WHITEPAPER

Vorbeugen. Schützen. Versichern.

Cyber-Risikoversicherung: Wie Vorsorgemaßnahmen die Überlebenschancen Ihres Unternehmens erhöhen.

ESET Made in EU IT-Security

Digital Security
Progress. Protected.

Vorwort

Das Bedürfnis nach Sicherheit ist tief in uns verankert – ob privat oder geschäftlich. Aus diesem Grund schließen viele Menschen Versicherungen ab. Sie helfen, unvorhersehbare Risiken abzufedern und im Ernstfall handlungsfähig zu bleiben. Schon in der Antike teilten Gemeinschaften finanzielle Lasten, um Einzelne zu schützen – ein Prinzip, das sich bis heute bewährt.

Mit der Digitalisierung sind neue Gefahren entstanden: Cyberangriffe können Unternehmen finanziell lähmen. Sogenannte Cyber-Risikoversicherungen bieten Schutz vor den Folgen von Datenlecks, Ransomware und IT-Schäden – doch sie setzen ein gutes Sicherheitsniveau voraus.

Der Markt für Cyberversicherungen wächst, da Unternehmen zunehmend mit Angriffen konfrontiert werden. Anbieter decken Risiken wie Datenverluste, regulatorische Verstöße und Erpressungsversuche ab. Neben finanziellen Erstattungen für Vorfälle bieten sie auch Unterstützung bei IT-Forensik, Rechtsbeistand und Systemwiederherstellung – bis hin zur Deckung von Lösegeldzahlungen bei Ransomware-Attacken.

Doch eine Cyber-Risikoversicherung ist mehr als nur eine finanzielle Absicherung. Sie ist ein Indikator für die eigene IT-Sicherheitslage: Ohne robuste Schutzmaßnahmen ist eine Police heute kaum noch erhältlich. Die Anforderungen an Unternehmen steigen, denn Schadensdaten und forensische Analysen machen Cyberrisiken messbarer.

Angesichts der hohen Kosten eines Cybervorfalls – laut IBM durchschnittlich 4,5 Millionen US-Dollar – wird eine Cyberversicherung für viele Unternehmen zur Notwendigkeit. Doch wer sich schützen will, muss auch seine Sicherheitsstrategie überdenken und kontinuierlich anpassen, um den Versicherungsschutz zu erhalten.

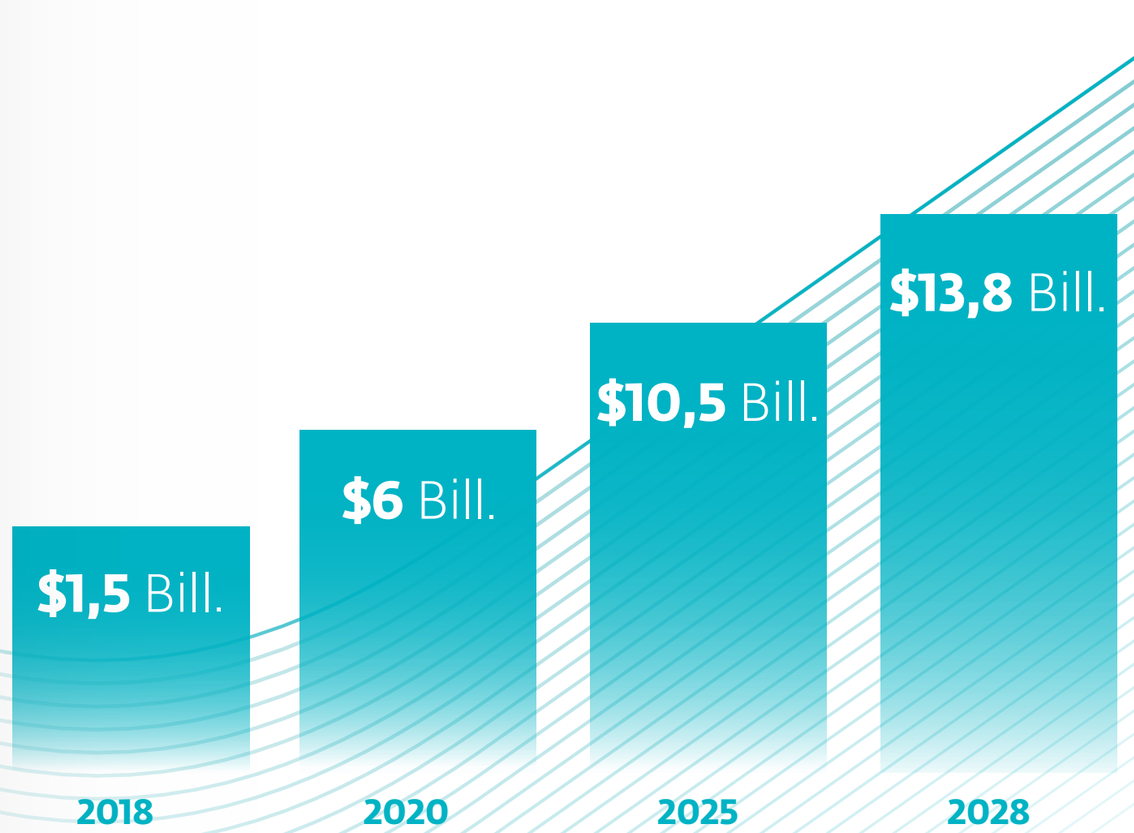


Abb1: Kosten durch Cyberkriminalität: Entstandene Schäden und erwartete Kosten

Inhaltsverzeichnis

Digital Security
Progress. Protected.

1. Bedrohung und Risiko für Unternehmen durch Cyberkriminalität

Da die Cyberkriminalität mit generativer KI, maschinellem Lernen und anderen fortschrittlichen Tools ihre Angriffe automatisiert und schwerer erkennbar macht, ist jedes vernetzte Unternehmen direkt bedroht. Wer wertvolle oder sensible Daten nicht ausreichend schützt, riskiert schwerwiegende Folgen.

Die jüngste Bitkom-Studie „Wirtschaftsschutz 2024" deckt auf, dass 81 Prozent der Unternehmen in den letzten 12 Monaten von Datendiebstahl, digitaler und analoger Industriespionage oder Sabotage betroffen waren. Weitere zehn Prozent sind sich nicht sicher. Nur 37 Prozent haben einen Notfallplan, um auf Sicherheitsvorfälle in ihrer Lieferkette zu reagieren. Genauso viele gaben an, dass im Unternehmen das Bewusstsein für solche Risiken fehle.

In einer Forsa-Umfrage unter 300 mittelständischen Unternehmen schätzten die Befragten das Risiko, dass Firmen Opfer von Cyberkriminalität werden können, als hoch ein. Trotzdem wird die Gefahr für das eigene Business von den meisten als eher gering eingestuft. Das liegt unter anderem daran, dass 82 Prozent ihre IT-Systeme für umfassend geschützt halten, 66 Prozent ihr Unternehmen als zu klein einschätzen, um angegriffen zu werden. 63 Prozent sind der Meinung, dass ihre Daten nicht interessant genug sind, um ins Visier von Cyberkriminellen zu geraten. (Bei der Umfrage waren Mehrfachantworten möglich.)

In der gleichen Umfrage zeigt sich, dass nur jedes dritte der befragten mittelständischen Unternehmen den Basisschutz im Bereich IT-Sicherheit vollständig erfüllt. Sehr bedenklich ist, dass elf Prozent sich so gut wie gar nicht schützen.

Laut der Bitkom-Studie „Wirtschaftsschutz 2023" gaben mehr als die Hälfte der Unternehmen an, dass sie ihre wirtschaftliche Existenz durch Cyberangriffe bedroht sehen. Zwei Jahre zuvor waren es nur neun Prozent.

"Das Risiko gibt es - aber mein Unternehmen betrifft das nicht"

Frage: "Wie schätzen Sie das Risiko ein, Opfer von Cyberkriminalität zu werden?"

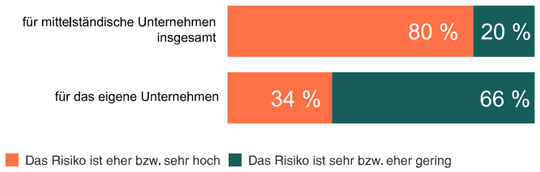


Abb2: Laut Forsa-Umfrage ist das Risiko hoch, aber nur für andere.

IT-Sicherheit mittelständischer Unternehmen zeigt deutliche Lücken

Nur eine Minderheit erfüllt den Basisschutz vollständig

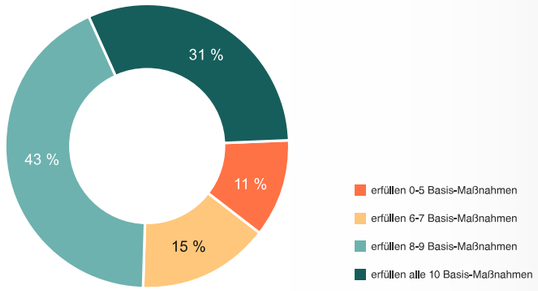


Abb3: Nur 31% erfüllen die Anforderungen an den kompletten Basisschutz.

