AEGYS DATALYTICS

12-PUNKTE-CHECKLISTE · MAI 2026

12-Punkte-Sicherheits-Checkliste für Steuerkanzleien

Was Cyberversicherer 2026 verlangen.
Was §203 StGB technisch bedeutet.
Was den Stand der Technik für Steuerkanzleien ausmacht.

> Erstellt von der AEGYS DATALYTICS AG. Basierend auf BSI-Lagebericht 2025, BSI IT-Grundschutz, dokumentierten Versicherer-Anforderungen 2026 (CyberDirekt, Munich Re), juristischer Standardliteratur zu §203 StGB, sowie der praktischen Erfahrung aus Einsätzen bei Steuerkanzleien und Mittelstand.

Diese Checkliste ersetzt keine Rechts- oder Versicherungsberatung. Bei konkreten Fragen ziehen Sie bitte einen Fachanwalt oder Versicherungsmakler hinzu.

EINFÜHRUNG

Wie diese Checkliste zu nutzen ist

Diese Checkliste ist kein Marketing-Material. Sie ist ein Werkzeug, mit dem Sie in 30 Minuten eine ehrliche Bestandsaufnahme der IT-Sicherheit Ihrer Kanzlei machen können — gemeinsam mit Ihrer Kanzleileitung und idealerweise auch mit Ihrem IT-Betreuer. Die zwölf Punkte stammen aus drei Quellen, die für Steuerkanzleien 2026 entscheidend sind:

1. Versicherer-Anforderungen 2026	2. §203 StGB & §62a StBerG	3. BSI Stand der Technik 2026
Was Cyberversicherer im Antragsformular detailliert abfragen — von MFA bis Vulnerability Scanning. Wer hier nicht klar antworten kann, wird abgelehnt oder verliert im Schadensfall die Deckung.	Was die Verschwiegenheitspflicht im digitalen Kontext technisch bedeutet — inklusive der „Offenbarung durch Unterlassen“, die strafrechtliche Verantwortung des Berufsträgers auslösen kann.	Was nach BSI-Lagebericht 2025 und IT-Grundschutz von einer Kanzlei mit Mandantendaten erwartet wird. Maßstab für Versicherer und Gerichte gleichermaßen.

So gehen Sie vor

Schritt 1: Selbstbewertung

Lesen Sie jeden Punkt durch. Beantworten Sie die Prüf-Fragen mit Ja, Teilweise oder Nein. Seien Sie dabei ehrlich — diese Checkliste sieht niemand außer Ihnen, und eine optimistische Selbsteinschätzung hilft im Schadensfall nicht weiter.

Schritt 2: Mit dem IT-Betreuer abstimmen

Bei Punkten mit „Teilweise“ oder „Nein“ sprechen Sie mit Ihrem IT-Betreuer. Nicht jeder Punkt muss sofort umgesetzt werden — wichtiger ist, dass Sie den Status kennen und wissen, was als Nächstes ansteht.

Schritt 3: Prioritäten setzen

Nutzen Sie die Prioritäten-Matrix auf Seite 9. Sie zeigt, welche Punkte sofort umgesetzt werden sollten, welche kurzfristig anstehen, und welche mittelfristig sinnvoll sind.

Wichtiger Hinweis

Diese Checkliste ist eine fachliche Orientierung, keine Rechts- oder Versicherungsberatung. Bei konkreten Fragen zur Cyberversicherung wenden Sie sich an einen unabhängigen Versicherungsmakler. Bei Fragen zu §203 StGB an einen Fachanwalt für IT-Recht oder Strafrecht.

Prüfen Sie jeden Punkt für Ihre Kanzlei

01 Multi-Faktor-Authentifizierung (MFA)

Warum: Die wichtigste einzelne Maßnahme. Ohne MFA bekommen Sie 2026 in den meisten Fällen keine Cyberversicherung mehr. Auch der BSI-Lagebericht 2025 nennt MFA als zentrale Basismaßnahme. Ein gestohlenes Passwort ist ohne MFA eine offene Tür; mit MFA ist es wertlos.

Prüf-Fragen für Ihre Kanzlei

- Ist MFA für das DATEV-Konto aktiviert (alle Mitarbeitenden)?
- Ist MFA für Microsoft 365 / E-Mail-Postfächer aktiviert?
- Ist MFA für den VPN-Zugang ins Kanzleinetzwerk aktiviert?
- Ist MFA für alle Administrator-Konten verbindlich?
- Ist MFA für Cloud-Speicher (OneDrive, SharePoint, Dropbox) aktiv?

