WHITEPAPER

Versichert heißt nicht abgesichert!

Eine Cyberversicherung stoppt keine Cyberangriffe.

ESET Made in EU IT-Security

ESET Cybersecurity
Progress. Protected.

Inhaltsverzeichnis

Autor: Ildikó Bruhns, ESET Deutschland GmbH

Stand: September 2025

Cybersecurity
Progress. Protected.

01 SICHERHEIT BEGINNT VOR VERSICHERUNG

Eine Cyberversicherung allein schützt Unternehmen nicht

Eins vorweg: Wer glaubt, eine Cyberversicherung hilft, sich gegen Hacker zu schützen, täuscht sich leider. Sie ist kein Abwehrschild gegen Angriffe, sondern ein Weckruf. Sie zeigt klar, wo die IT-Sicherheitslücken im eigenen Unternehmen liegen – vom schwachen Passwort über ungesicherte Backups bis hin zu fehlenden Erkennungsmechanismen für Angriffe.

Noch vor wenigen Jahren waren Cyberversicherungen ein Nischenprodukt. Die Nachfrage wächst jährlich, doch aktuell gibt es keinen gesetzlichen Zwang in Deutschland für den Abschluss einer Cyberversicherung, wie es etwa bei Kfz-Versicherung der Fall ist. In manchen Branchen (z. B. kritische Infrastrukturen, Finanzdienstleister, Gesundheitswesen) wird eine Cyberversicherung allerdings quasi zur Pflicht, weil Auftraggeber, Investoren oder Aufsichtsbehörden den Nachweis einer Cyberversicherung verlangen oder sie als Teil der Risikostrategie voraussetzen. Im Gegensatz zu den vergangenen Jahren fordern heutige Policen immer häufiger ein ganzheitliches IT-Sicherheitskonzept von Unternehmen, in dem sie präventive Maßnahmen nachweisen müssen – von starken Authentifizierungen über Backups bis hin zu Monitoring-Systemen.

Auch in Lieferketten wird sie immer öfter vertraglich vorgeschrieben – etwa wenn ein Unternehmen IT-Dienstleister oder Zulieferer verpflichtet, Cyberversicherung nachzuweisen.

„Vor allem kleinere Unternehmen sind sich immer noch nicht bewusst, dass sie ein digitales Geschäftsmodell haben. Jeder Friseur, Zahnarzt oder Anwalt nutzt heutzutage Technologien in moderner Büroausstattung und sie sind viel abhängiger davon, als sie glauben."

— Maik Wetzel,
Strategic Business Development Director,
ESET Deutschland GmbH

Denn IT Security-Spezialisten haben verstärkt alle Hände voll zu tun. Unabhängig von Größe und Branche werden Unternehmen und Organisationen immer häufiger Ziel von Cyberangriffen. Vor diesem Hintergrund denken Entscheider an eine Cyberversicherung. Sie glauben, im Falle eines Angriffs würden sie die finanziellen Kosten für Betriebsausfall, die Wiederherstellung ihrer Daten, Schadensersatzansprüche von Kunden oder Partnern und ggf. Lösegeldzahlungen ausgleichen. Viele haben die (falsche) Vorstellung, dass sie eine Art „Rundumschutz" ist, der automatisch alle Risiken abdeckt. Dafür gibt es mehrere Gründe:

1. **Sicherheitsgefühl durch Versicherung**
   Eine Cyberversicherung kann ein Gefühl der Absicherung vermitteln, vergleichbar mit einem sogenannten Notfallkonzept – sie ersetzt jedoch keine aktiven Schutzmaßnahmen.

2. **Fehlendes Bewusstsein für Prävention**
   Cyberversicherungen decken in der Regel Folgeschäden ab, wie Betriebsunterbrechungen, Rechtskosten oder Lösegeldzahlungen (je nach Vertrag). Sie verhindern allerdings keinen Angriff. Unternehmen verstehen häufig nicht, dass Prävention deutlich günstiger und effektiver ist als die reine Schadensregulierung.

3. **Marketing der Versicherer**
   Manche Versicherungen kommunizieren in der Öffentlichkeit stark die finanziellen Absicherungen und weniger die Notwendigkeit von technischen Schutzmaßnahmen, was bei Entscheidern den Eindruck erweckt, dass Cybersecurity zweitrangig ist.

4. **Komplexität von IT-Sicherheit**
   IT-Sicherheit ist technisch und organisatorisch vielschichtig und kann schnell unübersichtlich werden. Viele Unternehmen versuchen, diese Anforderungen auszulagern oder glauben, Risiken einfach „einkaufen" zu können, ohne selbst in Cybersicherheit investieren zu müssen. Eine Versicherung erscheint als vermeintlich einfachste Lösung.

5. **Kulturelles Missverständnis**
   In einigen Branchen herrscht die Einstellung: „Wir haben das Geld für den Fall des Falles – alles gut." Das ist allerdings gefährlich, weil ein Sicherheitsvorfall nicht nur finanzielle Kosten verursacht, sondern häufig auch Datenverlust, regulatorische Konsequenzen und vor allem Rufschädigung nach sich zieht, die besonders schwer zu beheben ist.

Versicherer als Treiber und Risiko zugleich

Cyberversicherer sind längst nicht mehr nur finanzielle Rettungsanker, die im Schadenfall einspringen. Mittlerweile verstehen sich Versicherer als Impulsgeber für die kontinuierliche Verbesserung der Sicherheitslage. Studien und Branchenanalysen wie Allianz Risk Barometer zeigen, dass Cyberangriffe mittlerweile als Top-Risiko eingestuft werden. Viele Cbyerversicherer, aber auch Regulierer, schieben deshalb die Entwicklung immer mehr in Richtung „Pflichtbestandteil im Risikomanagement". So wird das Sicherheitsniveau in Unternehmen neben gesetzlichen Regulierungen durch Versicherungsdruck gestützt: Unternehmen haben ihre IT-Security verbessert, weil es eine zwingende Voraussetzung für Versicherungsschutz war.