Digitale Angriffe auf die Wirtschaft nehmen weiter zu

Dem BKA zufolge wurden 2023 über 800 deutsche Unternehmen und Institutionen Opfer von Ransomware-Angriffen. Auch kleine und mittlere Organisationen sowie Behörden und Kommunen hatten in den letzten Jahren zunehmend mit Erpressersoftware zu kämpfen.

Angriffe wie die auf einen IT-Dienstleister Ende Oktober 2023, bei dem 72 Gemeinden mit rund 20.000 Arbeitsplätzen betroffen waren, sind kein Einzelfall mehr.

Laut der jüngsten Studie von Bitkom entstand der deutschen Wirtschaft im Jahr 2024 ein Gesamtschaden von rund 266,6 Milliarden Euro durch Diebstahl von IT-Ausrüstung und Daten, Spionage und Sabotage. Cyberattacken verursachten zwei Drittel der Schäden und Kosten von knapp 179 Millionen Euro. Das ist ein weiterer Anstieg im Vergleich zum Vorjahr (203/148,2 Mrd. Euro). Ein weiterer Bitkom-Bericht deckt auf, dass deutsche Unternehmen im Durchschnitt 5,7 Millionen Euro für die Reaktion auf Cybervorfälle ausgeben.

Schaden steigt auf 266,6 Milliarden Euro

Welche Schäden sind Ihrem Unternehmen im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

Schaden durch…	Schadenssummen in Mrd. Euro (2024)	Schadenssummen in Mrd. Euro (2023)	Schadenssummen in Mrd. Euro (2022)
Ausfall, Diebstahl oder Schädigung von Informations - und Produktionssystemen oder Betriebsabläufen	54,5	35,0	41,5
Kosten für Rechtsstreitigkeiten	53,1	29,8	16,2
Umsatzeinbußen durch nachgemachte Produkte bzw. Plagiate	39,2	15,3	21,1
Kosten für Ermittlungen und Ersatzmaßnahmen	32,2	25,2	10,1
Datenschutzrechtliche Maßnahmen, z.B. durch Behörden	27,2	12,4	18,3
Imageschaden bei Kunden oder Lieferanten, Negative Medienberichterstattung	20,2	35,3	23,6
Patentrechtsverletzungen, auch vor Anmeldung	14,8	10,4	18,8
Erpressung mit gestohlenen Daten	13,4	16,1	10,7
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	11,2	21,5	41,5
Geldabfluss durch Betrugsversuche	0,8	3,9	-
Sonstige Schäden	0	1,1	0,9
Gesamtschaden pro Jahr	266,6	205,9	202,7

Basis: Alle Unternehmen (n=1.003) | Mehrfachnennungen möglich | rundungsbedingt kann die Summe der Einzelschäden vom Gesamtschaden abweichen. | Quelle: Bitkom Research 2024

Abb4: Der wirtschaftliche Schaden ist zum Vorjahr erneut gestiegen.

Aktuelle Bedrohungslage in der Schweiz und Österreich

Auch in der Schweiz ist die Situation nicht rosiger: 2023 wurden 60 Prozent mehr Cyberangriffe auf kleine und mittlere Unternehmen (KMU) registriert als in den letzten drei Jahren[1]. Auch wenn 2024 verhältnismäßig wenige Schadensfälle gemeldet wurden, bleibt die Bedrohungslage weiter angespannt. Vor allem Erpressersoftware und Schwachstellen in der Lieferkette treiben die Kosten immer mehr in die Millionenhöhe.

Die finanziellen Schäden liegen im Durchschnitt pro Cybervorfall bei etwa einer Million Franken, wobei die Kosten für die Wiederherstellung der Systeme und die Krisenbewältigung das meiste der Gesamtkosten ausmachen, und zwar rund 61 Prozent, Betriebsunterbrechungen 34 Prozent. Durch Cyberangriffe verursachte Drittschäden und Haftpflichtansprüche belaufen sich „nur" auf ein Prozent.

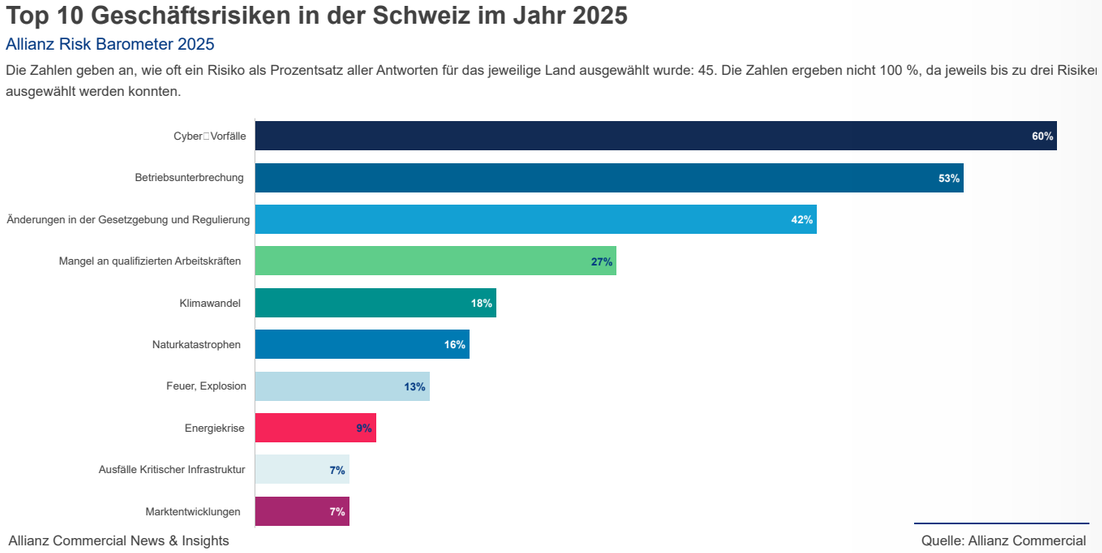


Abb5: Cybervorfälle halten Schweizer Unternehmen für die größte Gefahr.

Laut der KPMG-Studie „Cybersicherheit in Österreich" unter 1.000 Unternehmen war in 2024 schon jedes sechste Unternehmen von einem Cyberangriff betroffen und jedes dritte zahlte mindestens einmal nach einer Ransomware-Attacke Lösegeld. In der Studie aus dem Vorjahr gaben alle der befragten 903 Unternehmen an, dass sie schon mal Opfer eines Cyberangriffs geworden sind. Phishing, Business-E-Mail-Compromise (BEC), CEO-Fraud, Social Engineering sowie Attacken auf die Lieferkette zählten zu den häufigsten Bedrohungen. Vor allem die Gefahr von staatlich motivierten und unterstützten Attacken und das zunehmende Interesse an kritischer Infrastruktur wird zusehends größer. Jeder zehnte Cyberangriff erwies sich in 2023 als erfolgreich und verursachte bei jedem siebten Unternehmen Betriebsunterbrechungen von über drei Monaten.

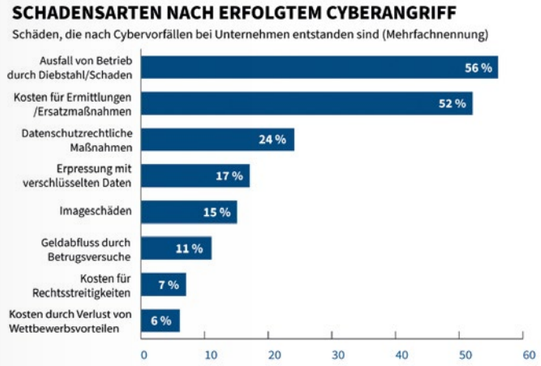


Abb6: Betriebsunterbrechungen waren 2024 häufigste Folge nach einem Angriff auf Schweizer Unternehmen.

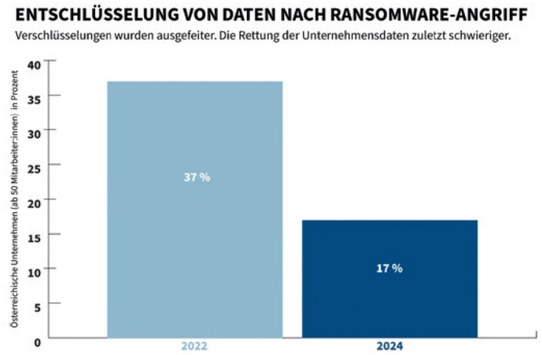


Abb7: In Österreich konnten 2024 Unternehmensdaten weniger gerettet werden.

Erhöhte Kosten der Geschäftstätigkeit

Eine effektive Cybersicherheit erfordert Investitionen in Technologie, Fachwissen, Überwachung, Governance, Versicherungsprämien, Risikomanagement, rechtlicher Unterstützung und mehr.

Betriebsstörungen

Ausfallzeiten, die zu Produktivitäts- und Umsatzeinbußen führen, können eine der schlimmsten Auswirkungen nach einem Cybersicherheitsvorfall sein.

