Backups ist die regelmäßige Wiederherstellungsprüfung. In 22 der 30 Betriebe ließ sich kein dokumentierter Restore-Test innerhalb der letzten zwölf Monate nachweisen. In drei Betrieben scheiterte der stichprobenartige Restore-Versuch im Rahmen des Audits, weil die Sicherungsdaten unvollständig oder die Wiederherstellungssoftware nicht mehr funktionsfähig war. Ein Backup, das nicht regelmäßig getestet wird, ist im Versicherungsfall regelmäßig kein Backup im Sinne der Obliegenheiten.

VOM BACKUP ZUR BELASTBAREN SICHERUNG — WIE VIELE DER 30 BETRIEBE JEDE STUFE ERREICHEN

LISSER IT STICHPROBE



Jeder Betrieb hat ein Backup — aber nur 8 können belegen, dass es funktioniert. In drei Betrieben scheiterte der Wiederherstellungsversuch während des Audits: unvollständige Sicherungsdaten oder eine nicht mehr funktionsfähige Wiederherstellungssoftware.

3.2 PATCH-MANAGEMENT

Verizon weist im Data Breach Investigations Report auf eine Verschiebung der Einstiegsvektoren hin: 2024 hatte die Ausnutzung bekannter Schwachstellen um 180 Prozent zugenommen, im DBIR 2025 stieg sie um weitere 34 Prozent auf 20 Prozent aller Datenpannen — knapp hinter dem Missbrauch von Zugangsdaten (22 Prozent). Im DBIR 2026 ist Schwachstellen-Ausnutzung mit 31 Prozent erstmals der wichtigste Einstiegsvektor, während Zugangsdaten-Missbrauch auf 13 Prozent fällt. Bemerkenswert ist ein zweiter Wert aus demselben Bericht: Nur 26 Prozent der als kritisch geführten, aktiv ausgenutzten Schwachstellen wurden 2025 vollständig geschlossen — 2024 waren es noch 38 Prozent.

In der Lisser IT Stichprobe verfügen 11 von 30 Betrieben über einen funktionierenden, dokumentierten Patch-Prozess für Server und Clients. Bei den übrigen 19 Betrieben wurden Updates gar nicht eingespielt, manuell und unregelmäßig vorgenommen oder nur für die Workstations automatisiert, während Server, Firewalls und Switches mit dem Stand der Erstinstallation liefen. Die kritischsten Befunde betrafen netzaktive Komponenten: In fünf Betrieben war die Firmware der Firewall älter als drei Jahre, in zwei Betrieben war die Firewall selbst End-of-Life und erhielt keine Sicherheitsupdates mehr.

3.3 ENDPOINT PROTECTION

Die klassische Antivirensignatur reicht nach übereinstimmender Auffassung von Versicherern und BSI für den Schutz produktiver Endgeräte nicht mehr aus; für die Erneuerung von Cyber-Policen wird zunehmend „Endpoint Detection and Response“ mit zentralem Management gefordert. In der Stichprobe verfügen 16 Betriebe über eine professionell verwaltete Endpoint-Lösung mit Zentralkonsole. 14 Betriebe nutzen ausschließlich die in Windows enthaltenen Bordmittel ohne zentrale Auswertung oder kostenlose Produkte für den Heimanwendermarkt,

die für den geschäftlichen Einsatz weder lizenzkonform noch funktional ausreichend sind. In drei Betrieben war die Lizenz der Schutzsoftware abgelaufen, ohne dass dies dem Inhaber bekannt war.

3.4 E-MAIL-SICHERHEIT UND MULTI-FAKTOR-AUTHENTIFIZIERUNG

E-Mail bleibt der häufigste Einstiegsvektor. Der GDV berichtet aus der forsa-Befragung, dass 68 Prozent aller erfolgreichen Angriffe mit einer Phishing-Mail oder einer E-Mail mit Schadsoftware beginnen; Verizon nennt Phishing im DBIR 2025 als dritthäufigsten Einstiegsvektor (16 Prozent).