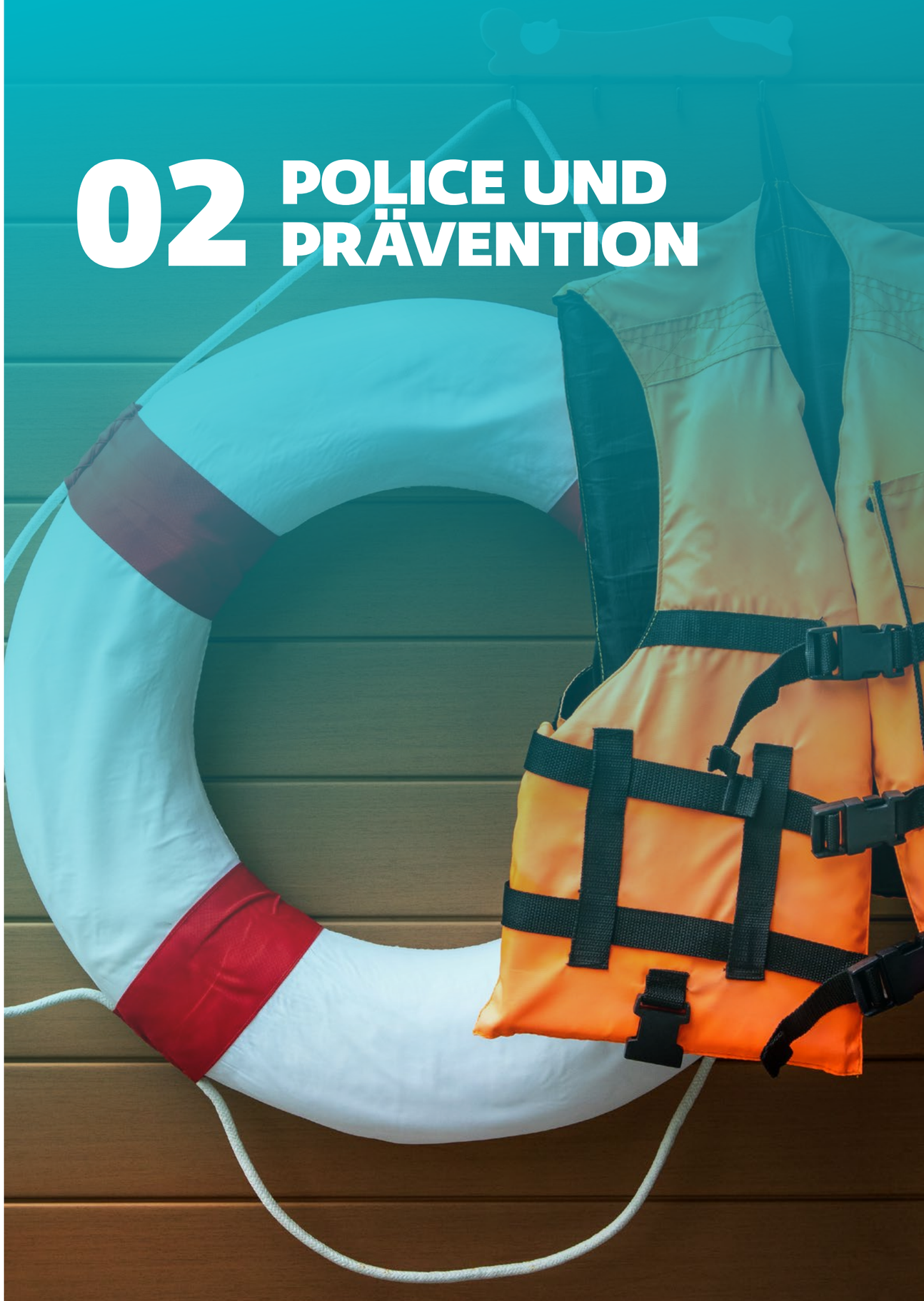
Über Partnerschaften mit Security-Anbietern und empfohlene Tools (z. B. für Schwachstellen-Management oder Angriffssurface-Monitoring) erleichtern sie Unternehmen den Versicherungsschutz und fördern Investitionen in geeignete Technologien. Besonders für kleine und mittelständische Unternehmen bedeutet dies: weniger Aufwand, ein zentral koordinierter Schutz – quasi Versicherung und Sicherheit aus einer Hand. So entwickeln sich die Anbieter von reinen Absicherern zu aktiven Antreibern von Investitionen in IT-Sicherheit und nehmen maßgeblichen Einfluss darauf, welche Technologien eingesetzt werden.

Doch diese Entwicklung birgt Risiken. Wenn viele Versicherte auf dieselben Schutzlösungen setzen, entsteht eine „Cybersicherheits-Monokultur" - mit dem gefährlichen Effekt, dass bei erfolgreichem Angriff auf eine weit verbreitete Lösung viele Unternehmen gleichzeitig betroffen sein können."

„Viele Unternehmen glauben noch, dass eine Cyberversicherung im Ernstfall einfach so sämtliche Kosten deckt – von Betriebsausfall über Datenwiederherstellung bis hin zu Schadensersatz oder Lösegeld. Dabei wird oft übersehen, dass Versicherer hierfür IT-Sicherheitsanforderungen zur Voraussetzung machen und diese erfüllt sein müssen, um im Schadensfall abgesichert zu sein."

— Dr. Jens Eckhardt, pitc legal Eckhardt Rechtsanwälte

02 POLICE UND PRÄVENTION



Ohne IT-Sicherheit keine Police

Was viele Unternehmen immer noch übersehen ist, dass Versicherer mit Blick auf die wachsende Bedrohungslage ihre Leistungen an klare Mindeststandards in der IT-Sicherheit knüpfen. Sie verlangen Nachweise für Prävention, Monitoring und Notfallpläne. Und genau das sind aber auch die zentralen Bausteine jeder wirksamen IT-Sicherheitsstrategie. Wer die Standards nicht erfüllt, steht im Ernstfall trotz Police im Regen, vorausgesetzt, er bekommt überhaupt eine.

An dieser Stelle zeigt sich zugleich die enge Beziehung zwischen beiden Bereichen: IT-Sicherheit und Cyberversicherungen sind keine zwei abgeschlossenen Bereiche – im Gegenteil: Sie sind komplementär und eng miteinander verzahnt. Sie bedingen einander, denn die Bedeutung von Cyberversicherungen wächst parallel zur steigenden Komplexität der IT-Sicherheitslandschaft und der zunehmenden Gefahren durch Cyberangriffe.

Aus Sicht eines IT-Security-Herstellers ist eine Cyberversicherung für Unternehmen nur ein Teil der Lösung. Eine Police hilft, finanzielle Schäden abzufedern, aber nicht, die Gefahr zu beseitigen. Wer wirklich abgesichert und nicht nur versichert sein will, muss die IT-Strukturen analysieren, Schwachstellen schließen und Abläufe überwachen. In der Praxis ergeben sich vielfältige Schnittstellen und Chancen, die Schutzlevel von Unternehmen nachhaltig zu verbessern und die Versicherbarkeit zu erhöhen.

In diesem Sinne sollte eine Cyberversicherung im besten Fall als Katalysator für Prävention und Risikobewusstsein sowie strategische Ergänzung verstanden werden. Denn die Versicherungsnehmer prüfen in der Regel die IT-Infrastruktur, Prozesse und Sicherheitsmaßnahmen eines Unternehmens, bevor eine Police abgeschlossen werden kann. Dadurch werden Schwachstellen sichtbar, die sonst möglicherweise unentdeckt geblieben wären.

Fundament

IT-Sicherheit

Ohne funktionierende Schutzmaßnahmen kein Versicherungsschutz

Sicherheitsnetz

Cyberversicherung

Sie springt ein, wenn trotz aller Maßnahmen ein Angriff erfolgreich ist und finanzielle Schäden entstehen

Beziehungsstatus: Voll vernetzt

Kurz gesagt: IT-Sicherheitsmaßnahmen reduzieren Risiken, Cyberversicherungen schützen vor finanziellen Schäden. Für Unternehmen können beide Branchen ein effektives Schutzsystem bilden, bei dem die eine Disziplin die andere ergänzt:

1. **Prävention trifft Versicherung**
   IT-Sicherheit sorgt dafür, dass Unternehmen Risiken minimieren, indem sie technische, organisatorische und personelle Schutzmaßnahmen einbetten.

   Cyberversicherungen decken die finanziellen Folgen von Sicherheitsvorfällen ab, ersetzen aber keine Präventionsmaßnahmen.

Beziehungsstatus: Interessengemeinschaft
Cyberversicherung greift dort, wo Restrisiken bestehen bleiben – durch finanzielle Absicherung im Falle eines Abwehrversagens. Beide wirken an unterschiedlichen Stellen der Bedrohungskette und ergänzen sich so zu einer ganzheitlichen Schutzstrategie.

2. **Risikotransparenz und Datengrundlage**
   Cyberversicherer verlangen genaue Informationen über IT-Systeme, Prozesse und Sicherheitsmaßnahmen.

   Diese Daten helfen Versicherern wiederum, Risiken zu bewerten und Policen zu gestalten. Gleichzeitig erkennen Unternehmen dadurch, wo ihre Sicherheitslücken liegen.

Beziehungsstatus: Strategische Allianz
IT-Security liefert die Grundlage für die Versicherungsbewertung und Versicherungen schaffen Anreize zur Verbesserung der Sicherheitslage.

3. **Kosten-Nutzen-Synergie**
   Mit unzureichender IT-Sicherheit steigen Schadenswahrscheinlichkeit und Versicherungsprämien.

   Je umfangreicher der Schutz und weniger Risiken, umso kleiner die Premium und erweiterter die Abdeckungen.

Beziehungsstatus: Zweckgemeinschaft
Versicherungsbranche und Cybersicherheitsbranche arbeiten zusammen, um finanziellen Schaden zu begrenzen und gleichzeitig IT-Schutzstandards zu erhöhen.

4. **Strategische Partnerschaft**
   Cyberversicherer bieten Beratung, Risikobewertung und haben Kenntnisse zu Cyberbedrohungen.

   IT-Sicherheit integriert technologische Schutzmaßnahmen, Monitoring und Awareness-Programme.