Reputationsverlust

Massive Datenpannen können das Image einer Marke lange nach Abklingen der Meldungen schädigen. Nicht nur Kunden, sondern auch Partner, Investoren und andere Interessengruppen könnten zu einem Wettbewerber wechseln, den sie als vertrauenswürdiger wahrnehmen.

Fallender Aktienkurs

Als Folge des Imageverlusts erleben börsennotierte Unternehmen nach Offenlegung einer Datenpanne häufiger eine kurzfristige Einbuße an Marktwert oder sogar einen dramatischen Kurssturz. Die Sensibilität der betroffenen Daten sowie die wahrgenommene Transparenz des Unternehmens bei der Aufklärung des Vorfalls können die Schwankungen des Aktienkurses erheblich beeinflussen.

Cyberbedrohungen:

Die größten Risiken für Organisationen und Unternehmen

Umsatzeinbrüche

Unternehmen verbuchen nach einem Cyberangriff oft sinkende Einnahmen, da Kunden und Geschäftspartner aus Sorge um ihre Daten oder Geschäftsbeziehung den Anbieter wechseln.

Eingeschränktes Geschäftsmodell

Cyberrisiken und damit verbundene Kosten können Unternehmen dazu zwingen, ihr Geschäftsmodell anzupassen, z. B. in welcher Form sie Daten speichern und verarbeiten, welche Produkte und Services sie online anbieten, welche Cloud-Dienste sie nutzen oder mit welchen Lieferanten sie zusammenarbeiten.

Verlust oder Verletzung von geistigem Eigentum

Das geistige Eigentum eines Unternehmens zählt oft zu seinen wertvollsten Daten. Der Diebstahl oder die unerlaubte Weitergabe von Forschungsdaten, neuen Produktdesigns, Geschäftsstrategien oder Kundenlisten kann die Wettbewerbsgrundlage eines Unternehmens massiv schädigen – oder sogar die nationale Sicherheit gefährden.

Ein Cybervorfall kostet Unternehmen mehr als Geld

Ein Cybervorfall wie ein Ransomware-Angriff oder eine Datenschutzverletzung kann für Unternehmen weitreichende Folgen haben – weit über Lösegeldzahlungen oder den Verlust vertraulicher Daten hinaus. Die Betroffenen stehen vor hohen Kosten für Incident Response, Anwaltsgebühren und mögliche Strafen, wie auch die ↗NetDiligence Cyber Claims Study 2023[2] zeigt.

Doch damit nicht genug: Selbst nach der Wiederherstellung des Betriebs können monetäre Belastungen weiter steigen. In den USA sind beispielsweise Sammelklagen in Millionenhöhe keine Seltenheit, vor allem wenn persönliche oder finanzielle Kundendaten kompromittiert wurden. ↗Aktuelle Studien[3] belegen, dass genau dieser Datenverlust der größte Kostenfaktor eines Cyberangriffs ist – oft verbunden mit langwierigen Rechtsstreitigkeiten.

Langfristig trifft Unternehmen vor allem der Vertrauensverlust. Imageschäden können sich noch auf Jahre finanziell auswirken. Wer für schwache Cybersicherheitsmaßnahmen bekannt ist, riskiert sogar eine schlechtere Kreditwürdigkeit – mit teuren Folgen für Finanzierungen. Insgesamt sind die Schäden eines Cyberangriffs kaum bezifferbar, doch sie können leicht in die Milliarden gehen, wie der Cyberangriff auf den US-Bezahldienst Change Healthcare im nächsten Abschnitt zeigt.

Abb8: Gesamtkosten einer Datenschutzverletzung in Mio.

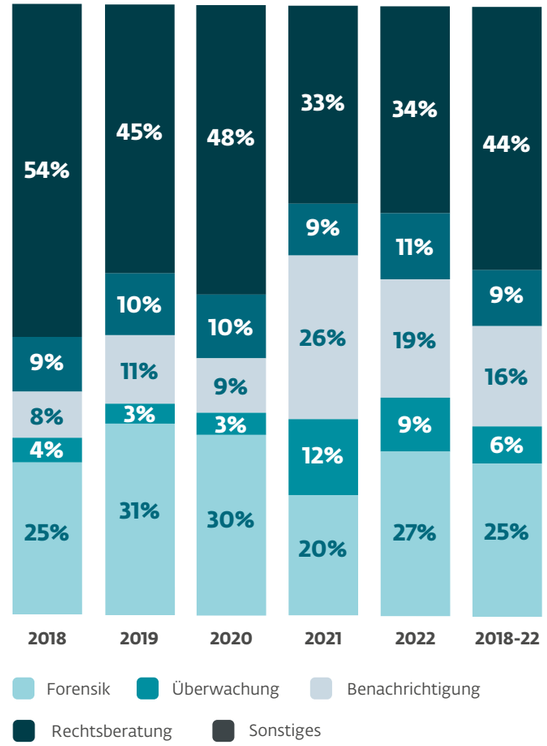


Abb9: Verteilung der Kosten für Krisendienste

Sicherheitslücke mit Milliardenfolgen: Der Fall Change Healthcare

Der bislang schwerwiegendste Cyberangriff auf die kritische Infrastruktur der USA traf den Gesundheitssektor mitten ins Herz. Im Februar 2024 wurde Change Healthcare lahmgelegt, eines der weltweit größten Unternehmen für die Verarbeitung von Gesundheitszahlungen und Tochtergesellschaft von UnitedHealth. Bei der Attacke verschafften sich Cyberkriminelle Zugriff auf vier Terabyte Daten: von großen Versicherungsgesellschaften bis zum „kleinen" Patienten.

Auch nach Zahlung eines Lösegelds in Höhe von 22 Millionen US-Dollar blieb die Situation unverändert. Erst nach Monaten begann Change Healthcare, die Betroffenen über den Verlust ihrer Daten zu informieren. Im Oktober bestätigte das Unternehmen schließlich, dass Daten von etwa 100 Millionen Menschen erbeutet wurden.

Mit Ausfällen zu kämpfen hatten vor allem Unternehmen und Dienstleister in der Lieferkette wie Apotheken, Krankenhäuser, Militärkliniken und Patienten. Der Angriff offenbart das Risiko eines fatalen Dominoeffekts, an dem Tausende von Unternehmen miteinander verbunden sind.

$595 Mio.

- Wiederherstellung der Clearinghouse Plattform
- Maßnahmen zur Reaktion
- Medizinische Kosten, die direkt mit der vorübergehenden Aussetzung bestimmter Versorgungsmanagement-Aktivitäten verbunden sind

$280 Mio.

- Betriebsunterbrechung
- Umsatzeinbußen

$1,35-$1,6 Mill.

- Erwartete endgültige Kosten

Die Attacke konnte vor allem so erfolgreich wie verheerend sein, weil es Sicherheitslücken gab, die nicht hätten sein müssen:

- **Gestohlene Daten verschaffen Zugang:** Der Zugriff auf die Systeme erfolgte durch gestohlene Zugangsdaten aus einer vorangegangenen Phishing-Attacke. Damit gelangten die Cyberkriminellen in ein mit Change Healthcare verbundenes Softwareportal. Es wird vermutet, dass die erbeuteten Daten im Dark Web von den Hackern gekauft wurden.
- **Fehlende Multi-Faktor-Authentifizierung:** Bei dem besagten Softwareportal, worüber die Cyberkriminellen eindringen konnten, war keine Multi-Faktor-Authentifizierung (MFA) aktiviert.
- **Unbemerkte Aktivitäten:** Über neun Tage lang gelang es den Angreifern, sich unerkannt im Netzwerk zu bewegen und weitere Daten zu entwenden, ehe Ransomware zum Einsatz kam.
- **Veraltete Systeme und Backups:** Den jüngsten Erkenntnissen nach war eine 40 Jahre alte Technologie für die Verarbeitung von Zahlungen und Abrechnungen im Einsatz. Darüber hinaus wurden die Daten nur auf lokalen Servern gespeichert.
- **Fehlende Cyber-Risikoversicherung:** Die Entscheidung von UnitedHealth, auf eine Cyber-Risikoversicherung zu verzichten, hat das Unternehmen finanziell und dessen Reputation stark beschädigt. Sie hätte nicht nur die Kosten des wirtschaftlichen Schadens abgefedert, sondern vermutlich auch dazu beigetragen, den Vorfall zu verhindern. Die nach dem Angriff offen gelegten Schwachstellen beim Gesundheitsdienstleister hätte es in der Form wahrscheinlich nicht gegeben, denn die Versicherer haben hohe Anforderung an die IT Security.

Erkenntnisse

aus dem Angriff auf Change Healthcare

#1

Risiken durch Drittanbieter evaluieren

Die Abhängigkeit von externen Dienstleistern wie Change Healthcare führt zu einer erheblichen Steigerung des Cyberrisikos. Unternehmen sind besser beraten, ihre Drittanbieter ausführlich zu prüfen und deren Security-Maßnahmen sorgfältig zu bewerten.

#2

Effiziente Cybersicherheitsmaßnahmen umsetzen

Die Cyberkriminellen verwendeten kompromittierte Zugangsdaten, um sich Zugriff aufs System von Change Healthcare zu verschaffen. Daran lässt sich ablesen, wie notwendig starke Zugangskontrollen, regelmäßige Sicherheitsüberprüfungen und Multi-Faktor-Authentifizierung sind.