SCHADENSFALL Wenn im Versicherungs-Antrag MFA mit „ja“ bestätigt wurde und im Schadensfall stellt sich heraus, dass MFA an einem Verwaltungs-Account fehlte, kann der gesamte Vertrag rückabgewickelt werden — auch wenn dieser Account nicht der Eintrittspunkt war (§22 VVG).

02 Backup-Strategie nach 3-2-1-Regel

Warum: 88 Prozent der Versicherer stellen laut CyberDirekt-Marktanalyse 2024 eine Risikofrage zum Thema Datensicherung. Die 3-2-1-Regel ist Industriestandard: drei Kopien der Daten, zwei verschiedene Medien, eine Kopie offline oder logisch isoliert. Ein Backup, das zusammen mit den Live-Systemen verschlüsselt werden kann, gilt versicherungstechnisch nicht als Backup.

Prüf-Fragen für Ihre Kanzlei

- Existieren mindestens drei Kopien der wichtigsten Mandantendaten?
- Sind diese Kopien auf mindestens zwei verschiedenen Medien gespeichert?
- Ist mindestens eine Kopie offline oder logisch vom Netzwerk isoliert?
- Wurde im letzten Jahr ein vollständiger Restore-Test durchgeführt?
- Ist der Wiederherstellungs-Prozess schriftlich dokumentiert?

SCHADENSFALL Bei Ransomware-Angriffen werden Live-Backups regelmäßig mit verschlüsselt. Wer keine isolierte Kopie hat, hat keine Backup, sondern eine Illusion — und im Schadensfall einen Totalverlust der Mandantendaten.

03 Patch-Management mit Dokumentation

Warum: Versicherer wollen „zeitnahe Einspielung sicherheitsrelevanter Updates und Patches“ nachweisbar sehen. Der Begriff „zeitnah“ wird im Schadensfall sehr eng ausgelegt: Wochen sind zu lang. Beispiel ProxyLogon (2021): Ungepatchte Exchange-Server führten in zahlreichen deutschen Unternehmen sowohl zu Sicherheitsvorfällen als auch zu verweigerten Versicherungsleistungen.

Prüf-Fragen für Ihre Kanzlei

- Existiert ein dokumentierter Patch-Management-Prozess?
- Wer ist für das Patch-Management zuständig (intern / IT-Betreuer)?
- In welchen Intervallen werden Server gepatcht? Arbeitsplätze? Netzwerk?
- Wird der Patch-Status regelmäßig dokumentiert (Excel, Tool, Bericht)?
- Gibt es einen Notfall-Prozess für kritische Sicherheits-Patches?

SCHADENSFALL Wenn ein bekannter, gepatchter Exploit der Eintrittspunkt war — und der Server ungepatcht blieb — ist das eine klassische Obliegenheitsverletzung. Versicherer verweigern in solchen Fällen die Leistung mit Verweis auf die AVB.

04 Endpoint Detection & Response (EDR)

Warum: Klassischer Virenschutz erkennt nur, was er kennt. EDR erkennt auch verdächtige Verhaltensmuster auf Endgeräten. Versicherer fragen 2026 explizit nach EDR-Lösungen. Wer im Antrag „Antiviren-Software“ ankreuzt, aber nur klassischen AV einsetzt, macht möglicherweise eine irreführende Angabe.

Prüf-Fragen für Ihre Kanzlei

- Ist auf allen Servern eine EDR-Lösung installiert? (Microsoft Defender for Endpoint, SentinelOne, CrowdStrike, etc.)
- Ist EDR auf allen Arbeitsplätzen — auch im Home-Office — aktiv?
- Werden EDR-Warnungen durch jemanden geprüft (intern oder durch IT-Betreuer)?
- Ist die EDR-Konfiguration dokumentiert?

SCHADENSFALL Bei Falschangaben im Antrag („wir haben EDR“, aber nur klassischer AV) kann der Versicherer den Vertrag wegen arglistiger Täuschung anfechten (§123 BGB). Auch ohne Vorsatz ist eine Vertragsanpassung möglich.