Beziehungsstatus: Partner with Benefits
Gemeinsam schaffen sie ein „Doppelpaket" aus Schutz, Prävention und finanzieller Absicherung – ähnlich wie Sicherheitsgurte plus Unfallversicherung beim Auto.

5. **Zukunftsperspektive**
   Mit zunehmender Digitalisierung, Cloud-Nutzung und KI-basierten Angriffen bestehen Cyberversicherer vermehrt auf den Einsatz präventiver Schutzmaßnahmen. Sie werden immer häufiger Voraussetzung für Versicherungsabschlüsse, nicht nur Boni.

Beziehungsstatus: Erfolgsteam
Die Versicherungsbranche treibt insofern indirekt die Sicherheitsstandards in der Wirtschaft voran.

Synergien zwischen
Cybersicherheit und Cyberversicherungen

Die Verzahnung von Cybersicherheit und Cyberversicherungen führt zu strategischen und operativen Vorteilen: Unternehmen werden besser vor digitalen Bedrohungen geschützt, Hersteller können ihre Lösungen kontinuierlich verbessern und insgesamt entsteht eine resilientere Cybersicherheitslandschaft.

Vorteile für Cyberversicherer durch die Zusammenarbeit mit IT-Sicherheitsherstellern

1

Reduziertes Schadensrisiko: Durch den Einsatz von fortschrittlichen Sicherheitslösungen bei versicherten Unternehmen können potenzielle Schäden durch Cyberangriffe signifikant reduziert werden. Beispielsweise ermöglichen moderne Technologien zur Gefahrensuche und -abwehr wie Endpoint-Protection oder Intrusion Detection Systeme eine frühzeitige Erkennung von Angriffen, bevor sie zu teuren Schadensfällen führen.

2

Verbesserte Risikobewertung: Hersteller geben Tools, Benchmarks und Analysen an die Hand, mit deren Hilfe Unternehmen und Cyberversicherer den Sicherheitsstatus dank detaillierter Risikoanalyse einschätzen können. So lassen sich Prämien besser kalkulieren und gleichzeitig Anreize für höhere Sicherheitsstandards schaffen.

3

Entwicklung neuer Versicherungsprodukte: Die Zusammenarbeit ermöglicht es Versicherern, Policen zu entwickeln, die speziell auf bestimmte Technologien oder Sicherheitslösungen zugeschnitten sind. Beispiele sind Versicherungslösungen, die nur Unternehmen abdecken, die bestimmte Compliance- oder Sicherheitsstandards einhalten, oder Policen für Unternehmen mit Managed Security Services.

4

Stärkung der Kundenbindung: Durch integrierte Angebote, bei denen Sicherheitslösungen und Versicherungen kombiniert werden, können Versicherer ihren Kunden einen klaren Mehrwert bieten. Kunden profitieren von einem ganzheitlichen Schutzkonzept, was die Loyalität erhöht und die Abwanderung reduziert.

5

Förderung proaktiver Sicherheitsmaßnahmen: Die enge Zusammenarbeit mit IT-Sicherheitsherstellern motiviert Versicherungsnehmer, kontinuierlich in Sicherheitsmaßnahmen zu investieren. Dies reduziert nicht nur das Risiko von Schadensfällen, sondern verringert das Gesamtrisiko des Versicherers, was zu günstigeren Konditionen und stabileren Policen führen kann.

Vorteile für Hersteller von IT-Sicherheitslösungen

03 VON RISIKEN ZU ANFORDERUNGEN

Cyberrisiken: Tendenz steigend

Ransomware, Phishing, Datendiebstahl: Cyberversicherer haben auf die Bedrohungslage reagiert und hochentwickelte Risikobewertungen etabliert, die Unternehmensgröße, Branche und das IT-Schutzniveau berücksichtigen. Die Policen sind spezialisierter denn je und decken gezielt überlebenswichtige Bereiche eines Unternehmens ab wie Betriebsunterbrechungen, Datenschutzverletzungen, Rechtsstreitigkeiten oder auch PR-Kosten, zur Wiederherstellung des geschädigten Rufs.

Entgegen der weit verbreiteten Annahme sind viele Datenpannen nicht auf böswillige Absichten zurückzuführen. Eine aktuelle globale Studie des Ponemon Institute zeigt: 55 Prozent der Cybervorfälle entstehen durch Fahrlässigkeit von Mitarbeitenden. Die durchschnittlichen jährlichen Kosten zur Eindämmung solcher Vorfälle beliefen sich 2023 auf 7,2 Millionen US-Dollar. Das ist zehnmal höher als die durchschnittlichen Kosten zur Behebung schädlicher unternehmensinterner Angriffe (Quelle: Ponemon Insider Risks Global Report 2023).

Nicht-böswillige Schäden entstehen durch Fahr- oder Nachlässigkeit, z. B.:

- Versand sensibler Daten an unbefugte Empfänger
- unsachgemäße Entsorgung vertraulicher Dokumente
- unachtsames Klicken auf Links in Phishing-Mails
- das Wiederverwenden unsicherer Passwörter
- versäumte Software-Updates
- das Speichern sensibler Daten auf unverschlüsselten USB-Sticks, die verloren gehen

Cybersecurity-Analysten erwarten, dass der Einsatz von KI die Anzahl von Spear-Phishing-Angriffen weiter erhöhen wird. Da soziale Medien Informationen über Arbeitsplätze, Jobs, Freunde und Interessen liefern, können KI-Systeme diese Daten nutzen. So lassen sich täuschend echte und personalisierte E-Mails erstellen, die gezielt an Personen in wichtigen Unternehmenspositionen gesendet werden.

„Ransomware war der größte Katalysator für den Anstieg der Schadensmeldungen und machte 19 % aller gemeldeten Fälle aus. Ansprüche im Zusammenhang mit Überweisungsbetrug blieben stabil bei 28 %, hingegen sank der Anteil von Business Email Compromise (Bec) auf 28 %.“

— Quelle: Cyber Claims Report 2024 von Coalition

Hier finden Sie
↗weiterführende
Informationen.

Mindestanforderungen

der Versicherer an die IT-Sicherheit

Mit der Zunahme von Cyberangriffen, insbesondere Ransomware und KI-gestützten Angriffen, steigen die Risiken für Versicherer. Dies führt zu höheren Prämien, strengeren Anforderungen an Sicherheitsmaßnahmen und gezielteren Policen mit Risikobegrenzungen. Die unten aufgezahlten Anforderungen stellen grobe Vorgaben dar, die je nach Unternehmensgröße, Branche und Risikoprofil und auch im Laufe der Zeit variieren können. Bis dato gibt es keinen einheitlich gültigen Standard.

Eine Checkliste mit den verschiedenen technischen, organisatorischen und branchenspezifischen Anforderungen finden Sie im Anhang.

- **Virenschutz und Firewalls:** Grundlegende Schutzmaßnahmen gegen Malware und unbefugte Zugriffe.
- **Regelmäßige Datensicherung:** Sicherungskopien von Daten, um im Falle eines Vorfalls eine Wiederherstellung zu ermöglichen.
- **Aktualisierung von Software und Systemen:** Sicherstellung, dass alle Systeme auf dem neuesten Stand sind, um bekannte Sicherheitslücken zu schließen.
- **Schulung der Mitarbeitenden:** Sensibilisierung der Belegschaft für Sicherheitsrisiken und bewährte Sicherheitspraktiken.
- **Dokumentierte Sicherheitsrichtlinien:** Festlegung von Sicherheitsstandards und -verfahren im Unternehmen.
- **Identitäts- und Zugriffssicherheit:** Absicherung sensibler Zugänge, etwa per Mulit-Faktor-Authentifizierung plus strenge Passwortregeln hinsichtlich Länge und Komplexität
- **Governance & Compliance:** Benennung eines Datenschutzbeauftragten (intern oder extern) sowie verbindliche Datenschutzrichtlinien