#3

Proaktives Incident-Management einführen

Der Cyberangriff auf Change Healthcare veranschaulicht die Notwendigkeit eines umfassenden Notfallplans für solche Vorfälle. Für Unternehmen gilt es, präventive Maßnahmen zu treffen und klare Prozesse zur Schadensbegrenzung festzulegen.

#4

Finanzielle Absicherung über eine Cyber-Risikoversicherung

Selbst ein Riesenunternehmen wie Change Healthcare mit umfassenden Ressourcen ist nicht von Haus aus immun gegen Cyberrisiken. Nur wer seine Systeme und Netzwerke effektiv absichert, kann seine Überlebenschancen erhöhen. Eine Cyber-Risikoversicherung ermöglicht zusätzlich, wirtschaftliche Verluste im Falle eines Angriffs einzudämmen.

#5

Zahlung von Lösegeld ist keine Option

Einer der wichtigsten Lektion für Unternehmen Prozent Co.: Niemals Lösegeld zahlen! Die Zahlung von 22 Millionen US-Dollar führte zu gar nichts, außer zu einem weiteren Erpressungsversuch, weil bereits schon einmal gezahlt wurde.

2. Schadensbegrenzung
durch Cyber-Risikoversicherungen

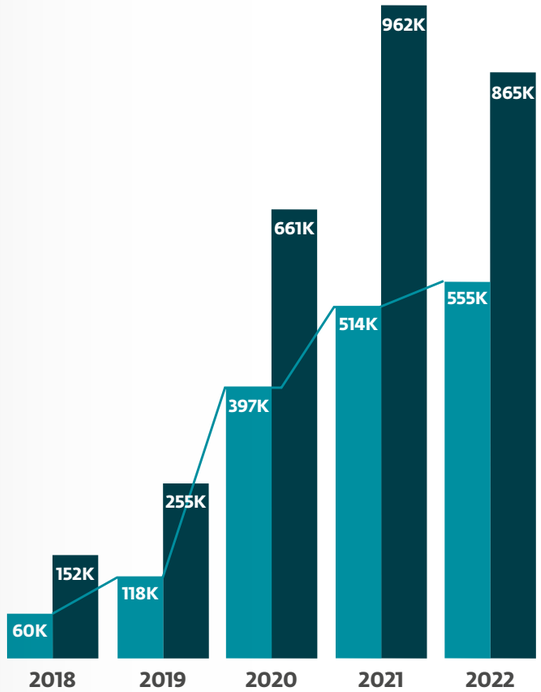


Abb10: Durchschnittliche Kosten für Ransomware

Cybersicherheit im 21. Jahrhundert betrifft nicht mehr nur den Betrieb eines Unternehmens, sondern vor allem auch seine Daten, die heute oft „wertvoller als Gold“ gehandelt werden. Datensicherheit bedeutet weit mehr, als nur zu wissen, wo sich Informationen befinden und wie sie genutzt werden. Cyberversicherungen schützen Unternehmen vor der wachsenden Intensität und Komplexität von Cyberbedrohungen sowie vor den unvorhersehbaren und möglichen verheerenden Folgen solcher Angriffe. Traditionelle Versicherungen wie allgemeine Haftpflichtversicherungen oder Fehler- und Unterlassungsversicherungen decken Cybervorfälle in der Regel nicht ab und bieten daher keinen ausreichenden Schutz gegen digitale Risiken.

Der Internationale Währungsfonds (IWF) stellt in seinem Global Financial Stability Report vom April 2024 fest, dass extreme finanzielle Verluste durch Cybervorfälle (die schlimmsten zehn Prozent der Verluste) seit 2017 um mehr als 400 Prozent gestiegen sind und weiterhin schnell zunehmen. Die Kosten eines Ransomware-Vorfalls im KMU-Bereich, einer der teuersten Vorfälle, liegen im internationalen ↗Durchschnitt bei 850.000 US-Dollar[4] plus einer Lösegeldzahlung von durchschnittlich 555.000 US-Dollar.

Zusätzlich zu den damit verbundenen Umsatzverlusten, Wiederherstellungskosten und Reputationsschäden können diese finanziellen Katastrophen unvorbereitete Unternehmen lahmlegen oder sogar zum Stillstand bringen.

Wer braucht eine Cyberversicherung?

Auch wenn eine Cyberversicherung keinesfalls ein Ersatz für präventive Sicherheitsmaßnahmen ist, bildet sie einen wichtigen Bestandteil eines effektiven, risikobasierten und vor allem ganzheitlichen IT-Sicherheitskonzepts für nahezu jedes Unternehmen, insbesondere für KMU. Die wichtigsten Gründe dafür sind:

- Auch wenn viele kleine Unternehmen auf das Prinzip „Sicherheit durch Unauffälligkeit" setzen, sieht die Realität anders aus. KMU stehen häufig im Visier von Cyberkriminellen, da sie häufig nicht in umfassende und leistungsstarke Cybersicherheitsmaßnahmen investieren, um mit den sich ständig weiterentwickelten Bedrohungen Schritt zu halten.
- Der Wechsel zum Homeoffice hat die Angriffsfläche vieler KMU erheblich vergrößert, neue Sicherheitslücken eröffnet und deutlich mehr Daten exponiert.
- Bei einem Cybervorfall könnten KMU Schwierigkeiten haben, die finanziellen Mittel, Fachkenntnisse und Ressourcen zu finden, um schnell zu reagieren und/oder vorausschauende Kosten und Haftungen abzudecken – besonders, wenn sie keinen Notfallplan haben.

Eine umfassende Cyberversicherung schützt die Geschäftskontinuität und bewahrt Unternehmen vor den Worst-Case-Szenarien. ↗In Großbritannien haben beispielsweise jedoch nur zehn Prozent der KMU eine Cyber-Risikoversicherung[5].

↗In Deutschland liegt dieser Anteil bei 12 Prozent und in den USA bei 21 Prozent – allesamt niedriger als erwartet angesichts der Vorteile einer Cyberversicherung[6]. Eine wahrscheinliche Erklärung dafür sind die komplexen Anforderungen, die verbindlichen Informationen für Versicherer bereitzustellen, die Notwendigkeit einer Sicherheitsanalyse und die Herausforderung, den Vorgaben der Versicherung während der gesamten Laufzeit der Police gerecht zu werden.

Der Erwerb einer Cyberversicherung kann allerdings KMU dabei helfen, sich gegen Angriffe zu wappnen, indem er ihre größten potenziellen Risiken im Rahmen eines umfassenden Risikomanagements identifiziert und abmildert. Viele Cyberversicherer stellen ihren Kunden zudem spezialisiertes Fachwissen und Ressourcen zur Verfügung, um die Auswirkungen eines Vorfalls zu verringern und die Auszahlungen zu minimieren.

$850k

Die durchschnittlichen internationalen Kosten eines Ransomware-Vorfalls für kleine und mittlere Unternehmen.

„Von kleinen Start-ups bis hin zu globalen Giganten – Unternehmen sind zunehmend auf vernetzte Geräte in irgendeiner Form angewiesen. Während dies den Unternehmen enorme Vorteile und Chancen bietet, erhöht die zunehmende Abhängigkeit von Technologie auch das potenzielle Risiko von Schäden durch Cyberbedrohungen."

— Verband der britischen Versicherer

Was deckt eine Cyber-Risikoversicherung ab?

(policenabhängig)

- Kosten für die Reaktion auf Vorfälle
- Rechts- und regulatorische Kosten
- IT-Sicherheits- und Forensikkosten
- Kosten für Krisenkommunikation
- Kosten für das Management von Datenschutzverletzungen
- Kosten für das Management von Datenschutzverletzungen Dritter
- Nachträgliche Schadensbehebung nach einem Vorfall
- Betrug bei Geldtransfers
- Diebstahl von in Treuhand gehaltenen Geldern
- Diebstahl von persönlichen Geldern
- Erpressung
- Diebstahl der Unternehmensidentität
- Telefon-Hacking
- Push-Zahlungsbetrug
- Unbefugte Nutzung von Computerressourcen
- Systemschäden und Korrekturkosten
- Direkter Gewinnverlust und erhöhte Betriebskosten
- Zusätzliche erhöhte Betriebskosten
- Abhängige Betriebsunterbrechung
- Folgeschäden durch Reputationsverlust
- Kosten für die Vorbereitung von Schadensersatzansprüchen
- Hardwareersatzkosten
- Haftung für Netzwerksicherheit
- Haftung im Bereich Datenschutz
- Haftung des Managements
- Regulatorische Geldbußen
- PCI (Compliance-) Strafen, Bußgelder und Bewertungen
- Verleumdung
- Verletzung von geistigen Eigentumsrechten
- Technologiefehler und -versäumnisse
- Gerichtskosten

Welche Leistungen bietet eine Cyber-Risikoversicherung?