05 Schwachstellen-Scans regelmäßig

Warum: Versicherer fordern den Nachweis, dass Schwachstellen aktiv gesucht werden — und nicht erst durch Angriffe entdeckt. Das BSI sieht Schwachstellen-Management als Kernpflicht: 2025 wurden täglich 119 neue Schwachstellen in IT-Systemen bekannt.

Prüf-Fragen für Ihre Kanzlei

- Werden regelmäßig Schwachstellen-Scans des Kanzleinetzwerks durchgeführt?
- Welche Frequenz (monatlich, quartalsweise)?
- Welches Werkzeug wird verwendet? (Wer ist verantwortlich?)
- Werden gefundene Schwachstellen dokumentiert und nachverfolgt?
- Gibt es eine Eskalationsstufe für kritische Funde?

SCHADENSFALL Ohne dokumentierte Scans hat die Kanzlei keine Position, sich zu verteidigen mit dem Argument: „wir kannten die Lücke nicht“. Die Position wäre dann: „wir haben nicht gesucht“ — was strafrechtlich und versicherungstechnisch deutlich schlechter ist.

06 Privilegierte Zugriffe begrenzt

Warum: 40 bis 50 Prozent der Cyberversicherer verlangen 2026 PAM-Lösungen (Privileged Access Management) oder zumindest das Konzept der „Zero Standing Privileges“: Kein Mitarbeitender hat dauerhaft Administrator-Rechte. Privilegierte Zugriffe werden nur temporär und dokumentiert vergeben.

Prüf-Fragen für Ihre Kanzlei

- Hat jeder Sachbearbeiter ausschließlich Standardrechte (kein Admin)?
- Gibt es klare Liste, wer Domain-Admin-Rechte hat (idealerweise nicht mehr als 1–2 Personen)?
- Sind Admin-Konten von normalen Arbeits-Konten getrennt? (Niemand sollte mit Admin-Account E-Mails lesen.)
- Werden privilegierte Aktionen geloggt?

SCHADENSFALL Wenn ein Mitarbeitender mit Admin-Rechten Opfer einer Phishing-Mail wird, ist der Angreifer sofort Domain-Admin. Bei eingeschränkten Rechten muss er erst einen Privilege-Escalation-Schritt schaffen — Zeit, in der Detection-Tools anschlagen können.

07 Incident Response Plan dokumentiert

Warum: Versicherer wollen 2026 explizit sehen, dass Sie im Ernstfall wissen, was zu tun ist. Der Plan muss nicht nur existieren, sondern getestet sein. Cyberversicherungen verlangen ausserdem die Schadensanzeige binnen 24–72 Stunden — das geht nur, wenn intern klar ist, wer den Versicherer anruft.

Prüf-Fragen für Ihre Kanzlei

- Existiert ein schriftlicher Incident Response Plan?
- Sind Verantwortlichkeiten klar definiert (wer entscheidet, wer kommuniziert, wer ruft Versicherer an)?
- Ist der Plan auch offline verfügbar (gedruckt, falls Server verschlüsselt)?
- Wurde der Plan in den letzten 12 Monaten getestet (Tabletop-Uebung, Notfall-Simulation)?
- Sind Notfall-Kontakte aktuell (IT-Forensik, Anwalt, Versicherer, Datenschutzaufsicht)?

SCHADENSFALL Ohne Plan verstreichen die ersten 24 Stunden mit Chaos und unklaren Zuständigkeiten. Genau diese 24 Stunden entscheiden über die Schadenshöhe — und über das Verhalten des Versicherers, der bei verspäteter Meldung Leistungen kürzen kann.

08 Mitarbeiter-Sensibilisierung jährlich

Warum: Phishing ist nach BSI-Lagebericht 2025 eine der häufigsten Angriffsmethoden — 26 Prozent aller Vorfälle. Versicherer fordern Nachweise über Awareness-Maßnahmen. Ohne Schulungs-Dokumentation argumentieren Versicherer im Schadensfall mit Obliegenheitsverletzung.

Prüf-Fragen für Ihre Kanzlei

- Wann fand die letzte Mitarbeiter-Schulung zu IT-Sicherheit statt?
- Werden Schulungen jährlich durchgeführt? Auch für Auszubildende?
- Werden Phishing-Simulationen durchgeführt? (DSGVO-konform: pseudonymisierte Auswertung)
- Gibt es einen klaren Meldeweg, wenn jemand auf eine Phishing-Mail geklickt hat? (Ohne Sanktion bei Selbstanzeige)
- Ist die Schulungsteilnahme dokumentiert (Liste mit Datum, Inhalt, Teilnehmenden)?