Zusätzliche Maßnahmen

für die Industrie/kritische Infrastruktur

- Einsatz von Systemen zur Angriffserkennung (SIEM, EDR, XDR)
- Entwicklung und Pflege von Business Continuity Plänen, einschließlich definierter Prozesse bei Sicherheitsverletzungen
- Durchsetzung von Sicherheitsstandards auch bei externen Dienstleistern (Lieferkette)
- Durchführung von Schwachstellenanalysen und Penetrationstests
- Klare Regeln zur Nutzung privater Geräte und physischer Schutz der IT-Infrastruktur
- Einsatz eines eigenen IT-Sicherheitsbeauftragten
- Netzwerksegmentierung (z. B. Trennung Büro- und Produktionsnetzwerke)
- Verschlüsselung von Endgeräten

Für Unternehmen in der Industriebranche gibt es spezifische Standards und Normen, die über die allgemeinen IT-Sicherheitsanforderungen hinausgehen:

- **IEC 62443:** Eine internationale Normenreihe, die Anforderungen an die IT-Sicherheit in industriellen Automatisierungs- und Steuerungssystemen stellt. Sie umfasst sowohl technische als auch organisatorische Maßnahmen zur Risikominimierung.
- **DIN SPEC 27076:** Diese Spezifikation bietet einen strukturierten Ansatz zur Durchführung von Cyber-Risiko-Checks in Unternehmen, insbesondere für kleine und mittlere Unternehmen. Sie beinhaltet Leitfragen zu Themen wie Patch-Management, Datensicherung und Zugangskontrollen.
- **BSI-Standards:** Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet mit dem IT-Grundschutz-Kompendium und spezifischen Standards wie BSI-Standard 200-4 (Business Continuity Management) praxisnahe Leitlinien zur Umsetzung von Informationssicherheits-Managementsystemen (ISMS).

Diese Maßnahmen dienen nicht nur dem Schutz vor Cyberangriffen, sondern auch der Erfüllung der Anforderungen von Versicherern und Regulierungsbehörden. Unternehmen, die diese Standards nicht erfüllen, riskieren im Schadensfall eine Ablehnung der Versicherungsleistung.

Regulatorische Vorgaben legen Messlatte
an Unternehmen und Cyberversicherer höher

Gesetze wie DSGVO, NIS2 und DORA haben die Spielregeln für Unternehmen in Sachen IT-Sicherheit und Cyberversicherung um ein Vielfaches verschärft. Sie definieren nicht nur Mindeststandards für den Schutz von Daten und kritischen IT-Systemen, sondern auch konkrete Pflichten bei Cybervorfällen. Für Versicherer sind diese Standards für den Abschluss einer Cyber-Police inzwischen entscheidend: Wer die Vorgaben nicht erfüllt, läuft Gefahr, im Schadenfall nicht abgesichert zu sein.

NIS2 (Netzwerk- und Informationssicherheit)

- Neue Mindeststandards: Die NIS2-Richtlinie verlangt von Unternehmen aus kritischen Bereichen umfassende Cyber-Sicherheitsmaßnahmen wie Risikomanagement, Lieferkettenkontrolle und Vorfallmeldung innerhalb von 24 Stunden – das ist kein Bonus, sondern Pflicht.
- Versicherungsrelevante Auswirkungen: Unternehmen, die diese Vorgaben erfüllen, gelten als „versicherbar". Versicherer nutzen NIS2 als Maßstab, um Risikoanalysen durchzuführen – Compliance-Punkte sind dabei wertvolle Argumente bei der Prämienfindung.
- Erfahren Sie hier, welche ↗Technologien von ESET Sie zur Umsetzung von NIS2 einsetzen können.

DORA (Digital Operational Resilience Act)

- Regelwerk für den Finanzsektor: DORA richtet sich an Banken und Finanzdienstleister. Sie müssen systematisch IT-Risiken managen, Vorfälle melden, Tests durchführen und Drittanbieter eng überwachen – verbindlich ab 2025.
- Brancheneinfluss: Versicherer werden selbst von DORA erfasst und müssen ihre eigene Cyber-Resilienz nachweisen. Gleichzeitig verlangen sie von Versicherungsnehmern ähnliche Maßnahmen – ein gegenseitiger Hebel.

DSGVO (Datenschutz-Grundverordnung)

- Meldepflichten und Sanktionen: Unternehmen müssen Datenschutzpannen schnell melden (innerhalb von 72 Stunden) – Verstöße können empfindliche Bußgelder zur Folge haben.
- Nutzen für Versicherer: Standardisierte Meldungen (Templates von Insurance Europe) verbessern unternehmensübergreifende Risikodaten und erlauben fundiertere Policen und Risikomodelle.

Cyber Resilience Act (CRA)

- Regelwerk für Hersteller: Der CRA ist eine EU-Verordnung, die verbindliche Cybersicherheitsanforderungen für Produkte mit digitalen Komponenten (Hardware und Software) einführt. Hersteller müssen Sicherheit über den gesamten Produktlebenszyklus nachweisen — von der Entwicklung bis zur Wartung. Dazu zählen regelmäßige Updates, klare Dokumentationspflichten, Risikobewertungen und Meldepflichten bei Schwachstellen.
- Nutzen für Cyberversicherer: CRA-konforme Produkte bieten ein höheres Sicherheitsniveau. Durch die Vorgaben verschieben sich Verantwortlichkeiten: Neben Kunden müssen auch Hersteller Sicherheit technisch nachweisen. Versicherer können CRA-konforme Produkte als Risikominderung werten und so Policen oder Prämien differenzieren.

Cybersecurity Act

- Regelwerk für Zertifizierungen: Der EU-Cybersecurity Act (Verordnung (EU) 2019/881) stärkt die Agentur ENISA und etabliert ein einheitliches Zertifizierungsrahmenwerk für Cybersecurity-Dienstleistungen und -Produkte in der EU.
- Einfluss auf die Versicherungswelt: Einheitliche Zertifizierungen schaffen klare Bewertungsmaßstäbe für Versicherer, die Sicherheitsprodukte und -services absichern oder als Compliance-Bilanz betrachten. Zertifizierte IT-Sicherheitslösungen bieten Versicherern Sicherheit bei der Risikoeinschätzung und können zu besseren Konditionen führen.

Versicherungsaufsichtliche Anforderungen an die IT (VAIT)

Diese Anforderungen der BaFin richten sich an Versicherungsunternehmen und beinhalten Vorgaben zu IT-Governance, Risikomanagement und Sicherheitsmanagement.

Praxisbeispiele, wie Versicherer regulatorische Anforderungen prüfen

Regulierung

(NIS2, DORA, DSGVO) zwingt Unternehmen zu strukturiertem IT-Risikomanagement und erhöht das Mindestniveau, das Unternehmen erreichen müssen.

Gegenseitige Verstärkung

Unternehmen geraten doppelt unter Druck – von der Pflichtseite (Regulatorik) und von der Marktseite (Versicherungsschutz).

Versicherer

nutzen diese Anforderungen als Basis für ihre Risikoeinschätzungen und Prämiengestaltung (z. B. Compliance-Nachweise, Penetration Testing, Logging-Systeme). Versicherungen verlangen sogar oft noch mehr, weil sie ihr eigenes Risiko minimieren wollen.