Der Markt für Cyberversicherungen hat sich in den letzten 20 Jahren ständig weiterentwickelt, parallel zur zunehmenden Bedrohung durch Cyberangriffe. Das erste Cyberversicherungsangebot wurde aus Berufshaftpflicht-Policen abgeleitet und konzentrierte sich auf Risiken durch Online-Software, Website-Inhalte und -Medien.

Mit dem Aufkommen von E-Commerce und digitalen Geschäftsprozessen wurde die Deckung auf Datenverlust, Schäden durch Viren und Malware sowie Netzwerksicherheitsverletzungen erweitert. Regulatorische Strafen, Betriebsunterbrechungen, Insider-Angriffe und Schäden an Netzwerkressourcen wurden häufig explizit von dieser Deckung ausgeschlossen.

Cyberversicherungen decken in der Regel sowohl Schäden ab, die direkt der eigenen Organisation entstehen (Eigenschaden), als auch Schäden, die Dritte betreffen, wie Kunden oder Partner (Drittschaden). Auch wenn es Unterschiede zwischen den einzelnen Policen gibt, bieten die meisten Anbieter ähnliche Leistungen für beide Schadensarten.

Welche Risiken sind möglicherweise ausgeschlossen?

Mit der stetig zunehmenden Vernetzung und dem fortschreitenden Zugänglichmachen von Daten werden Cyberversicherer voraussichtlich ihren Deckungsumfang entsprechend erweitern. Dieser Trend wird den Stellenwert einer Cyberversicherung für das Risikomanagement nicht nur für einzelne Unternehmen, sondern auch für die gesamte globale Wirtschaft weiter verstärken.

Gleichzeitig nutzen Versicherer Datenanalysen, um ihre Schadensquote durch strengere Risikoprüfungen und kontinuierliche Prämienerhöhungen zu verbessern. Sie verringern ihre Risikobelastung durch folgende Maßnahmen:

- **Reduzierung der Auszahlungslimits** für verschiedene Schadenskategorien
- **Erhöhung der Selbstbeteiligung der Versicherungsnehmer**, d. h. des Betrags, den der Versicherte vor Beginn der Deckung selbst zahlen muss
- **Erhöhung der Transparenz in Bezug auf die Cybersicherheitskonzepte von Organisationen** (bis hin zu einer Prüfung), um ihre tatsächliche Risikobelastung genauer zu beurteilen und die Preisgestaltung festzulegen
- **Weiterhin Betonung präventiver Cybersicherheitsmaßnahmen**, um das Cyberrisiko zu senken
- **Strengere Auswahl von Risiken**, die akzeptiert werden, und von Branchen, die bedient werden

Was sind die häufigsten Ausnahmeregelungen in Policen?

- Finanzbetrug durch Social-Engineering-Angriffe wie Business-Email-Compromise (BEC) oder Spearphishing. Häufig werden verlorene Gelder nicht erstattet, wenn sie freiwillig von einem Mitarbeiter gezahlt wurden.
- Kosten für die Erhöhung der Cybersicherheit nach erfolgreichem Angriff. Diese Investitionen können zukünftige Cyberversicherungsprämien senken und/oder einem Unternehmen helfen, eine Cyberversicherung zu erhalten oder behalten. Obwohl diese Kosten möglicherweise nicht gedeckt sind, kann der Versicherer einen „Breach Coach" oder Berater bereitstellen oder empfehlen, um Schwachstellen zu identifizieren und die Cybersicherheit zu verbessern.
- Potenzieller Verlust von zukünftigen Gewinnen durch langfristige Schäden wie Datenverlust, Diebstahl von geistigem Eigentum, Rufschädigung etc. Diese langfristigen Auswirkungen können den Umsatz, den Marktanteil, die Rekrutierung von Talenten und mehr beeinträchtigen. Allerdings ist es ziemlich schwierig, sie ausschließlich einem Cybervorfall zuzuordnen.
- Verminderter Wert von geistigem Eigentum nach Diebstahl vertraulicher Materialien wie neuer Produktdesigns. Der Verlust von Daten durch einen Cyberangriff kann ein Unternehmen stark schädigen oder seinen Marktanteil schwächen, aber dieses Risiko ist in der Regel nicht durch die Versicherung abgedeckt.
- Angriffe von Staaten oder Kriegshandlungen. Mittlerweile schließen einige Policen explizit eine Deckung für Angriffe aus, die als „Kriegshandlung" erklärt oder einem staatlichen Akteur zugeschrieben werden. Es gibt viele offene Fragen zur Anwendung solcher Klauseln, z. B. wie die Beteiligten entscheiden, was ein nationalstaatlicher Angriff ist.
- Geografische Einschränkungen, wo Deckungen gültig sind. Zum Beispiel werden möglicherweise Operationen außerhalb des Heimatlandes nicht vollständig abgedeckt. Oder eine Police, die außerhalb des Heimatlandes abgeschlossen wurde, könnte Einschränkungen für Aktivitäten im Heimatland enthalten.

Ein Versicherer wird einen Schaden nur dann ersetzen oder zuvor absichern, wenn die getroffenen Maßnahmen für die jeweilige Organisation als angemessen angesehen werden können und somit das Risiko von Sicherheitsvorfällen nachweislich minimiert wurde. Versicherungsnehmer sollten daher unbedingt ihrer Verantwortung für den ↗Stand der Technik[7] nachkommen.

Versicherer können für einige oder alle der oben genannten Risiken Zusatzdeckungen anbieten. Unternehmen sollten sorgfältig abwägen, wie wahrscheinlich das Eintreten dieser Risiken ist und welche möglichen Schäden daraus resultieren könnten, bevor sie auf Zusatzversicherungen oder wichtige Schutzmaßnahmen verzichten.

Wie immer bestimmt die genaue Formulierung der Policen und Ausschlüsse maßgeblich den Umfang der Abdeckung. Daher ist es entscheidend, Cyber-Risikoversicherungsverträge gründlich zu prüfen und bei Unklarheiten einen Rechtsexperten zu Rate zu ziehen.

Die Frage, wer hinter einem bestimmten Hackerangriff steckt, hat bereits Schlagzeilen gemacht. Das US-amerikanische Lebensmittelunternehmen Mondelez, das von der NotPetya-Malware betroffen war, verklagt die große Versicherungsgesellschaft Zurich, weil sie sich weigert, im Rahmen einer allgemeinen Versicherungspolice zu zahlen. Zurich beruft sich auf eine Ausschlussklausel für Schäden im Zusammenhang mit Kriegshandlungen, mit der Begründung, dass der Angriff von Russland verübt worden sein soll.

Sogar eine technologisch hoch entwickelte Regierung hätte Schwierigkeiten, einen solchen Vorwurf mit der von einem Gericht geforderten Beweislast zu untermauern.

Sollte Zurich allerdings gewinnen, könnte dies den gesamten Markt erheblich verunsichern – es sei denn, Versicherer akzeptieren, dass Cyber-Versicherungen auch Risiken abdecken müssen, die sie bislang zu vermeiden suchten.

— Andrew Coburn, Risk Management Solutions

Was ist mit der Absicherung von Ransomware?

Ransomware-Angriffe – in Versicherungspolicen meist als „Erpressung" oder „Cyber-Erpressung" bezeichnet – machen einen Großteil der Cyber-Versicherungsansprüche aus, unabhängig von Unternehmensgröße oder Branche. Laut einer Studie von NetDiligence waren Ransomware-Vorfälle von 2018 bis 2022 für rund 85 Prozent der Schadensmeldungen verantwortlich, einschließlich der Kosten für die Wiederherstellung (Kosten für die Vermeidung und Minimierung von Geschäftsunterbrechungen).

Auch wenn betroffene Unternehmen kein Lösegeld zahlen, sind solche Angriffe oft extrem kostspielig und stören den Geschäftsbetrieb erheblich. Unternehmen sollten sich bestmöglich auf Ransomware-Attacken vorbereiten. Dazu gehören neben Cyber-Versicherungen auch bewährte Sicherheitsmaßnahmen wie externe Backups und regelmäßige Notfallübungen zur Überprüfung interner Prozesse und Richtlinien.

In der Hoffnung, ihre Schadensquoten zu begrenzen und die Kosten für Ransomware-Zahlungen zu senken, bauen Versicherer vermehrt dahingehende Einschränkungen in ihre Policen ein oder finden immer mehr Möglichkeiten, die Ansprüche auf solche Schäden ganz oder teilweise abzulehnen. Darüber hinaus fordern sie unter anderem verstärkt sogenannte „Ransomware-Readiness"-Bewertungen und setzen auf professionelle Vermittler, um ihr Risiko zu begrenzen. Laut der Insurer Coalition konnten durch solche Verhandlungen Lösegeldzahlungen um 64 Prozent gesenkt werden.

Die Deckelung von Ransomware ist meist als Zusatzoption mit einer Obergrenze in einer umfassenderen Cyber-Versicherung integriert. Beispielsweise könnte in Deutschland eine Versicherungspolice mit einer Gesamtabdeckung von 1 Million Euro eine Obergrenze von lediglich 50.000 Euro für Ransomware enthalten – je nach individuellem Risiko des Versicherungsnehmers. Eigenständige Ransomware-Versicherungen sind eine zunehmend gefragtere Alternative, insbesondere da einige Policen jetzt ausdrücklich die Ransomware-Deckung ausschließen.