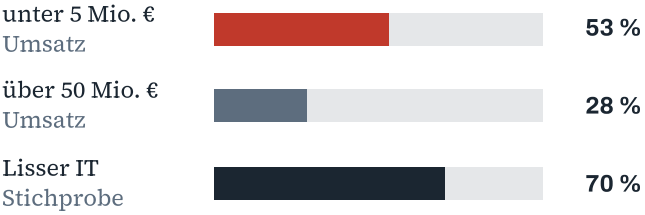
In der Stichprobe nutzen 26 der 30 Betriebe Microsoft 365 für E-Mail und Office. Bei 21 dieser Betriebe ist Multi-Faktor-Authentifizierung nicht durchgängig aktiviert: In neun Fällen war MFA für die Administratorenkonten aktiv, nicht jedoch für die Anwenderkonten, in zwölf Fällen war MFA gar nicht aktiv. Microsoft sieht seit 2024 für neue Tenants MFA als Standard vor; in älteren Tenants bleibt die Aktivierung eine bewusste Konfigurationsentscheidung. Der Data Breach Report 2026 von Baobab Risk Solutions — ausgewertet über mehr als 10.000 Angriffsoberflächen-Scans — beziffert den Anteil der Unternehmen ohne MFA bei unter 5 Mio. € Umsatz auf 53 Prozent, bei über 50 Mio. € Umsatz auf 28 Prozent. Die Lisser-Befunde liegen damit im Bereich dessen, was auch marktweit gemessen wird.

In den vier Betrieben mit On-Premises-Postfach (Exchange Server) fehlte eine externe E-Mail-Filterung: Spam-Filter, Anhangs-Sandboxing und URL-Rewriting waren nicht vorhanden oder nicht aktiv konfiguriert.

MFA-STATUS DER 26 MICROSOFT-365-BETRIEBE

MFA gar nicht aktiv	12
nur Administratorkonten	9
durchgängig aktiv	5

ANTEIL OHNE MFA NACH UNTERNEHMENSGRÖSSE



Marktwerte: Baobab Risk Solutions, Data Breach Report 2026. Der Lisser-Wert bezieht sich auf alle 30 Betriebe und auf sämtliche externen Zugänge, nicht nur auf Microsoft 365 — die Werte sind daher benachbart, nicht deckungsgleich.

3.5 IDENTITÄTS- UND BERECHTIGUNGSMANAGEMENT

Zugriffsrechte sammeln sich an. Mitarbeitende erhalten beim Eintritt Rechte für ihre Aufgabe, beim Wechsel weitere für die neue — beim Austritt werden die Konten oft nicht oder nur verzögert deaktiviert. Bei 18 der 30 Betriebe (60 Prozent) fand sich mindestens ein aktiver Zugang einer Person, die das Unternehmen verlassen hatte. Im Median lag der Zeitraum seit Austritt bei neun Monaten, in zwei Fällen waren die Konten seit mehr als drei Jahren aktiv.

(Der Median ist der mittlere Wert einer nach Größe sortierten Reihe: eine Hälfte der Fälle liegt darunter, eine darüber. Anders als der Durchschnitt wird er von einzelnen Extremfällen — hier den beiden Konten mit über drei Jahren — nicht nach oben gezogen.) In neun Betrieben fanden sich aktive Konten ehemaliger externer Dienstleister oder Praktikanten.

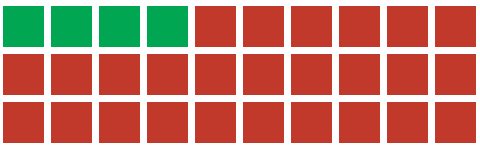
11 Betriebe arbeiten standardmäßig mit lokalen Administrationsrechten auf den Arbeitsplatzrechnern. Eine Malware, die in diesem Nutzerkontext startet, kann unmittelbar systemweite Änderungen vornehmen. Sieben Betriebe nutzen für die tägliche Arbeit dasselbe Konto wie für die Server-Administration.

3.6 NETZWERK UND FIREWALL

In 12 Betrieben war die Perimeter-Firewall in einem Zustand, der bei einem nüchternen Versicherer-Audit zur Ablehnung führen würde: drei Geräte End-of-Life, fünf ohne aktive Signatur- und Lizenzpflege, zwei mit Portfreigaben ohne aktiven Zweck, zwei mit Standard-Administratorpasswörtern aus der Werkseinstellung. Der Befund trifft auf einen Trend: Laut Verizon stieg der Anteil der Vorfälle, die über Edge-Geräte und VPN-Zugänge begannen, im DBIR 2025 von 3 auf 22 Prozent.

Netzwerksegmentierung ist in der Größenklasse 5 bis 25 Arbeitsplätze keine Selbstverständlichkeit. Vier Betriebe trennen Produktion oder medizinische Geräte vom Bürobereich. In 26 Betrieben hängen Drucker, Kassensysteme, Heizungssteuerungen, Türsprechanlagen, IP-Kameras und Bürorechner im gleichen flachen Netz. Eine kompromittierte IP-Kamera kann dort unmittelbar mit dem Buchhaltungsserver kommunizieren.