1. **Patchmanagement und Software-Updates:**
   - Versicherer prüfen, ob Unternehmen regelmäßig Sicherheitsupdates auf Servern, Arbeitsplatzrechnern und Netzwerkgeräten durchführen.
   - Beispiel: Ein Finanzdienstleister, der DORA-konform ist, muss dokumentieren, wann Updates eingespielt wurden und wie Schwachstellen priorisiert werden. Ein Verstoß kann nicht nur zu aufsichtsrechtlichen Strafen, sondern auch zur Ablehnung einer Schadensmeldung führen.
2. **Multi-Faktor-Authentifizierung (MFA):**
   - NIS2 verlangt angemessene Zugriffskontrollen. Versicherer erwarten MFA für alle kritischen Systeme.
   - Beispiel: Ein Energieversorger, der kritische Infrastruktur betreibt, muss sicherstellen, dass sowohl interne Mitarbeitende als auch externe Dienstleister über MFA auf Steuerungssysteme zugreifen.
3. **Backup-Strategien und Wiederherstellung:**
   - DSGVO und NIS 2 fordern die Sicherstellung der Datenintegrität und Wiederherstellung im Notfall.
   - Beispiel: Ein Mittelstandsunternehmen dokumentiert regelmäßige Backups und Testläufe der Wiederherstellung. Ohne Nachweis wird ggf. nur ein Teil des Schadens zu übernommen.
4. **Schulungen und Awareness:**
   - Versicherer erwarten, dass Angestellte für Phishing, Social Engineering und Datensicherheit sensibilisiert werden.
   - Beispiel: Ein Softwareunternehmen führt quartalsweise Security-Awareness-Trainings durch. Versicherer werten dies als Reduktion des Risikos menschlicher Fehler, die immerhin laut Ponemon Institute über 50 % aller Cybervorfälle ausmachen.
5. **Notfall- und Krisenpläne:**
   - DORA und NIS2 schreiben Incident-Response-Pläne vor. Versicherer prüfen, ob Unternehmen wissen, wer im Fall eines Angriffs Entscheidungen trifft, wie Systeme isoliert werden und wie Kommunikation mit Kunden und Partnern erfolgt.

Regulierung und Cyberversicherung sind heute eng verzahnt. Wer die Vorgaben ernst nimmt, erhöht die Resilienz seines Unternehmens, mindert Schadensrisiken und sichert gleichzeitig seine Versicherungsansprüche. Wer sie ignoriert, riskiert nicht nur Bußgelder und Imageschäden, sondern im Ernstfall auch den Verlust des Versicherungsschutzes. Ein Unternehmen, das im Jahr 2023 oder zuvor eine Cyberversicherung erhalten hat, aber grundlegende Sicherheitspraktiken nicht umgesetzt hat, würde heute mit hoher Wahrscheinlichkeit keine Versicherung mehr bekommen. Die Anforderungen der Versicherer sind gestiegen, und die Umsetzung grundlegender Sicherheitsmaßnahmen ist Voraussetzung für den Erhalt einer Police.

Hinweis: Unternehmen sollten bei der Beantwortung von Risikofragen im Rahmen des Versicherungsabschlusses sorgfältig und wahrheitsgemäß vorgehen, um spätere, teure Rechtsstreitigkeiten zu vermeiden.

Wie Cyberversicherer
das Sicherheitsniveau von Unternehmen prüfen

Versicherer erwarten heute ein ganzheitliches Schutzkonzept, das nicht nur Technologie, sondern auch Organisation, Mitarbeitende und Lieferketten abdeckt. Mit Fragen dieser Art prüfen Versicherer heute, ob ein Unternehmen überhaupt versicherbar ist und wie hoch die Prämie ausfällt.

- Haben Sie ein Notfallwiederherstellungsprogramm?
- Haben Sie ein Backup-Programm? Testen Sie es regelmäßig?
- Machen Sie Offsite-Backups?

Incident Response & Meldungen

- Gibt es ein Verfahren für den Umgang mit Cyberangriffen (inkl. Meldung an Aufsichtsbehörden/Kunden)?
- Wie lange dauert es, um Beteiligte über eine Datenpanne zu informieren?
- Haben Sie einen Disaster Recovery Plan (DRP) für den Wiederanlauf von IT-Systemen?

Technische Sicherheitsmaßnahmen

- Haben Sie ein Programm für das Patch-Management?
- Sind kritische Systeme isoliert und abgesichert?
- Verschlüsseln Sie Daten im Ruhezustand und/oder bei der Übertragung?

Monitoring & Protokollierung

- Überwachen und verwalten Sie Sicherheitsereignisprotokolle?
- Gibt es eine zentrale Erfassung und Auswertung sicherheitsrelevanter Ereignisse?

Change- & Configuration Management

- Haben Sie ein Programm für das Änderungsmanagement?
- Wie sieht Ihr Prozess für Notfalländerungen aus?

Schwachstellenmanagement & Testing

- Führen Sie regelmäßige Schwachstellenbewertungen durch?
- Führen Sie regelmäßige Penetrationstests durch?
- Gibt es ein geregeltes Verfahren für zeitnahe Updates & Notfall-Patches?

Compliance & Datenschutz

- Sind Sie mit Datenschutzvorgaben wie der DSGVO konform?
- Sind Richtlinien für IT-Sicherheit und Datenschutz verbindlich dokumentiert und allen Mitarbeitenden zugänglich?
- Werden interne Audits oder externe Zertifizierungen regelmäßig durchgeführt?

Awareness & Training

- Haben Sie ein Programm zur Sensibilisierung und Schulung in Cybersicherheit?

Physische Sicherheit

- Haben Sie ein Programm und eine Richtlinie für die physische Sicherheit?
- Gibt es Zugangskontrollen zu Serverräumen & Rechenzentren?
- Gibt es Notfallkonzepte für Stromausfall, Feuer, Umweltkatastrophen?

Third-Party Risk Management

- Haben Sie ein Programm für das Management von Drittanbieterrisiken?

04 CYBERVER-SICHERUNGEN IN ZEITEN VON KI & BIG DATA

Von individuellen Risiken zu gemeinsamer Resilienz

1. Gemeinsame Risikobewertung und -minderung

Für Cyberversicherer wächst die Bedeutung präziser Risikobewertungen, um Policen individuell und fair zu gestalten. IT-Sicherheitsanbieter können diesen Prozess unterstützen, indem sie detaillierte, KI-gestützte Sicherheitsanalysen, Reports und Monitoring-Tools bereitstellen, die Schwachstellen transparent machen und Prioritäten für Gegenmaßnahmen aufzeigen.

2. Integration von Sicherheitslösungen und Versicherungsprodukten

Immer mehr Unternehmen werden auf ganzheitliche Lösungen setzen, die IT-Sicherheitsdienstleistungen und Cyberversicherung kombinieren. So lassen sich Managed Security Operations Center (SOC) mit Versicherungsleistungen koppeln: Der IT-Sicherheitshersteller liefert die kontinuierliche Überwachung, Schwachstellenanalyse und Bedrohungserkennung, während die Versicherung im Ernstfall finanzielle Risiken abdeckt.

„Die zukünftige Zusammenarbeit zwischen IT-Sicherheitsherstellern und Cyberversicherungen wird durch technologische Integration, gemeinsame Standards und politische Unterstützung geprägt sein. Diese Synergien bieten Unternehmen einen umfassenderen Schutz vor Cyberbedrohungen und stärken die Resilienz gegenüber digitalen Risiken.“

— Maik Wetzel,
Strategic Business Development Director,
ESET Deutschland GmbH

3. Nutzung von KI und Automatisierung

Künstliche Intelligenz (KI) und maschinelles Lernen ermöglichen heute schon Echtzeiterkennung von Bedrohungen, automatische Reaktionen und eine kontinuierliche Verbesserung der Sicherheitslage. Kunden werden proaktiv geschützt, Sicherheitslücken frühzeitig identifiziert und die Effizienz der Sicherheitsmaßnahmen deutlich gesteigert. Versicherer profitieren von diesen Technologien, indem sie präzisere Risikobewertungen erstellen, sofortige Meldungen erhalten und das Schadenspotenzial schneller einschätzen können.

4. Entwicklung gemeinsamer Standards und Zertifizierungen

Die Einführung einheitlicher Sicherheitsstandards und Zertifizierungen kann die Zusammenarbeit zwischen IT-Sicherheitsherstellern und Versicherern erleichtern. Solche Standards würden es ermöglichen, Sicherheitsniveaus klar zu definieren und die Versicherbarkeit von Unternehmen transparenter zu gestalten.

5. Förderung durch politische Initiativen

Regulatorische Maßnahmen wie die NIS2-Richtlinie der EU setzen neue Mindestanforderungen an die IT-Sicherheit von Unternehmen. Diese regulatorischen Vorgaben fördern die Zusammenarbeit zwischen Sicherheitsanbietern und Versicherern, indem sie klare Rahmenbedingungen schaffen.

Cyberversicherungen
im Wandel

Zukünftige Cyberversicherungen werden technologiegetriebener, interaktiver und stärker auf individuelle Risiken zugeschnitten sein.