SCHADENSFALL Ohne dokumentierte Schulungen wird der Versicherer im Schadensfall argumentieren, dass die Awareness-Pflicht (organisatorische Maßnahme nach DSGVO und Versicherungs-Obliegenheit) nicht erfüllt wurde.

09 Drittanbieter §203-konform verpflichtet

Warum: §203 Abs. 4 Nr. 1 StGB stellt klar: Wer Dritte als „mitwirkende Personen“ einbindet — IT-Betreuer, Cloud-Anbieter, Software-Hersteller, KI-Tools — ohne sie schriftlich zur Verschwiegenheit zu verpflichten und über die strafrechtlichen Folgen zu belehren, macht sich selbst strafbar. Eine DSGVO-AVV reicht NICHT.

Prüf-Fragen für Ihre Kanzlei

- Ist mit dem IT-Dienstleister ein §203-konformer Verschwiegenheitsvertrag (mit Strafrechts-Belehrung) geschlossen?
- Sind alle Cloud-Anbieter (Microsoft 365, Dropbox, etc.) §203-konform verpflichtet?
- Sind eingesetzte KI-Tools (ChatGPT, Claude, andere) §203-konform?
- Wurde geprüft, welche Sub-Auftragnehmer der Hauptdienstleister einsetzt? (Lieferketten-Pflicht aus §203 Abs. 4 Nr. 2)
- Wird der §203-Status bei neuen Anbietern routinemäßig geprüft, bevor Mandantendaten dorthin gelangen?

SCHADENSFALL Persönliche strafrechtliche Verantwortung des Berufsträgers nach §203 StGB — bis zu einem Jahr Freiheitsstrafe oder Geldstrafe. Plus berufsrechtliche Maßnahmen der Steuerberaterkammer (§§ 81, 89, 90 StBerG) bis zur Ausschließung aus dem Beruf.

10 Netzwerk-Segmentierung umgesetzt

Warum: BSI-Best-Practice und zunehmend Versicherer-Standard. Drucker, Multifunktionsgeräte, Smartphones, IoT-Geräte und Gäste-WLAN sollten in separaten Netzwerk-Segmenten (VLANs) liegen — nicht im selben Netz wie die Arbeitsplätze. Verhindert laterale Bewegung von Angreifern.

Prüf-Fragen für Ihre Kanzlei

- Sind Drucker und Multifunktionsgeräte in einem eigenen VLAN?
- Liegen Mitarbeiter-Smartphones im Gäste-WLAN, nicht im Kanzleinetzwerk?
- Ist das Gäste-WLAN technisch vom Kanzlei-WLAN getrennt?
- Sind IoT-Geräte (Smart-TVs, Konferenztechnik, Klimaanlagen) isoliert?
- Ist die Segmentierung dokumentiert (Netzwerk-Plan)?

SCHADENSFALL Ohne Segmentierung verbreitet sich ein einmal erfolgreicher Angriff ungehindert im gesamten Netzwerk. Genau das ist 2024 in der VHP-Kanzlei (Werschak/DATEV-Magazin) passiert: Ein Eintrittspunkt, kompletter Datenverlust.

11 Sicht auf den Netzwerkverkehr

Warum: DATEVnet schützt den Internetverkehr in Richtung Aussenwelt. Was DATEVnet nicht sieht: die Kommunikation innerhalb Ihres Kanzleinetzwerks. Genau dort bewegen sich Angreifer aber, wenn sie einmal drin sind. Versicherer fragen 2026 nach „Tools zur Erkennung verdächtiger Aktivitäten“ — also genau diese interne Sichtbarkeit.

Prüf-Fragen für Ihre Kanzlei

- Sehen Sie aktuell, was zwischen den Geräten in Ihrem Netzwerk kommuniziert wird?
- Würden Sie auffällige Verbindungen erkennen (z.B. nächtliche Ausgangs-Verbindungen zu unbekannten Servern)?
- Werden Logs zentral gesammelt? (SIEM oder vergleichbare Lösung)
- Wer wertet die Logs aus? Wie oft?
- Im Schadensfall — könnten Sie nachvollziehen, was passiert ist (Forensik)?