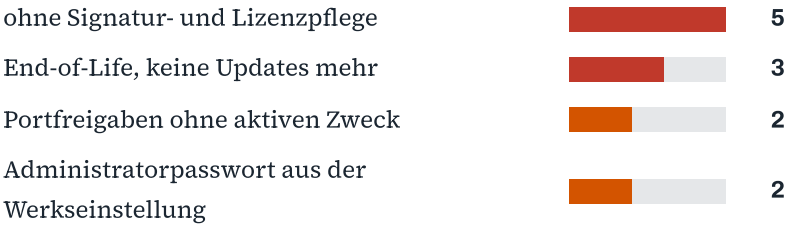
NETZWERKSEGMENTIERUNG, 30 BETRIEBE



4 Betriebe trennen Produktion oder Medizingeräte vom Bürobereich

26 Betriebe betreiben ein flaches Netz ohne Segmentierung

ZUSTAND DER 12 BEANSTANDETEN FIREWALLS



Jeder dieser vier Befunde würde in einem Versicherer-Audit für sich zur Ablehnung genügen.

3.7 SERVER-BESTAND UND HARDWARE-ALTER

In 13 Betrieben fand sich mindestens ein produktiver Server, der älter als sechs Jahre war oder ein nicht mehr unterstütztes Betriebssystem nutzte (Windows Server 2012 R2 oder älter, in zwei Fällen Windows Server 2008 R2). Diese Systeme erhalten keine regulären Sicherheitsupdates mehr. Das durchschnittliche Alter der produktiven Server lag bei 5,4 Jahren, das mediane bei sechs Jahren.

Vier Betriebe betrieben ihren zentralen Server in einem Büro- oder Vorraum ohne Klimatisierung und ohne ausreichenden Schutz vor unbefugtem Zugang. In zwei Fällen war der Serverraum gleichzeitig Lager- oder Putzraum.

ALTER DER PRODUKTIVEN SERVER — UND WO DIE HERSTELLERUNTERSTÜTZUNG ENDET

Achse: Alter der produktiven Server in Jahren; ab sechs Jahren endet in der Praxis die Herstellerunterstützung. Betriebssysteme ohne Support waren Windows Server 2012 R2 und älter, in zwei Fällen 2008 R2.

13
Betriebe mit mindestens einem Server ohne Sicherheitsupdates

4
Server in Büro- oder Vorräumen ohne Klimatisierung und Zutrittsschutz

2
Serverräume, die gleichzeitig Lager- oder Putzraum sind

3.8 DOKUMENTATION UND NOTFALLPLANUNG

25 der 30 Betriebe verfügen über keinen schriftlichen IT-Notfallplan. Diese Quote liegt deutlich über dem vom GDV berichteten Wert von 48 Prozent — plausible Erklärung ist, dass die vom GDV befragten Mittelständler in der Regel deutlich größer sind. Eine aktuelle Netzwerk- und Systemdokumentation fand sich in sieben Betrieben; in den übrigen 23 existierte keine Dokumentation, oder die Unterlagen waren veraltet, unvollständig oder nur im Kopf eines einzelnen Mitarbeitenden vorhanden. Ein Verzeichnis von Verarbeitungstätigkeiten gemäß Artikel 30 DSGVO lag in 11 Betrieben vor und war in vier davon aktuell.

3.9 SCHATTEN-IT

In 15 Betrieben (50 Prozent) wurden mindestens eine Cloud-Anwendung, ein Cloud-Speicher oder ein KI-Dienst aktiv genutzt, ohne dass die Geschäftsführung im Detail informiert war oder ein Auftragsverarbeitungsvertrag vorlag. Am häufigsten betroffen: Übersetzungsdienste, KI-Assistenten, private Dropbox- oder WeTransfer-Nutzung sowie der Austausch von Mandantendaten über persönliche E-Mail-Konten von Mitarbeitenden.

3.10 VERSICHERBARKEIT

Versicherer haben ihre Mindestanforderungen für Abschluss und Verlängerung einer Cyber-Police in den letzten zwei Jahren deutlich verschärft. Als faktischer Konsens für Unternehmen bis 10 Mio. € Umsatz gelten (Eccyber-Checkliste 2025, CyberDirekt-Marktanalyse 2024): MFA für alle externen Zugänge und Administrationskonten, regelmäßige und getestete Backups mit getrenntem Speicherort, zeitnahes Patch-Management, ein dokumentiertes Berechtigungskonzept, Mitarbeiterschulungen sowie aktueller Endpoint-Schutz und Firewall.

Auf Basis dieser Anforderungen waren 23 der 30 untersuchten Betriebe im Status der Erstbegehung voraussichtlich nicht versicherbar. Sieben Betriebe verfügten subjektiv über eine Cyber-Police; in fünf dieser Fälle bestanden im Audit erkennbare Verstöße gegen die Obliegenheiten — typischerweise fehlende MFA oder fehlende Backup-Tests —, die im Schadensfall eine Leistungskürzung oder Leistungsverweigerung wahrscheinlich machen.