Je nach Versicherung kann die Ransomware-Deckung folgende Leistungen umfassen:

- Zahlung des geforderten Lösegelds/ der Erpressersumme
- Unterstützung durch einen professionellen Ransomware-Vermittler
- Forensische Untersuchungen und Ermittlungen
- Schäden an Soft-, Hardware und Infrastruktur
- Kosten für die Wiederherstellung und Rekonstruktion von Daten
- Erstattung von Umsatzausfällen durch Betriebsunterbrechungen/Reputationsschäden

Unabhängig von der gewählten Versicherung ist es entscheidend, die Vertragsbedingungen im Wortlaut genau zu prüfen und zu analysieren, bevor Sie eine Forderung stellen. So wissen Sie, welche Leistungen abgedeckt sind und welche Kosten möglicherweise unter eine Ransomware-Deckelung fallen oder ausgeschlossen sind.

3. Anforderungen
für den Abschluss einer Cyber-Risikoversicherung

Versicherungen gegen Cyberrisiken sind im Vergleich zu anderen Policen noch relativ neu. Anfangs waren Versicherer bei der Erstellung von Verträgen eher lockerer. Zu Beginn hatten sie kein klares Verständnis von den Risiken. Heute wissen Versicherer mehr über die Kosten und Gefahren von Cyberkriminalität – und stellen deutlich höhere Anforderungen an die Sicherheit ihrer Kunden. Ihre Policen und Preisberechnungen haben die Anbieter mittlerweile stark überarbeitet.

Die meisten Cyber-Versicherungen beginnen mit einem ausführlichen Fragebogen, oft im „Ja/Nein"-Format. Wer bereits über eine gute IT-Sicherheitsstrategie verfügt, kann diesen Schritt schnell durchlaufen. Unternehmen mit weniger Schutzmaßnahmen sollten ihre IT-Security vorab verbessern, um sich für eine Versicherung zu qualifizieren und bessere Konditionen zu erhalten.

Eines steht fest: Cyber-Risikoversicherungen werden immer wichtiger. Laut führenden Versicherungsquellen ist der Markt von 7,2 Milliarden US-Dollar im Jahr 2020 auf 13,8 Milliarden US-Dollar im Jahr 2024 gewachsen. Der Versicherungskonzern Zurich erwartet, dass dieser Wert bis 2027 auf 33,3 Milliarden US-Dollar steigen wird.

In Deutschland hat der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) bereits 2017 erstmals Musterbedingungen und einen Risikofragebogen speziell für KMU entwickelt – für Betriebe mit bis zu 250 Mitarbeitern und einem Jahresumsatz von maximal 50 Millionen Euro. Der Fokus auf diese Zielgruppe kommt nicht von ungefähr: Gerade KMU haben es aufgrund von Fachkräftemangel, Zeitdruck und begrenzten Budgets oft schwer, effektive Cybersicherheitsmaßnahmen umzusetzen. Doch auch große Unternehmen sind nicht vor Angriffen sicher, wenn ihre IT-Sicherheit nicht ausreicht.

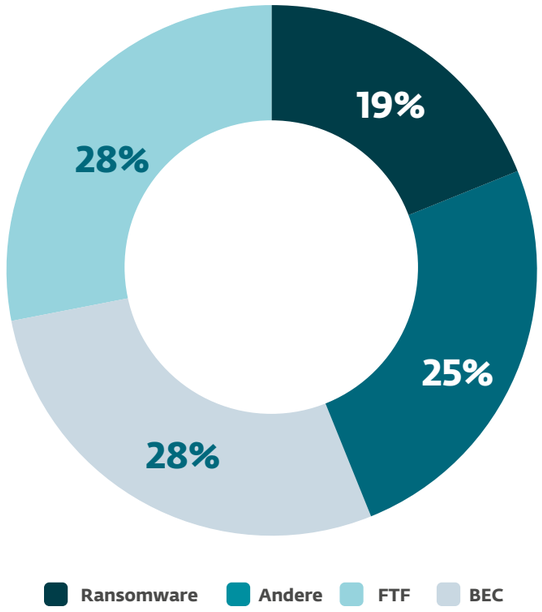


Abb11: Gesamtmeldungen von Ansprüchen nach Ereignistyp

Die vier Bausteine

einer Cyber-Risikoversicherung

Basis

Grundsätzlich sind nur Vermögensschäden versichert, die im Zuge einer Informationssicherheitsverletzung entstanden sind. Laut GDV ist eine „Informationssicherheitsverletzung […] eine Beeinträchtigung der Verfügbarkeit, Integrität, Vertraulichkeit von elektronischen Daten des Versicherungsnehmers oder von informationsverarbeitenden Systemen, die er zur Ausübung seiner betrieblichen oder beruflichen Tätigkeit – auch mittels Fernzugriff – nutzt."

Service Prozent Kosten

Der GDV legt fest, welche Kosten die Versicherung übernimmt. Dazu gehören laut Verband „Kosten, die infolge einer Verletzung datenschutzrechtlicher Vorschriften für die Prüfung und Erfüllung gesetzlicher oder behördlicher Informationspflichten entstehen." Darunter zählen z.B. IT-Forensik-Experten zur Analyse, Beweisaufnahme und Schadensbegrenzung sowie externe PR-Berater für die Krisenkommunikation und Wiederherstellung der Marke.

Drittschaden

Dieser Baustein enthält Elemente einer klassischen Haftpflichtversicherung. Entsteht einem Dritten durch eine Informationssicherheitsverletzung ein rechtlicher oder vertraglicher Schaden, kann er Ansprüche gegenüber dem Versicherungsnehmer geltend machen. Zu solchen Drittansprüchen zählen z. B. immaterielle Schäden durch Verletzungen des Persönlichkeits- oder Namensrechts sowie Verstöße gegen das Urheber- oder Markenrecht.

Eigenschaden

Hierin finden sich Elemente einer klassischen Betriebsunterbrechungsversicherung. Kommt es infolge einer Informationssicherheitsverletzung zu einem Stillstand, weil elektronische Daten oder IT-Systeme nicht mehr zugänglich sind und dadurch finanzielle Verluste entstehen, übernimmt die Versicherung die Kosten. Dazu zählen auch Ausgaben für die Wiederherstellung von Daten und Systemen.

Methoden zur Bewertung des eigenen Cyber-Risikos

Unternehmen können ihr Cyber-Risiko systematisch analysieren – von der Beantwortung standardisierter Fragebögen bis hin zur Nutzung etablierter Bewertungssysteme. Eine gründliche Bewertung der eigenen Cybersicherheitslage hilft Unternehmen dabei, Risiken frühzeitig zu erkennen und gezielt gegenzusteuern. Standardisierte Fragebögen umfassen:

- **Vergleich mit Mitbewerbern:** Unternehmen können ihre Sicherheitslage im Marktumfeld einordnen.
- **Analyse der Anbieter:** Identifikation von Partnern mit starker Sicherheitsinfrastruktur oder potenziellen Schwachstellen.
- **Transparenz in der Lieferkette:** Erkennen von Sicherheitslücken bei direkten und indirekten Dienstleistern.
- **Versicherbarkeit bewerten:** Grundlage zur Ermittlung von Cyber-Versicherungsprämien und Konditionen.

Bei der Risikobewertung für eine Cyber-Versicherung spielen mehrere Faktoren eine Rolle. Versicherer könnten unter anderem folgende Fragen stellen:

- **Welche sensiblen Daten verarbeitet Ihr Unternehmen?** Dazu zählen z. B. Kreditkarteninformationen, Gesundheitsdaten, personenbezogene Daten, Geschäftsgeheimnisse oder biometrische Zugangsdaten.
- **Wie groß ist das Datenvolumen?** Handelt es sich um einige wenige Datensätze oder um Hunderttausende?
- **Unterliegt Ihr Unternehmen bestimmten Datenschutzvorschriften?** Beispielsweise DSGVO, NIS/NIS2 oder DORA. Falls ja: Können Sie die Einhaltung dieser Vorschriften nachweisen?

Neben Typ und Menge der verarbeiteten Daten stellen Versicherer weitere gezielte Fragen:

- **Orientiert sich Ihr Cybersicherheitskonzept an etablierten Standards?** Wie ISO 27001, TISAX, Cyber Essentials o.ä.
- **Gibt es externe Partner mit Zugriff auf Ihre IT-Systeme?** Falls ja, welche Maßnahmen ergreifen Sie zur Überprüfung und Absicherung dieser Zugriffe?
- **Nutzen Mitarbeiter mobile Endgeräte für Unternehmensdaten?** Beispielsweise Laptops, Tablets oder Smartphones – und welche Sicherheitsrichtlinien gibt es dafür?
- **Gibt es definierte Informationssicherheitsrichtlinien?** Und ist ein Chief Information Security Officer (CISO) oder eine vergleichbare Position für die Cybersicherheit verantwortlich?