Echtzeitüberwachung und dynamische Prämien

Ein denkbarer nächster Schritt ist die Nutzung von Dashboards oder Apps, die den aktuellen Sicherheitsstatus eines Unternehmens transparent abbilden. Versicherer könnten auf dieser Basis Risiken frühzeitig erkennen und Unternehmen gezielt beraten. Auch dynamische Anpassungen von Prämien sind möglich: Sie könnten steigen, wenn Mindestanforderungen nicht erfüllt werden, oder sinken, wenn die Sicherheitsstruktur vorbildlich ist. Ähnlich wie bei Black-Box-Systemen in der Autoversicherung könnte dies Unternehmen dazu motivieren, kontinuierlich sicherheitsbewusst zu handeln.

Der menschliche Faktor und Cyber-Risiko-Scores

Social Engineering und Fahrlässigkeit von Mitarbeitenden bleiben eine der größten Schwachstellen. Versicherer prüfen zunehmend, wie Risiken auf Unternehmensebene quantifiziert werden können, zum Beispiel über aggregierte Cyber-Risiko-Benchmarks. Sie berücksichtigen die Umsetzung von Awareness-Schulungen, Sicherheitsrichtlinien und technischen Maßnahmen. Prämien oder Deckungsoptionen können auf dieser Grundlage angepasst werden, ohne einzelne Mitarbeitende individuell zu sanktionieren. So entstehen Anreize für eine stärkere Sicherheitskultur und ein reduziertes Gesamtrisiko.

Rechtliche Herausforderungen und Haftungsfragen

Eine enge Zusammenarbeit zwischen Versicherern und Unternehmen kann zu rechtlich komplexen Situationen führen: Wer haftet, wenn trotz Sicherheitsmaßnahmen ein Vorfall eintritt? Solche Fragen könnten die Gestaltung von Versicherungsbedingungen deutlich komplexer machen und neue Beratungsfelder für die Rechtsbranche eröffnen.

Zukünftige Entwicklungen könnten unter anderem folgende Punkte umfassen:

- **KI-gestützte Risikoanalysen**, die Bedrohungen prognostizieren und präventive Maßnahmen empfehlen.
- **Automatisierte Schadensbegrenzung**, bei der Systeme bei Angriffen isoliert und wiederhergestellt werden.
- **Integration in Unternehmensprozesse**, sodass Versicherungsschutz direkt an Sicherheitsrichtlinien oder Compliance-Standards gekoppelt wird.
- **Präventive Boni**, etwa Prämienreduktionen für kontinuierliche Schulungen, Penetrationstests oder transparente Sicherheitsberichte.

Die Zukunft der Cyberversicherung wird damit mehr als nur ein finanzielles Sicherheitsnetz: Sie entwickelt sich zu einem integrierten System aus Technologie, Verhalten und rechtlicher Klarheit, das Unternehmen aktiv bei der Abwehr von Cyberbedrohungen unterstützt.

Trend „Made in EU“:
Vom IT-Schutz zur Versicherungsvertrauensfrage

Für IT-Sicherheitslösungen scheint das Label „Made in EU“ bereits ein starkes Qualitäts- und Vertrauenssignal zu sein. So hat der europäische Anbieter ESET im März 2025 eine Umfrage unter 536 Unternehmensentscheidern durchführen lassen (YouGov). Die Ergebnisse zeigen: 75 % der deutschen Unternehmen bevorzugen bei IT-Sicherheitsprodukten eindeutig EU-Lösungen, insbesondere die deutsche Industrie (51 %). Für 67 % der Befragten spielt die Herkunft der IT-Sicherheitslösung eine Rolle, und fast die Hälfte der größeren Unternehmen (44 % ab 250 Mitarbeitenden) denkt über einen Anbieterwechsel nach. Die Hauptgründe: Datenschutz, DSGVO-Konformität, geringere Abhängigkeit von US-Regulierungen wie dem Cloud Act und nationale Zugriffsgesetze.

Dieser zunehmende Fokus auf die europäische Herkunft eröffnet auch für Cyberversicherungen neue Perspektiven: IT-Lösungen „Made in EU“ erfüllen oft bereits viele Sicherheitsanforderungen, die für den Abschluss einer Cyberversicherung relevant sind. Das kann niedrigere Prämien und eine effektivere Schadensprävention ermöglichen.

EU-Versicherer als verlässliche Partner

Eine Cyberversicherung „Made in EU“ garantiert keine automatisch besseren IT-Sicherheitsstandards, bietet aber transparente Prozesse, regulatorisch abgesichertes Risikomanagement und Rechtsklarheit. Unternehmen profitieren von robusten Sicherheitsmaßnahmen der Versicherer, leichterer Compliance und einer verlässlichen Basis für Schadensfälle.

Warum EU-Versicherer für Unternehmen interessant sein können:

- **Strenge regulatorische Rahmenbedingungen**
  EU-Versicherer unterliegen DORA, Solvency II und anderen Regelwerken, die hohe IT-Sicherheitsstandards, Meldepflichten und Transparenzvorgaben erzwingen.
  Unternehmen können davon ausgehen, dass der Versicherer regelmäßig auditiert wird und Sicherheitsmaßnahmen nachweist.
- **Verlässliche Compliance für Unternehmen**
  Wenn Unternehmen selbst EU-weit oder national reguliert sind (z. B. Banken oder kritische Infrastruktur), ist es einfacher, mit einem EU-Anbieter rechtlich kompatible Verträge abzuschließen.
  Die Versicherung kennt die gesetzlichen Anforderungen und kann passgenaue Deckungen anbieten.
- **Transparenz und Rechtsklarheit**
  EU-Versicherer müssen klar dokumentieren, welche Risiken abgedeckt sind und unter welchen Bedingungen Leistungen erbracht werden.
- **Das reduziert Unsicherheiten bei Schadensfällen.**
  Cyberversicherer und Hersteller von Sicherheitslösungen „Made in EU“ könnten in Zukunft in enger Zusammenarbeit ein vertrauensbasiertes, datenschutzkonformes und technologisch ausgereiftes Risikomanagement anbieten – zugeschnitten auf die Werte und Erwartungen des europäischen Marktes. Analog zu bekannten Gütesiegeln könnte „Made in EU“ künftig auch als Indikator für Vertrauen, Sicherheit und Verlässlichkeit bei Versicherungen dienen.

Interview

Welchen Sinn ergibt es, europäische Lösungen einzusetzen?

Dr. Jens Eckhardt ist Fachanwalt für Informationstechnologierecht, Datenschutzauditor (TÜV) sowie IT-Compliance-Manager (TÜV) bei der Düsseldorfer Kanzlei pitc Legal Eckhardt Rechtsanwälte PartmbB. Im Gespräch mit Thorsten Urbanski, Director of Marketing bei ESET Deutschland GmbH erklärt er, warum es in der IT-Sicherheit Sinn ergibt, auf „Made in EU" zu setzen.

Thorsten Urbanski: Warum ist der Begriff „Made in EU" im Cybersecurity-Kontext mehr als nur eine geografische Angabe?

Dr. Jens Eckhardt: In der Cybersicherheit geht es nicht nur darum, woher eine Lösung stammt – sondern auch darum, welchem Rechtsrahmen sie originär unterliegt. Ein Anbieter mit Sitz in der EU unterliegt denselben Gesetzen wie seine Kunden – etwa der DSGVO, dem zukünftigen BSI-Gesetz in Gestalt der NIS2-Richtlinie. Das schafft Vertrauen, rechtliche Klarheit und Verlässlichkeit, insbesondere im Haftungsfall.

Thorsten Urbanski: Gibt es aus juristischer Sicht konkrete Vorteile für Unternehmen, wenn sie auf europäische Anbieter setzen?

Dr. Jens Eckhardt: Ja. Zum einen vermeiden sie zusätzliche Hürden wie Drittland-Transfers nach DSGVO oder unklare Zugriffsbefugnisse ausländischer Behörden, die nicht durch den EU-Rechtsrahmen gebunden sind. Anbieter und Anwender bewegen sich im gleichen Rechtsrahmen. Das bedeutet: Ein möglicher Rechtsstreit endet im Zweifel beim Europäischen Gerichtshof, dessen Entscheidungen im Ergebnis beide Seiten binden. Das ist ein großer Vorteil gegenüber Anbietern aus außereuropäischen Rechtsordnungen.