4 SCHADENSPOTENZIAL UND WIRTSCHAFTLICHE EINORDNUNG

Die in den Medien zirkulierenden Schadenssummen sind für Kleinunternehmen nur eingeschränkt aussagekräftig. Sophos beziffert die durchschnittliche Lösegeldzahlung im „State of Ransomware 2024“ weltweit auf 2 Mio. US-Dollar und die Wiederherstellungskosten ohne Lösegeld auf 2,73 Mio. US-Dollar. Diese Zahlen beziehen sich auf Organisationen mit 100 bis 5.000 Mitarbeitenden. Für die hier betrachtete Größenklasse sind vier andere Datenpunkte aussagekräftiger.

REALISTISCHE GRÖSSENORDNUNGEN FÜR EINEN BETRIEB MIT 5 BIS 25 ARBEITSPLÄTZEN

25.000 – 100.000 €

DIREKTER SCHADEN PRO VORFALL

Referenz: GDV 45.370 € je versichertem Cyberschaden 2023 (+8,3 % gegenüber 2022); Verizon nennt bei Erpressungsvorfällen einen Median um 46.000 US-Dollar.

30.000 – 250.000 €

WIEDERHERSTELLUNGSKOSTEN

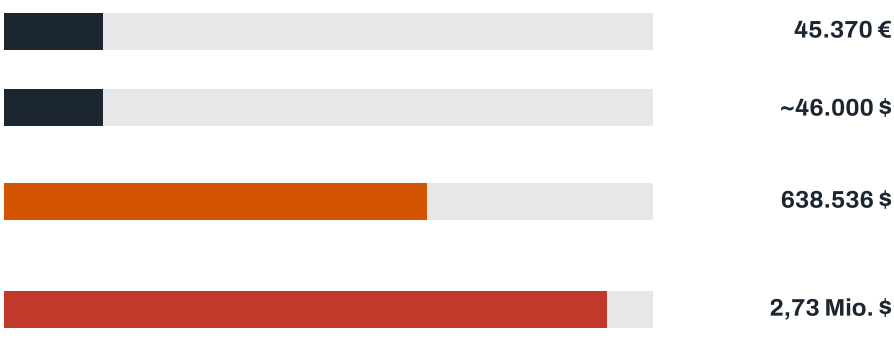
Forensik, Wiederherstellung, externe Dienstleister, Anwaltskosten, Mehraufwand der eigenen Leute. Sophos nennt für Unternehmen mit 100 bis 250 Mitarbeitenden 638.536 US-Dollar — nach unten nicht linear skalierbar.

1 – 4 Wochen

AUSFALL BIS ZUR WIEDERHERSTELLUNG

Sophos „State of Ransomware 2025“: 53 % stellen binnen einer Woche wieder her, 18 % brauchen länger als einen Monat. Coveware nennt als Median 24 Tage.

WARUM DIE ZITIERTEN MILLIONENBETRÄGE NICHTS ÜBER EINEN KLEINBETRIEB SAGEN — LOGARITHMISCHE SKALA



Die beiden oberen Werte stammen aus Erhebungen, die auch kleine Schäden erfassen; die beiden unteren aus Befragungen von Organisationen ab 100 Beschäftigten. Für einen Betrieb mit 5 bis 25 Arbeitsplätzen ist der obere Bereich der Maßstab — die Millionenbeträge beschreiben eine andere Größenklasse.

Ausfallzeit ist der teuerste Posten. Für einen Handwerksbetrieb mit 15 Mitarbeitenden und einem Tagesumsatz von 3.000 € je Mitarbeitenden bedeuten zehn Arbeitstage Stillstand einen Umsatzverlust in der Größenordnung von 450.000 €. Das ist eine Modellrechnung, keine

Messung — aber sie zeigt die Relation: Der Betriebsstillstand kostet in dieser Größenklasse ein Mehrfaches des unmittelbaren IT-Schadens, und schon ein anteiliger Ausfall belastet die Liquidität spürbar.

DSGVO-Bußgeldrisiko. Bei einer Datenschutzverletzung mit Meldepflicht nach Artikel 33 DSGVO drohen Bußgelder bis zu 20 Mio. € oder 4 Prozent des weltweiten Jahresumsatzes. Für Kleinunternehmen ist die obere Grenze irrelevant; in der Praxis bewegen sich die von deutschen Aufsichtsbehörden gegen kleine Unternehmen verhängten Bußgelder im niedrigen fünfstelligen Bereich. Erheblicher als das Bußgeld sind meist die Kosten der Meldung selbst — Anwalt, Forensik, Benachrichtigung der Betroffenen — und die Reputationsfolgen.