SCHADENSFALL §203 StGB durch Unterlassen setzt voraus, dass die Kanzlei nicht weiß, was im eigenen Netzwerk passiert. Wer keine Sicht hat, kann im Schadensfall weder dem Versicherer noch der Datenschutzaufsicht detailliert erklären, was abgeflossen ist — und wann.

12 Dokumentation aller Sicherheitsmaßnahmen

Warum: Im Schadensfall ist der Unterschied zwischen „strafrechtlich angreifbar“ und „strafrechtlich verteidigbar“ oft nicht das technische Niveau selbst, sondern die Dokumentation. Auch Versicherer verlangen „nachweisbare Maßnahmen“ — nicht „umgesetzte Maßnahmen“.

Prüf-Fragen für Ihre Kanzlei

- Existiert ein schriftliches IT-Sicherheitskonzept?
- Sind alle 11 vorherigen Punkte dokumentiert (Wer? Wie? Wann zuletzt geprüft?)
- Sind Verträge mit IT-Dienstleistern und Cloud-Anbietern dokumentiert?
- Werden Sicherheitsvorfälle (auch kleine, behobene) dokumentiert?
- Liegt die Dokumentation auch offline vor, falls Server verschlüsselt werden?

SCHADENSFALL Ohne Dokumentation kann der Versicherer im Schadensfall die Antragsangaben anzweifeln und den Vertrag nach §22 VVG iVm §123 BGB anfechten. Dokumentation ist die einzige Verteidigung gegen „arglistige Täuschung“-Vorwürfe.

Prioritäten-Matrix — Was zuerst?

Die wenigsten Kanzleien können alle 12 Punkte gleichzeitig angehen. Sinnvoller ist eine Priorisierung nach Risiko-Reduktion und Aufwand. Diese Matrix gibt eine empirische Reihenfolge, die in der Praxis funktioniert hat.

SOFORT — Woche 1 bis 2	Punkt 1: MFA flächendeckend Höchster Hebel, geringster Aufwand. DATEV-Konto, Microsoft 365, VPN, Admin-Konten. Wenn nichts anderes geschafft wird, dann das. Punkt 2: Backup-Test Einen einzigen Restore-Test durchführen. Sie werden überrascht sein, was dabei nicht funktioniert. Punkt 9: §203-Status der IT-Dienstleister prüfen Brief an Hauptdienstleister: „Haben wir eine §203-konforme Verschwiegenheitsvereinbarung?“ — Wenn nicht, sofort nachholen.
KURZFRISTIG — Monat 1 bis 3	Punkt 3: Patch-Management dokumentieren Falls Patches schon laufen: aufschreiben, mit Verantwortlichen und Frequenzen. Punkt 4: EDR ausrollen Microsoft Defender for Endpoint ist in vielen Microsoft-365-Plänen schon enthalten — aktivieren und konfigurieren lassen. Punkt 8: Mitarbeiter-Schulung planen Nicht aufschieben. Auch ein 60-Minuten-Termin mit Dokumentation der Teilnehmenden zählt. Punkt 7: Incident Response Plan schreiben Eine A4-Seite reicht: Wer ruft wen an, wenn etwas passiert. Drucken, an Empfang aufhängen.

MITTELFRISTIG — Monat 3 bis 6

Punkt 10: Netzwerk-Segmentierung
VLAN-Trennung von Druckern, Smartphones, IoT. Aufgabe für den IT-Betreuer.

Punkt 5: Vulnerability Scanning
Werkzeug auswählen (z.B. Nessus, OpenVAS) und Scan-Routine etablieren. Wer Schwachstellen nicht nur auflisten, sondern in realistischen Angriffspfaden bewerten will: AEGYS Pentest zeigt, was Angreifer in Ihrem Netzwerk tatsächlich erreichen könnten.

Punkt 6: PAM-Konzept
Klare Trennung von Standard- und Admin-Konten. Reduktion der Domain-Admins auf das absolute Minimum.

Punkt 11 + 12: Sichtbarkeit und Dokumentation
Hier kommt eine Lösung wie AEGYS Monitor ins Spiel: liefert kontinuierliche Sicht auf den Netzwerkverkehr und die Dokumentation, die Versicherer und Gerichte 2026 erwarten.

AUSWERTUNG

Was Ihre Antworten bedeuten

Zählen Sie nach: Bei wie vielen Punkten konnten Sie alle Prüf-Fragen mit Ja beantworten? Die Verteilung gibt eine grobe Einordnung der Risikolage Ihrer Kanzlei.