Unternehmen müssen auch Ihre Technologieumgebung und Kontrollen bewerten:

- **Nutzt Ihr Unternehmen Multi-Faktor-Authentifizierung (MFA)** für den Zugriff auf alle kritischen Systeme und das Unternehmensnetzwerk?
- **Haben Sie eine Firewall?** Von welchem Anbieter?
- **Setzen Sie einen E-Mail-Filter oder eine Antispam-Lösung ein**, um Phishing-E-Mails zu blockieren?
- **Verfügen Sie über eine Passwortrichtlinie nach Best Practices**, die konsequent durchgesetzt wird?
- **Haben Sie Antiviren- und Antimalware-Software** zum Schutz vor Cyberbedrohungen?
- **Setzen Sie ein Intrusion Detection System (IDS) oder ein Intrusion Prevention System (IPS) ein**, um unbefugte Zugriffe auf Ihr Netzwerk zu erkennen oder zu verhindern?

Anforderungen
an die IT Security von Organisationen und Unternehmen

Multi-Faktor-Authentifizierung (MFA)

Passwörter bieten heutzutage keinen ausreichenden Schutz mehr. Ohne Multi-Faktor-Authentifizierung (MFA) für Fernzugriffe, privilegierte Konten und sensible Anwendungen können vertrauliche Daten nicht vor unbefugtem Zugriff geschützt werden – und Sie könnten Schwierigkeiten haben, überhaupt eine Cyber-Risikoversicherung abzuschließen.

Best-Practice Backups

Sie sind entscheidend, um sich vor den kostspieligen Ransomware-Angriffen zu schützen. Eine effektive Strategie umfasst Verschlüsselung, regelmäßige Tests der Wiederherstellung und die Speicherung der Daten an einem sicheren, externen Ort.

E-Mail-Filter

Sie verhindern, dass Phishing-E-Mails Ihre Nutzer erreichen, wodurch das Risiko für Ihre Systeme und Daten erheblich gesenkt wird. Diese kostengünstige Lösung prüft in der Regel Anhänge und Links auf schadhafte Inhalte und hilft so, Bedrohungen frühzeitig abzufangen.

Schwachstellen- und Patchmanagement

Die Ausnutzung bekannter Schwachstellen öffnet Cyberkriminellen häufig Tür und Tor in ein Firmennetzwerk. Durch automatisiertes Scannen und Patchen lässt sich das Risiko erheblich verringern.

Endpoint Detection and Response (EDR)

EDR schützt vor Cyberangriffen, indem es Geräte sowie Aktivitäten innerhalb eines Firmennetzwerks überwacht und so tiefe Einblicke in die IT-Infrastruktur bietet. Werden Anomalien (z. B. in Form von irregulären Prozessen) erkannt, schlägt es Alarm und unterstützt Sie bei der Vorfallreaktion. Unternehmen ohne Sicherheitsspezialisten im Haus können Managed Detection and Response (MDR)-Angebote von externen Dienstleistern nutzen.

Privileged Access Management (PAM)

PAM schützt vertrauliche Daten, indem es privilegierte Konten wie Administratorenkonten mit strengeren Sicherheitsmaßnahmen absichert. PAM-Systeme funktionieren wie ein Tresor, der Zugangsdaten vor Diebstahl schützt und nur für berechtigte Aktivitäten zugänglich macht.

Regelmäßige Cybersicherheitsschulungen

So stellen Sie sicher, dass Mitarbeitende über aktuelle Bedrohungen und Sicherheitsverfahren informiert sind. Dadurch wird das Risiko von Cyberangriffen verringert und ein hohes Sicherheitsbewusstsein signalisiert, das von Versicherern positiv bewertet wird.

Erweiterte Fragen und Schutzmaßnahmen

- **Haben Sie Kundenverträge?** Falls ja, enthalten sie „Haftungsausschluss"-Klauseln, die Ihre Haftung im Falle eines Vorfalls reduzieren könnten?
- **Haben Ihre Cloud-Service-Anbieter von Dritten geprüfte Cybersicherheitsnachweise**, wie z. B. ISO 27001?

Zusammen mit den Risikoprofilen, die durch die Fragebögen und externe Scans ermittelt wurden, spielen die Cybersicherheitsmaßnahmen eines Unternehmens eine entscheidende Rolle bei der Bestimmung der Versicherbarkeit, der Deckungskonditionen und der Prämien.

Auf der einen Seite gibt es grundlegende Sicherheitskontrollen, die für den Abschluss einer Cyber-Versicherung erforderlich sind. Auf der anderen Seite können erweiterte Schutzmaßnahmen das Risiko eines Antragstellers weiter reduzieren und dazu beitragen, ein günstigeres Angebot zu erhalten. Zu diesen Maßnahmen gehören:

- Netzwerksegmentierung gemäß den Zero-Trust-Prinzipien
- Extended Detection and Response (XDR) mit kontinuierlicher Überwachung aller Endpoints
- Managed Detection and Response (MDR), das einen ausgelagerten EDR/XDR-Service mit kontinuierlicher Überwachung durch spezialisierte Analysten bietet
- Einsatz einer Lösung für Security Information and Event Management (SIEM) oder ein verwaltetes SIEM
- Regelmäßige Schwachstellenprüfung und Penetrationstests
- Eine Cybersicherheitszertifizierung oder ein Bericht auf Grundlage einer Drittanbieterprüfung, wie eine ISO 27001-Zertifizierung
- Dokumentierte Risikobewertungen und Datenmanagement-Richtlinien sowie Verfahren und Nachweise, dass anerkannte Vorgaben für Cybersicherheit befolgt werden

Der Abschluss einer Cyber-Versicherung ist ein komplexer Prozess, der an die spezifische IT-Konfiguration und die Rahmenbedingungen des Versicherungsnehmers angepasst wird. Das bedeutet, dass Unternehmen ihre individuellen Bedürfnisse genau abwägen sollten, bevor sie eine Entscheidung treffen. Für den Abschluss einer solchen Versicherung ist es entscheidend, dass Unternehmen sich ihres Cyber-Risikos bewusst sind und nachweisen können, dass sie die nötigen Maßnahmen ergriffen haben. In gewisser Weise ähnelt dies einer Hausbegehung in der analogen Welt, bei der Versicherer überprüfen, ob geeignete Schlösser und Alarmanlagen vorhanden sind.

> ***„Es ist ein grundlegendes Konzept, aber es ist überraschend, wie viele Organisationen entweder überhaupt keine Backups haben oder allgemein Backups der Daten und ihres Betriebssystems machen, aber nie überprüft haben, ob sie wiederhergestellt werden können."***
>
> — Ein Aspekt, auf den Professor Andrew Jones, einer der weltweit führenden Experten für Cyberforensik, bei der Erstellung dieses Whitepapers hinweist.

Die Entwicklung der Cyber-Risikoversicherung in DACH

Wie wichtig Cybersicherheitsmaßnahmen geworden sind, zeigt beispielsweise die jüngste Studie VDMA-Studie „Industrial Security und Produktpiraterie 2024".[8] Bei einer Umfrage im Verband deutscher Maschinen und Anlagenbau e.V. mit mehr als 3.600 Mitgliedsunternehmen haben mehr als die Hälfte der befragten Unternehmen eine Cyber-Risikoversicherungspolice abgeschlossen. Sechs Prozent mussten sie bereits in Anspruch nehmen. Darüber hinaus gab jedes vierte Unternehmen an, in den letzten zwei Jahren einen gravierenden Cybersicherheitsvorfall erlitten zu haben.

Das zunehmende Risiko für Cyberangriffe sorgte in den letzten Jahren dafür, dass Versicherer ihre Anforderungen und Mindestbedingungen an die IT-Sicherheit zunehmend verschärft haben. Unternehmen müssen immer tiefer in die Tasche greifen, um eine gute Cyber-Resilienz und Cyber-Hygiene vorzuweisen, die erheblichen Einfluss auf die Eintrittswahrscheinlichkeit und Schadenhöhe von Vorfällen haben.