Reputations- und Folgekosten. Geschäftspartner erwarten inzwischen den Nachweis eines Mindestmaßes an IT-Sicherheit. Steuerberater, Rechtsanwälte und Ärzte sind ohnehin durch Berufsrecht verpflichtet; im Maschinenbau und in der Logistik werden Anforderungen über Lieferketten-Klauseln und Auftragsverarbeitungsverträge weitergegeben. Ein bekannt gewordener Vorfall führt regelmäßig zu Kundenanfragen, zusätzlichem Audit-Aufwand und im Einzelfall zum Verlust größerer Aufträge.

Versicherungsdeckungslücken. Versicherer prüfen die Obliegenheiten im Schadensfall genau. Häufigste Gründe für Leistungskürzung oder -verweigerung sind fehlende oder nicht nachweisbare MFA, nicht getestete Backups, verspätet eingespielte Sicherheitsupdates und fehlende Mitarbeiterschulungen. Eine Cyber-Police ohne belastbare Dokumentation der vereinbarten Maßnahmen ist kein zuverlässiger Risikotransfer.

5 RECHTLICHER RAHMEN

5.1 NIS-2 UND IHRE INDIREKTE WIRKUNG

Das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) wurde am 5. Dezember 2025 im Bundesgesetzblatt verkündet und ist am 6. Dezember 2025 in Kraft getreten — ohne allgemeine Übergangsfrist. Direkt betroffen sind rund 29.500 Unternehmen in 18 Sektoren, im Wesentlichen Betreiber kritischer Infrastrukturen und Unternehmen ab 50 Beschäftigten oder 10 Mio. € Jahresumsatz; bisher waren es etwa 4.500. Die Registrierungsfrist beim BSI ist für die meisten Einrichtungen am 6. März 2026 abgelaufen. Mikro- und Kleinunternehmen unter diesen Schwellen sind von den direkten Pflichten grundsätzlich ausgenommen.

Für die hier betrachteten Kleinunternehmen ist NIS-2 dennoch relevant — über die Lieferkette. Das novellierte BSI-Gesetz verpflichtet betroffene Unternehmen, die Cybersicherheit ihrer unmittelbaren Zulieferer und Dienstleister in ihr Risikomanagement einzubeziehen (§ 30 BSIG). In der Praxis heißt das: Größere Auftraggeber verpflichten ihre kleinen Zulieferer vertraglich auf Sicherheitsstandards. Steuerkanzleien, IT-Dienstleister, Wartungsfirmen, Software-Zulieferer, Logistiker und Reinigungsdienste mit Zugang zu IT-Systemen werden zunehmend Fragenkataloge, Mindestanforderungen und Audit-Klauseln in ihren Verträgen wiederfinden. Wer diese Anforderungen nicht erfüllen kann, verliert mittelfristig Kunden.

NIS-2: VOM GESETZ ZUR ANFRAGE BEIM ZULIEFERER

5. DEZ. 2025	6. DEZ. 2025	6. MÄRZ 2026	H2 2026
Verkündung im Bundesgesetzblatt	In Kraft — ohne Übergangsfrist	Registrierungsfrist beim BSI abgelaufen	Erwartete Welle von Lieferanten-Fragebögen

Direkt beaufsichtigte Einrichtungen in 18 Sektoren, ab 50 Beschäftigten oder 10 Mio. € Umsatz.

Kleinbetriebe unter diesen Schwellen sind **nicht direkt verpflichtet** — aber jeder dieser 29.500 Auftraggeber muss die Cybersicherheit seiner unmittelbaren Zulieferer in sein Risikomanagement einbeziehen (§ 30 BSIG). Die Pflicht erreicht den Kleinbetrieb über den Vertrag.

5.2 DSGVO

Für Kleinunternehmen sind die zentralen Pflichten unverändert: Verzeichnis von Verarbeitungstätigkeiten (Artikel 30), technische und organisatorische Maßnahmen (Artikel 32), Meldepflichten bei Datenschutzverletzungen (Artikel 33) und Verträge zur Auftragsverarbeitung mit Dienstleistern (Artikel 28). Die Befreiung von der Pflicht zur Benennung eines Datenschutzbeauftragten gemäß § 38 BDSG für Unternehmen mit weniger

als 20 ständig automatisiert verarbeitenden Personen befreit nicht von den materiellen Pflichten. Die Aufsichtsbehörden in Niedersachsen und Bremen haben wiederholt deutlich gemacht, dass bei Kleinunternehmen vor allem Defizite bei technisch-organisatorischen Maßnahmen und Auftragsverarbeitungsverträgen gerügt werden.