Thorsten Urbanski: Was ändert sich durch die neue EU-Security-Regulation für die Unternehmensverantwortung – gerade mit Blick auf aktuelle Regulierungen wie NIS2?

Dr. Jens Eckhardt: Die Verantwortung der Geschäftsführung für IT-Sicherheit nimmt deutlich zu. Die NIS2-Richtlinie und damit die Umsetzung im zukünftigen BSI-Gesetz verpflichtet das Leitungsorgan explizit zur Billigung und Überwachung von „Cybersicherheitsmaßnahmen". Gleichzeitig wird auch eine Schulungspflicht verankert. Das heißt: IT-Sicherheit ist kein technisches Randthema mehr, sondern eine zentrale Compliance- und Haftungsfrage auf Führungsebene.

Thorsten Urbanski: Wie lautet Ihr Fazit in Bezug auf die Frage, ob „Made in EU" ein valides Auswahlkriterium für Cybersicherheitslösungen ist?

Dr. Jens Eckhardt: Absolut. Unternehmen profitieren von Rechtssicherheit, Nachvollziehbarkeit und politischen Stabilitätsvorteilen. In einer Welt zunehmender geopolitischer Spannungen bietet „Made in EU" ein Maß an Vertrauen und Verlässlichkeit, das über technische Aspekte hinausgeht. Es ist eine strategische Entscheidung – sowohl für die Sicherheit als auch für die Unternehmensführung.

Fazit

Aus Sicht eines IT-Sicherheitsherstellers sind Cyberversicherungen weit mehr als reine finanzielle Absicherung: Sie wirken direkt als Impulsgeber für bessere Sicherheitsinfrastrukturen in Unternehmen. Versicherungen schaffen Anreize, bestehende Maßnahmen zu überprüfen, Schwachstellen zu identifizieren und proaktive Schutzlösungen umzusetzen. Sie fungieren sozusagen als Spiegel und Werkzeug zugleich, der Unternehmen zeigt, wo Handlungsbedarf besteht, und gleichzeitig die Implementierung von Best Practices unterstützt.

Für Hersteller ergeben sich konkrete Chancen: Ihre Produkte und Dienstleistungen stärken die Cybersicherheit in Unternehmen direkt und schaffen gleichzeitig Mehrwert für Versicherer, die auf robuste Sicherheitsmaßnahmen setzen. Durch die Bereitstellung fortschrittlicher Lösungen unterstützen Hersteller sowohl die Risikominimierung als auch die Einhaltung von Sicherheitsstandards.

Ein praktisches Beispiel liefert die Sparda-Banken-Gruppe in Deutschland: Sie bietet Kunden eine Cyberversicherung gegen finanzielle Schäden durch Phishing, Pharming und Skimming bis zu 10.000 € pro Jahr an. Für IT-Sicherheitshersteller entsteht hier eine wertvolle Datenbasis zu Angriffsmustern, Schwachstellen und Präventionsbedarf – Daten, die genutzt werden können, um technologische, organisatorische und menschliche Sicherheitsmaßnahmen weiterzuentwickeln.

Die zukünftige Zusammenarbeit zwischen IT-Sicherheitsanbietern und Cyberversicherungen verspricht eine nachhaltige Transformation der Cybersicherheitslandschaft: Durch gemeinsame Datenanalysen, standardisierte Sicherheitsanforderungen und innovative Technologien können Unternehmen effektiver vor digitalen Bedrohungen geschützt werden. Für Hersteller eröffnet dies Potenziale für präventive Sicherheitslösungen, die Lücken schließen, Prozesse optimieren und Risiken sichtbar machen. Denn nur wer seine IT versteht, kann wirklich geschützt sein – und im Ernstfall schnell reagieren.

Anhang

Checkliste zur IT-Sicherheit und Cyberversicherung
für Unternehmen – sowohl aus Sicht der Versicherer als auch regulatorisch und branchenspezifisch:

1. Mindestanforderungen der Versicherer

- ☐ Virenschutz und Firewalls installiert und aktuell
- ☐ Regelmäßige Datensicherung (Backups) vorhanden und getestet
- ☐ Software und Systeme regelmäßig aktualisiert (Patch-Management)
- ☐ Mitarbeitende geschult zu Cyberrisiken (Phishing, Passwörter, Social Engineering)
- ☐ Dokumentierte Sicherheitsrichtlinien vorhanden und umgesetzt

2. Regulatorische Vorgaben

- ☐ NIS 2-Richtlinie: Sicherheitsmaßnahmen und Vorfallmeldung implementiert
- ☐ DSGVO: Schutz personenbezogener Daten, technische und organisatorische Maßnahmen (TOMs) umgesetzt
- ☐ DORA (falls Finanzsektor): IT-Risikomanagement und digitale Resilienz etabliert
- ☐ VAIT (für Versicherer): IT-Governance, Risikomanagement, Sicherheitsmanagement dokumentiert

3. Branchenspezifische Standards (Industrie / kritische Infrastruktur)

- ☐ IEC 62443: Sicherheitsmaßnahmen für industrielle Steuerungs- und Automatisierungssysteme
- ☐ DIN SPEC 27076: Cyber-Risiko-Checks durchgeführt
- ☐ BSI IT-Grundschutz: Leitlinien umgesetzt, Business Continuity Management etabliert

4. Präventive Maßnahmen

- ☐ Passwortrichtlinien: komplexe und einzigartige Passwörter, MFA (Multi-Faktor-Authentifizierung)
- ☐ Zugriffskontrollen: rollenbasierte Berechtigungen
- ☐ Überwachung: Intrusion Detection / Prevention Systeme, Log-Analyse
- ☐ Notfallpläne: Wiederherstellungspläne, Krisenkommunikation, Lösegeldstrategien geprüft

5. Regelmäßige Überprüfung & Dokumentation

- ☐ Interne Audits & Risikobewertungen regelmäßig durchführen
- ☐ Versicherungspolicen prüfen: Deckung, Ausschlüsse, Anforderungen erfüllen
- ☐ Sensibilisierung der Mitarbeitenden regelmäßig auffrischen

Checkliste an Kernanforderungen in Sicherheitsfragebögen

Die aufgelisteten Punkte sind korrekt und decken viele Kernanforderungen ab, u. a.:

- Business Continuity & Disaster Recovery (BCP/DRP)
- Patch- und Änderungsmanagement
- Protokollierung & Monitoring
- Verschlüsselung von Daten
- Backup-Strategien
- Schwachstellen- & Penetrationstests
- DSGVO-Konformität
- Awareness-Schulungen
- Physische Sicherheit
- Drittanbieter-Risikomanagement

Mögliche Ergänzungen, die häufig ebenfalls abgefragt werden:

1. **Mehrfaktor-Authentifizierung (MFA):**
   Besonders für privilegierte Konten und Remote-Zugriffe.
2. **Zugriffs- und Berechtigungsmanagement:**
   Prinzip der minimalen Rechtevergabe („least privilege").
3. **Sicherheitsrichtlinien & Governance:**
   Gibt es ein ISMS (z. B. nach ISO 27001 oder BSI-Grundschutz)?
4. **Cloud-Sicherheit:**
   Nutzung von Cloud-Diensten und deren Absicherung (z. B. durch Verschlüsselung, Monitoring, Shared Responsibility Model).
5. **Incident Response Plan:**
   Gibt es ein definiertes Verfahren für den Umgang mit Cyberangriffen, inkl. Kommunikationsstrategie?
6. **Endgeräte-Sicherheit:**
   Endpoint Detection & Response (EDR), Mobile Device Management (MDM).
7. **Netzwerk-Segmentierung & Firewalls:**
   Schutz vor lateralen Bewegungen von Angreifern.
8. **Lieferkettensicherheit:**
   Wie wird die Sicherheit von Zulieferern/Partnern überprüft?
9. **Regelmäßige Audits & Zertifizierungen:**
   Interne und externe Prüfungen (z. B. ISO, TISAX).
10. **Richtlinien zu Remote Work/Homeoffice:**
    Umgang mit BYOD, private Netzwerke, VPN.