10 – 12 Punkte	Sehr gute Position. Sie sind technisch und organisatorisch gut aufgestellt. Die verbleibenden Punkte sollten dokumentiert und gelegentlich überprüft werden. Versicherungsanträge sollten für Sie problemlos abschließbar sein.
6 – 9 Punkte	Solide Basis, klare Lücken. Sie sind nicht ungeschützt, aber es gibt Bereiche, in denen Sie im Schadensfall verwundbar sind. Vor dem Versicherungs-Antrag sollten die offenen Punkte zumindest in einem dokumentierten Aktionsplan stehen.
3 – 5 Punkte	Erhöhte Risikolage. Eine Cyberversicherung wird unter diesen Bedingungen entweder abgelehnt oder mit erheblichen Einschränkungen angeboten. Wichtiger ist aber: Sie haben ein reales operatives Risiko, das vor allen anderen Schritten angegangen werden sollte.
0 – 2 Punkte	Akute Risikolage. Die Wahrscheinlichkeit eines Vorfalls ist hoch — und die Wahrscheinlichkeit, dass im Schadensfall keine Versicherung greift, ebenfalls. Ein offenes Gespräch mit dem IT-Betreuer ist heute wichtiger als der nächste Mandantenabschluss. Sofort-Maßnahmen aus der „Sofort"-Spalte sind unverzichtbar.

NÄCHSTE SCHRITTE

Wenn Sie Hilfe bei der Umsetzung brauchen

Die ersten zwei Punkte (MFA, Backup-Test) und der §203-Vertrag mit dem IT-Dienstleister sind Aufgaben, die Sie gemeinsam mit Ihrem IT-Betreuer in wenigen Tagen erledigen können. Bei Punkten 11 und 12 — kontinuierliche Sicht auf den Netzwerkverkehr und die dafür nötige Dokumentation — helfen wir gerne.

Was AEGYS liefert

AEGYS Monitor

BEOBACHTEN

Sicht auf den Netzwerkverkehr. Was Geräte in Ihrer Kanzlei tatsächlich kommunizieren — ohne Software-Installation, ohne Eingriff in DATEV.

Dokumentation für Versicherer. Die Nachweise, die im Antrag und im Schadensfall den Unterschied machen — strukturiert, jederzeit abrufbar.

Plug-and-Play. Sensor anschließen, Erstauswertung mit der Kanzleileitung, klare Empfehlungen — keine Folien.

Asset-basiertes Pricing. Typisch 100–300 EUR pro Monat für Steuerkanzleien.

AEGYS Pentest

ANGREIFEN

Bewiesene Angriffspfade. Autonomer Penetrationstest mit echten Angriffspfaden — ohne Skripte, ohne Disruption Ihres Tagesgeschäfts.

Realitäts-Check. Sie sehen, was Angreifer in Ihrem Netzwerk wirklich erreichen könnten — nicht nur, was theoretisch möglich wäre.

Priorisierte Empfehlungen. Konkrete Maßnahmen nach tatsächlichem Risiko sortiert — kein Bericht, der unbearbeitet im Regal liegt.

Pricing. Einmalig zur Erstaufnahme oder als laufende Subscription. Auf Anfrage.

15-MINUTEN-ERSTGESPRÄCH

Sehen, was passiert.
Und was passieren könnte.

Kein Sales-Call. Wir gehen die 12 Punkte mit Ihnen durch und sagen ehrlich, wo Sie stehen — und ob AEGYS Monitor oder AEGYS Pentest für Ihre Situation Sinn ergibt.

Erstgespräch vereinbaren →

hallo@aegysdata.com

KONTAKT

AEGYS DATALYTICS AG
Berg am Starnberger See, Bayern

hallo@aegysdata.com
www.aegysdata.com

WEITERFÜHRENDE LEITFÄDEN

DATEV-Sicherheit für Steuerkanzleien →

§203 StGB für Steuerberater →

Cyberversicherung 2026 →

QUELLEN

BSI-Lagebericht zur IT-Sicherheit in Deutschland 2025 · BSI IT-Grundschutz-Kompendium · CyberDirekt Marktanalyse 2024 · Munich Re Cyber Insurance Risk Survey 2026 · Hiscox Cyber Readiness Report 2025 · MRTK Cyber-Monitor 2025 · §203 StGB, §22 VVG, §62a StBerG · Bitkom Wirtschaftsschutzstudie 2025