5.3 DIN SPEC 27076

Die im Mai 2023 veröffentlichte DIN SPEC 27076 hat sich als pragmatischer Einstieg in die strukturierte Bestandsaufnahme etabliert. Sie ersetzt kein Managementsystem nach ISO 27001 oder IT-Grundschutz, sondern liefert eine kompakte Standortbestimmung. Der Vorteil für Kleinunternehmen liegt im überschaubaren Aufwand — ein bis zwei Stunden Interview — und in der Förderfähigkeit durch verschiedene Bundes- und Landesprogramme.

5.4 VERSICHERBARKEIT ALS FAKTISCHER STANDARD

Der Abschluss einer Cyber-Versicherung ist gesetzlich nicht verpflichtend, doch der von Versicherern geforderte Maßnahmenkatalog hat sich zum faktischen Mindeststandard entwickelt: Wer die Anforderungen erfüllt, ist versicherbar, wer sie nicht erfüllt, nicht. Diese Anforderungen überlappen erheblich mit denen der DIN SPEC 27076 und mit den NIS-2-Mindestmaßnahmen. Der Versicherbarkeits-Check kann daher als pragmatischer Hebel dienen, IT-Sicherheit organisatorisch zu strukturieren.

5.5 GESCHÄFTSFÜHRERHAFTUNG

Die Haftung der Geschäftsführung für IT-Sicherheitsversäumnisse leitet sich aus der allgemeinen Sorgfaltspflicht (§ 43 GmbHG, § 93 AktG) und aus bereichsspezifischen Vorschriften ab; das novellierte BSIG stellt Cybersicherheit für betroffene Einrichtungen ausdrücklich in die Verantwortung der Unternehmensleitung. Bei nachweisbarer Sorgfaltspflichtverletzung kann der Geschäftsführer gegenüber der Gesellschaft persönlich haften. Entscheidend ist: Es genügt nicht, IT an externe Dienstleister zu delegieren — die Geschäftsführung muss die Umsetzung überwachen und ihre Sorgfalt belegen können. Ein schriftlicher IT-Sicherheitsbericht des Dienstleisters, ein durchgeführter CyberRisikoCheck nach DIN SPEC 27076 oder ein dokumentierter Maßnahmenplan sind hierfür geeignete Belege.

6 HANDLUNGSEMPFEHLUNGEN

Die folgenden sieben Empfehlungen sind nach Wirkung und Aufwand priorisiert. Sie greifen die häufigsten Schwachstellen der Stichprobe auf und richten sich an Inhaber und Geschäftsführungen.

WIRKUNG UND AUFWAND DER SIEBEN MASSNAHMEN — NR. = EMPFEHLUNG 1–7 AUF DEN FOLGENDEN SEITEN

	AUFWAND GERING	AUFWAND HÖHER
WIRKUNG HOCH	**SOFORT UMSETZBAR** **Nr. 2** MFA flächendeckend aktivieren **Nr. 5** Notfallplan auf einer Seite **Nr. 6** Versicherbarkeits-Check	**PROJEKT MIT VORLAUF** Nr. 1 Backup absichern und testen Nr. 3 Patch-Management strukturieren
MITTEL	Nr. 4 Berechtigungen aufräumen Nr. 7 Mitarbeitende sensibilisieren	

Alle sieben Maßnahmen sind laufende Pflichten: einmal jährlich wiederholen und dokumentieren — der Nachweis zählt gegenüber Versicherern und Auftraggebern genauso wie die Maßnahme selbst.

1 Backup absichern und testen

Mindestens eine Backup-Generation liegt offline oder immutable und ist vom Produktivsystem nicht mit administrativen Rechten erreichbar. Einmal pro Quartal ein vollständiger Wiederherstellungstest, dokumentiert. Wer das nicht selbst leisten kann, beauftragt den IT-Dienstleister mit einem schriftlichen Restore-Protokoll.

2 Multi-Faktor-Authentifizierung flächendeckend aktivieren

MFA für alle externen Zugänge, alle Microsoft-365-Konten und alle Administrationskonten ist faktischer Mindeststandard für Versicherer und für NIS-2-pflichtige Auftraggeber. Die Umstellung in Microsoft 365 ist technisch innerhalb eines Tages umsetzbar; sie betrifft alle Nutzer und braucht eine kurze Ankündigung.

3 Patch-Management strukturieren

Server, Clients, Firewall, WLAN-Controller und alle aus dem Internet erreichbaren Systeme erhalten einen festen monatlichen Patch-Termin mit benannter Verantwortlichkeit. Veraltete Betriebssysteme (Windows Server 2012 R2 und älter, Windows 10 seit Oktober 2025) werden ersetzt oder isoliert betrieben.

4 Berechtigungen aufräumen

Einmal jährlich werden sämtliche Benutzerkonten überprüft; Konten ehemaliger Mitarbeitender, externer Dienstleister und Praktikanten werden deaktiviert. Lokale Administrationsrechte werden auf das notwendige Maß zurückgeführt. Geschäftsführung und Administration verwenden getrennte Konten für ihre jeweiligen Aufgaben.