Whitepaper

Cybersecurity und die neue Rechtslage

↗ Hier herunterladen

Umfrage

Stand der IT-Sicherheit 2025

↗ Hier herunterladen

Whitepaper

NIS2 und die Lieferkette

↗ Mehr erfahren

Whitepaper

Stand der Technik

↗ Hier herunterladen

Übersicht

ESET Lösungen für NIS2-Compliance

↗ Hier herunterladen

Studie

Digitale Souveränität auf dem Prüfstand

↗ Hier herunterladen

Whitepaper

NIS2 - Der Countdown läuft

↗ Mehr erfahren

Paper

Ransomware 2025:
Wenn Daten zum Druckmittel werden

↗ Hier herunterladen

IT-Sicherheit ist **Vertrauenssache**

ESET bietet Informationssicherheit für Unternehmen jeder Größe

Qualitätsmanagement – Made in EU:

- Überall verfügbar – vollautomatischer Schutz der gesamten Organisation
- Volle Kontrolle über Ihre Daten dank transparenter (Sample-)Analysen innerhalb der EU
- Einzigartige Geschwindigkeit bei der Analyse von eingehenden Warnmeldungen
- Zuverlässig und sicher – alle Anforderungen von Datenschutzbestimmungen (bspw. DSGVO) bequem erfüllen
- Große Flexibilität in puncto Lizenzform, Hardwareeinsatz und Anforderungen an die Infrastruktur

Vorteile für Unternehmen:

- Passgenaue IT-Sicherheit für alle Unternehmensgrößen und -anforderungen
- Mitarbeitende entlasten und (Hardware-) Ressourcen schonen
- Compliance und Sicherheitsstandards erweitern
- Verwaltung der Schutzlösungen für alle gängigen Betriebssysteme via ESET PROTECT (Cloud oder On-Premises)
- Lizenzvielfalt – Kombination beliebiger Betriebssysteme (Windows, macOS, Linux) und Geräte (Clients, Server, Mobilgeräte) entsprechend der Bedürfnisse

Security made in EU
Trust Seal
www.teletrust.de/itsmie

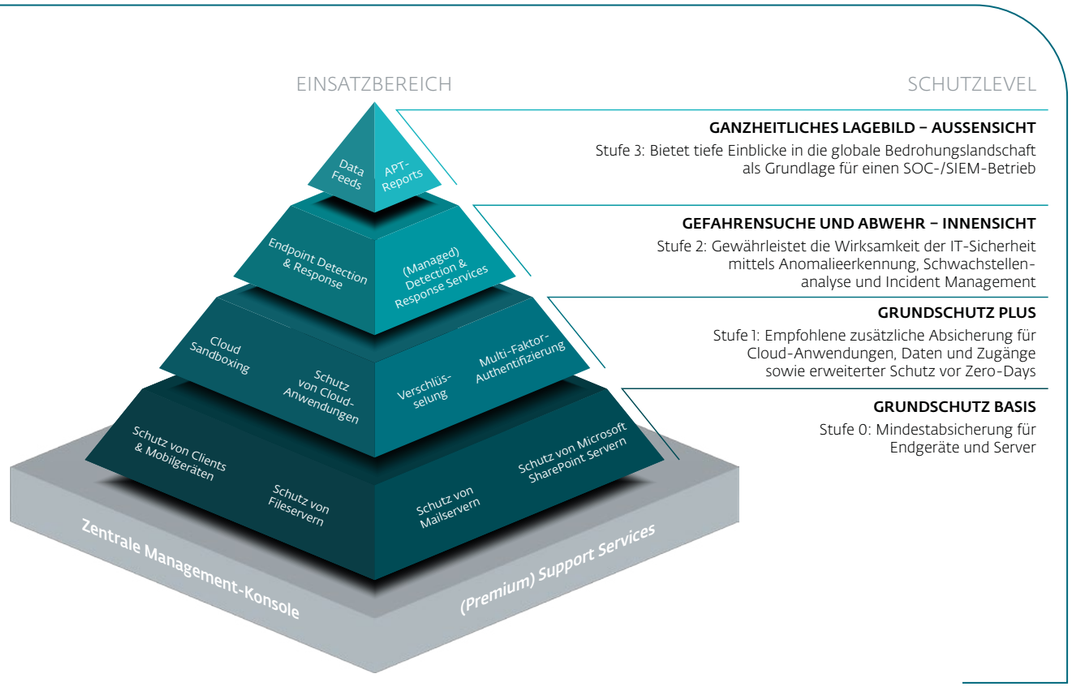
„Als Security-Hersteller bieten wir moderne Lösungen, Dienstleistungen und Konzepte an, mit denen Unternehmen und Verwaltungen eine Cyber-Resilienz auf höchstem Niveau gestalten können."

— Holger Suhl, Country Manager DACH,
ESET Deutschland GmbH

Sie möchten wissen, wie Sie ihr Unternehmen effektiv absichern?
↗Kontaktieren Sie uns!

Zero Trust Security von ESET

Das Zero Trust Security-Konzept von ESET besteht aus einem dreistufigen, aufeinander aufbauenden Reifegradmodell. Je höher die Stufe ist, desto sicherer ist die Schutzwirkung – also „reifer". Ob als Standardlösung oder als Managed Service - die Kombination aus Endpoint Security, Verschlüsselung, Multi-Faktor-Authentifizierung, Cloud Sandboxing und Schutz für Cloud-Anwendungen bildet dabei das richtige Fundament für Zero Trust.



ESET MDR: Frühzeitig erkennen, schnell reagieren

ESET bietet Managed Detection & Response (MDR) für KMU und Enterprise. Der Service ESET MDR überwacht Ihre Systeme rund um die Uhr. Die Kombination aus KI und menschlicher Kompetenz sorgt für einen erstklassigen Ransomware-Schutz, auch ohne eigene Sicherheitsspezialisten im Haus.

ESET MDR Ultimate bietet Großunternehmen ein effektives Security Operation Center. Die erfahrenen Spezialisten von ESET führen proaktives Threat Hunting und Threat Monitoring durch, unterstützen Sie bei der Analyse von Sicherheitsvorfällen und ergreifen sofort geeignete Maßnahmen.

3 VON ÜBER 500.000 ZUFRIEDENEN KUNDEN

BVB 09 CHAMPION PARTNER

Seit 2019 ein starkes Team auf dem Platz und digital

Allianz Suisse

Seit 2016 durch ESET geschützt
Mehr als 4.000 Postfächer

ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT

SecurITy made in EU
Trust Seal www.teletrust.de/itsmie

ESET wurde das Vertrauenssiegel „IT Security made in EU" verliehen

Unsere Lösungen sind nach den Qualitäts- und Informationssicherheitsstandards ISO 9001:2015 und ISO/IEC 27001:2022 zertifiziert

ESET IN ZAHLEN

110.000.000+
Geschützte Nutzer weltweit

178
Länder & Regionen

500.000+
Geschützte Unternehmen

11
Forschungs- und Entwicklungs-zentren weltweit

ÜBER ESET

Als europäischer Hersteller mit mehr als 30 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Organisationsgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihre Infrastruktur mithilfe von Cloud Sandboxing frei von Zero-Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungslösungen unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen sowie Compliance-Maßnahmen.

Unsere Endpoint Detection and Response-Lösung, dedizierte Services wie z.B. Managed Detection and Response und Frühwarnsysteme in Form von Threat Intelligence ergänzen das Angebot im Hinblick auf Incident Management sowie den Schutz vor gezielter Cyberkriminalität und APTs. Dabei setzt ESET nicht allein auf modernste KI-Technologie, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

welivesecurity by ESET

ESET Digital Security Guide

ESET Deutschland GmbH
Spitzweidenweg 32 | 07743 Jena | Tel.:+49 3641 3114 200

ESET.DE | ESET.AT | ESET.CH