5 Notfallplan auf einer Seite schreiben

Vier Fragen genügen für den Anfang: Wer ist im Ernstfall erste Ansprechperson? Wo liegen die Backup-Daten? Wer wird in welcher Reihenfolge informiert (IT-Dienstleister, Versicherung, Behörden, Mitarbeitende)? Welche Systeme dürfen vom Netz getrennt werden? Diese Seite wird gedruckt und dort verwahrt, wo sie auch ohne IT zugänglich ist.

6 Versicherbarkeits-Check als Hebel nutzen

Die Anforderungen der Cyber-Versicherer sind ein pragmatischer, branchenakzeptierter Maßnahmenkatalog. Wer die Versicherbarkeit anstrebt, deckt damit gleichzeitig die wichtigsten Pflichten aus DSGVO und NIS-2-Lieferkette ab. Eine Erstprüfung über einen unabhängigen Makler oder den IT-Dienstleister schafft eine konkrete Aufgabenliste.

7 Mitarbeitende sensibilisieren

Mindestens einmal jährlich eine Schulung zu Phishing, Zahlungsanweisungen, Umgang mit USB-Datenträgern und Verhalten im Verdachtsfall. Praxisnahe Übungen wirken besser als Frontalvorträge. Schulungen werden mit Datum, Teilnehmern und Inhalt dokumentiert — das ist auch der Nachweis gegenüber Versicherern.

7 AUSBLICK 2026 UND 2027

Vier Entwicklungen zeichnen sich aus heutiger Sicht ab, die für Kleinunternehmen in der Region relevant werden.

KI-GESTÜTZTE PHISHING- UND BETRUGSANGRIFFE

Die Qualität von Phishing-Mails und Vishing-Anrufen hat durch generative KI ein Niveau erreicht, das klassische Erkennungsmerkmale wie Grammatikfehler oder Stilbrüche obsolet macht. Allianz Trade berichtet, dass Wirtschaftskriminelle ihre Social-Engineering-Maschen mit KI-Werkzeugen weiter professionalisieren und Deepfakes beim Fake-President-Betrug eine große Gefahr darstellen; die Fallzahlen beim Fake-President-Betrug stiegen 2023 um 31 Prozent, für das Folgejahr erwartete der Kreditversicherer ein deutlich steigendes Schadenvolumen bei gleichbleibenden Fallzahlen. Für Kleinunternehmen liegt die wirksamste Gegenmaßnahme ohnehin nicht in Technik: ein Vier-Augen-Prinzip bei Zahlungen ab definierter Höhe und ein schriftlich vereinbartes Rückruf-Verfahren über bekannte Telefonnummern.

LIEFERKETTENANFORDERUNGEN DURCH NIS-2

Nachdem die BSI-Registrierungsfrist im März 2026 abgelaufen ist, arbeiten die betroffenen 29.500 Unternehmen ihre Risikomanagement-Pflichten ab — und geben sie an ihre Lieferanten weiter. In der zweiten Jahreshälfte 2026 ist mit einer Welle vertraglicher Anfragen zu rechnen, besonders bei Zulieferern im Maschinenbau, im Lebensmittel- und Logistiksektor sowie bei IT-nahen Dienstleistern. Kleinunternehmen, die einen strukturierten IT-Basisschutz nachweisen können — etwa über einen CyberRisikoCheck oder eine bestehende Cyber-Police —, haben hier einen Wettbewerbsvorteil.

STEIGENDE ANFORDERUNGEN DER CYBER-VERSICHERER

Die Schaden-Kosten-Quote der Cyber-Sparte lag laut GDV 2023 bei 97 Prozent, nach 77,7 Prozent im Jahr 2022 — die Prämieneinnahmen wurden von den Schäden fast vollständig aufgezehrt. Versicherer reagieren mit steigenden Prämien und schärferen Obliegenheiten. Für 2026 und 2027 ist mit zusätzlichen Anforderungen zu rechnen, insbesondere mit „Endpoint Detection and Response“ auch in kleineren Versichertenkategorien und mit der Pflicht zu dokumentierten Restore-Tests.

WEGFALL VON BORDMITTEL-LÖSUNGEN

Mit dem Auslaufen des Supports für Windows 10 im Oktober 2025 und der schrittweisen Abkündigung weiterer Office-Versionen entstehen 2026 und 2027 zusätzliche Investitionsbedarfe. Wer diese Gelegenheit nutzt, alte On-Premises-Server abzulösen und auf Microsoft 365 mit aktivierter MFA umzustellen, deckt mehrere Compliance-Anforderungen gleichzeitig ab.

8 ÜBER DEN AUTOR

Patrick Lisser ist seit 2005 in der IT tätig und führt das 2017 gegründete Lisser IT-Systemhaus mit Sitz in Hude (Landkreis Oldenburg). Er betreut kleine und mittlere Unternehmen in der Region Oldenburg und Bremen als verantwortlicher IT-Dienstleister — von der Standortbestimmung über den laufenden Betrieb bis zum Notfall. Schwerpunkte sind IT-Basisschutz nach DIN SPEC 27076, Managed Services für Microsoft 365, Datensicherung und der Nachweis der Cyber-Versicherbarkeit.

Die 30 Erstbegehungen dieses Reports hat er selbst durchgeführt, dokumentiert und ausgewertet. Kontakt: Auf der Nordheide 12, 27798 Hude · info@lisser-it.de · Tel. 04408-9999999 · lisser-it.de

STANDORTBESTIMMUNG

Die in diesem Report genannten Befunde entstammen einem CyberRisikoCheck nach DIN SPEC 27076 — einem strukturierten Interview von ein bis zwei Stunden mit schriftlichem Ergebnisbericht und Maßnahmenplan. Lisser IT-Systemhaus führt diesen Check für Betriebe in der Region durch; er ist über verschiedene Bundes- und Landesprogramme förderfähig. Kontakt: info@lisser-it.de, Tel. 04408-9999999.

9 QUELLENVERZEICHNIS

Bei allen Quellen, deren Zahlen im Text verwendet werden, ist der Bezugsrahmen — Stichprobe und Erhebungsjahr — genannt, weil er über die Übertragbarkeit auf Kleinbetriebe entscheidet.

- Bitkom e.V.: Wirtschaftsschutz 2025, September 2025. 1.002 Unternehmen ab 10 Beschäftigten und 1 Mio. € Umsatz, Befragung April–Juni 2025. Auch: Wirtschaftsschutz 2024 (1.003 Unternehmen).
- Bundesamt für Verfassungsschutz: Vorstellung der Bitkom-Studie „Wirtschaftsschutz 2025“, 18. September 2025 (Einordnung 87 % / 289,2 Mrd. €).
- Bundesamt für Sicherheit in der Informationstechnik (BSI): Die Lage der IT-Sicherheit in Deutschland 2024 und 2025, Bonn, jeweils November; CyberRisikoCheck nach DIN SPEC 27076 — Informationen für KMU.
- Sophos: The Impact of Compromised Backups on Ransomware Outcomes, 2024. 2.974 IT- und Sicherheitsverantwortliche, Vanson Bourne. Global, Organisationen mit 100–5.000 Beschäftigten.
- Sophos: The State of Ransomware 2024 (5.000 Befragte, 14 Länder) und The State of Ransomware 2025 (3.400 Befragte, 17 Länder).
- Verizon Business: 2025 Data Breach Investigations Report (22.052 Vorfälle, 12.195 bestätigte Datenpannen, 139 Länder, Zeitraum 11/2023–10/2024); 2024 DBIR; 2026 DBIR (Berichterstattung Mai 2026).
- GDV: Mehr Cyberschäden – Prävention wichtiger denn je, September 2024 (4.000 gemeldete Angriffe 2023, 180 Mio. € Leistungen, 45.370 € je Schaden, Schaden-Kosten-Quote 97 %).
- GDV / forsa: IT-Sicherheit vieler deutscher Unternehmen ist mangelhaft, September 2025, und Notfallplan für Cyberangriff fehlt oft, Dezember 2024. Jährlich 300 Entscheider und IT-Verantwortliche kleiner und mittlerer Unternehmen.
- Baobab Risk Solutions: Data Breach Report 2026 (über 10.000 Angriffsoberflächen-Scans, über 50.000 geleakte Datensätze) — Zusammenfassung im Sicherheits-Berater, Juni 2026.
- Bundesregierung: Umsetzung der NIS-2-Richtlinie beschlossen, Dezember 2025; NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, Bundesgesetzblatt 5. Dezember 2025.
- DIN SPEC 27076:2023-05, IT-Sicherheitsberatung für Klein- und Kleinstunternehmen, Berlin: DIN Media.
- Allianz Commercial: Allianz Risk Barometer 2025 und 2026, München, jeweils Januar. Allianz Trade: Schadensstatistik zu Fake-President-Betrug, November 2024.
- Weitere herangezogene Quellen: Gothaer KMU-Studie 2024 (1.022 Entscheider); HDI Cyberstudie 2024; Coveware Quarterly Ransomware Reports 2024/2025; CyberDirekt Marktanalyse Cyberversicherung 2024; Eccyber, Checkliste Mindestanforderungen Cyberversicherung, Stand 2025; DsiN-Praxisreport Mittelstand 2022.