Eine aktuelle, weltweite Umfrage aus 2024 unter mehr als 1.000 leitenden IT- und Cybersecurity-Entscheidern ergab, dass 55 Prozent der Unternehmen im DACH-Raum cyberversichert sind. Verglichen mit Skandinavien, den Benelux-ländern, dem Vereinigten Königreich und USA ist hier noch Luft nach oben. Laut Studie soll es vorwärts gehen: Knapp 40 Prozent der befragten Unternehmen wollen in naher Zukunft eine Cyberversicherung abschließen.[9]

Mit der verschärften Bedrohungslage steigen auch die Belastungen für Cyberversicherer. 2023 wurden 4.000 Hackerangriffe bei Versicherungen gemeldet, das waren knapp 19 Prozent mehr als im Jahr zuvor. Die Zahl der Schäden überstieg dabei die der abgeschlossenen Verträge. 180 Millionen mussten die Versicherer 2023 auszahlen, 50 Prozent mehr als noch 2022. Ein Cyber-Schaden kostete im Durchschnitt 45.370 Euro, im Vergleich zum Vorjahr ist dies ein Anstieg um 8,3 Prozent. Im Verlauf des Jahres wuchs die Zahl der Cyber-Versicherungen um fast 16 Prozent auf etwa 261.000.[10]

	Anzahl VU	Beiträge[2]		Leistungen[3]		Schadenquote[4]	Com
Jahr		in Mio. EUR	Veränderung gg. Vorjahr in Prozent	in Mio. EUR	Veränderung gg. Vorjahr in Prozent	in Prozent	
2020	33	106	x	37	x	35,1	
2021	39	178	49,2*	137	187,6*	77,0	
2022	41	249	56,3*	121	7,9*	48,6	
2023	41	309	24,5	180	49,8*	58,2	

- Wert gleich Null
° Wert liegt nicht vor
x Wert nicht sinnvoll

[1] inländisches Direktgeschäft
[2] gebuchte Brutto-Beiträge; ohne Versicherungsteuer
[3] Brutto-Aufwendungen für Versicherungsfälle des Geschäftsjahres
[4] Brutto-Aufwendungen für Versicherungsfälle des Geschäftsjahres in Relation zu den verdienten Brutto-Beiträgen
[5] Schaden-Kostenquote nach Abwicklung; in Relation zu den verdienten Brutto-Beiträgen
[6] Veränderungsraten: bereinigt aufgrund der Änderung der Grundgesamtheit

Quelle: GDV

Abb12: Geschäftsentwicklung in der Cyber-Riskoversicherungsbranche

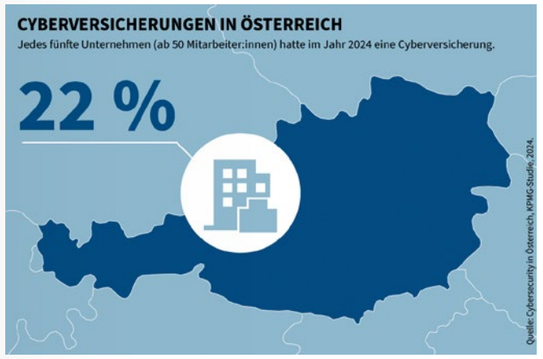


Abb13: Cyberversicherungen in Österreich

Datenerhebung Cyberversicherungen Schweiz 2020-2023

Teilnehmende Gesellschaften (16) - ausschliesslich Direktgeschäft: AIG, AXA (inkl. AXA XL), AXIS, Allianz (exkl. AGCS), Baloise, Chubb, Generali, Great Lakes, Helvetia, HDI, Liberty, Mobiliar, Swiss Re, Tokio Marine HCC, Vaudoise, Zurich

Geschäftsjahr	2023	2022 *	2021 *	2020 *
Bruttoprämien Total (Firmen+Privat) CHF Mio.	141	119	83	57
Anzahl Policen Total (Firmen+Privat)	399'000	332'000	267'000	205'000
Bruttoprämien Firmenkunden CHF Mio.	121	103	71	49
Anzahl Policen Firmenkunden	53'000	46'000	38'000	28'000
Bruttoprämien Privatpersonen CHF Mio.	20	16	12	8
Anzahl Policen Privatpersonen	346'000	286'000	229'000	177'000

*Anteil der Firmen mit Cyberversicherung: 8,7 %. * Die Zahlen für die Vorjahre wurden mit den Prämienvolumen von zwei neu teilnehmenden Gesellschaften ergänzt sowie von einzelnen Gesellschaften präzisiert. Deshalb weichen diese von den im Vorjahr kommunizierten Zahlen leicht ab.*

Quelle: SVV - Erstellt mit Datawrapper

Abb14: Entwicklung der Cyberversicherungen in der Schweiz von 2020 bis 2023

Ob eine Cyber-Risikoversicherung für jeden sinnvoll ist, müssen Unternehmer selbst entscheiden.

Eine ausführliche Analyse von über 90 Cyberversicherungsfällen von Schweizer Unternehmen zwischen 2016 und 2024 offenbart, dass die Sektoren Handel, Transport und Dienstleistungen am häufigsten von Cyberkriminalität betroffen sind[11]. Cyberversicherungen haben dabei etwa rund 75 Prozent der Schadenssumme abzüglich des Selbstbehalts gedeckelt und einige Unternehmen vor einem finanziellen Desaster bewahrt. Umso mehr verwundert es, dass laut der jüngsten Umfrage des Schweizer Versicherungsverbands (SVV) 2023 nur acht von 100 Unternehmen gegen Cyberrisiken versichert waren. Im Vergleich zum Vorjahr bedeutet das zwar einen Anstieg um einen Prozentpunkt, aber macht deutlich, dass Unternehmen die Bedrohung durch Cyberkriminalität immer noch nicht ernst genug nehmen.

4. Zusammenfassung
Prozent Ausblick

Um in der Geschäftswelt erfolgreich zu sein, muss eine Organisation ständig Herausforderungen und Risiken angehen und häufig Dinge überwinden, die ihre Existenz bedrohen können. Versicherungen bieten seit Jahrhunderten eine stabile Möglichkeit, einige dieser Risiken abzumildern. Sie ermöglichen es Unternehmen, sich auf Wachstum und Chancen zu konzentrieren und gleichzeitig Maßnahmen zu treffen, um mögliche Gefahren zu minimieren.

Schon vor dem Internet bot das digitale Zeitalter den Versicherern sowohl Chancen als auch Herausforderungen. In den Anfangsjahren verlangten Versicherer, dass Computerräume mit Halon-Feuerlöschsystemen ausgestattet sind. Als die Kosten für diese Technologie sanken, wurden wasserbasierte Systeme zur Brandbekämpfung zur Norm. Solche Entscheidungen werden auf Grundlage von Daten, der Wahrscheinlichkeit eines Schadenfalls und einer möglichen finanziellen Auszahlung getroffen. Mit der Zeit und sinkenden Kosten der Technik rückte zunehmend der Schutz des menschlichen Lebens in den Fokus der Versicherer.

Die größte Herausforderung für Versicherer in der heutigen digitalen Welt ist der Mangel an relevanten Daten. Die durch die Pandemie beschleunigte digitale Transformation und der Anstieg von Ransomware-Angriffen, insbesondere durch Kryptowährungen, haben die Situation innerhalb der letzten sechs Jahre deutlich verschärft. Diese Kombination aus der Notwendigkeit für Unternehmen, Risiken abzusichern, um ihre Überlebenschancen zu verbessern, und der Mangel an aussagekräftigen Daten führt dazu, dass Versicherer ihre Anforderungen ständig anpassen und die Prämien in rasantem Tempo steigen.

Darüber hinaus spielt die Verfügbarkeit von Künstlicher Intelligenz (KI) eine immer größere Rolle. Sie ist mittlerweile ein kostengünstiges Werkzeug, das Unternehmen helfen kann, ihr Geschäft zu erweitern – sowohl aus finanziellen als auch aus Effizienzgründen. Doch wie bei jeder neuen Technologie entstehen auch hier unbekannte Risiken, etwa die Möglichkeit, dass Cyberkriminelle KI missbrauchen könnten, um Erpressermethoden zu optimieren.

> ***„Die Cyber-Versicherungsbranche wird eine entscheidende Rolle dabei spielen, die Sicherheitsstandards in allen Bereichen und Branchen zu erhöhen. Dies erfolgt durch die Anforderungen, die Unternehmen erfüllen müssen, um entweder die richtige Prämie zu erhalten oder überhaupt eine Versicherung zu bekommen.“***
>
> — Richard Breavington, Anwalt und Partner bei RPC, Leiter für Cyber- Prozent Technologieversicherungen

Heute ist es für Unternehmen unerlässlich, Cybersecurity-Maßnahmen zu ergreifen, die den bestmöglichen Schutz bieten – unabhängig davon, ob sie eine Versicherung haben oder nicht. Versicherer, die das Risiko anhand von Daten bewerten, fordern eine Vielzahl von Technologien und Prozessen, wie etwa den Einsatz von Backup-Systemen, Multi-Faktor-Authentifizierung und fortschrittliche Endpoint Detection and Response (EDR)-Lösungen. Diese Anforderungen stimmen oft mit den Empfehlungen von Cybersicherheitsexperten und -vorgaben überein.

Die Versicherer sind darauf fokussiert, das Risiko eines finanziellen Schadens zu minimieren, die Cybersicherheitsbranche wiederum konzentriert sich darauf, das Risiko eines Cyberangriffs zu verringern. Der Nutzen für alle Unternehmen besteht darin, die Anforderungen, die beide Seiten benötigen oder empfehlen, zu verstehen und die relevanten Maßnahmen umzusetzen. So können sie eine optimale Cybersicherheitslage und das geringste finanzielle Risiko erreichen.

Diese Beziehung zwischen Cyberversicherung und Cybersicherheit ist untrennbar miteinander verbunden. Da sich die Einnahmen aus Cyber-Risikoversicherungen voraussichtlich Jahr um Jahr fast verdoppeln, entwickeln sich diese beiden Branchen schnell zu einer Zweckgemeinschaft.

Ein großes Hindernis bleibt, das diese Beziehung zu einer glücklichen und wirklich erfüllenden Partnerschaft machen könnte: Die Finanzierung von Cyberkriminalität durch die Zahlung von Ransomware-Forderungen durch Versicherer muss gestoppt werden, es sei denn, es liegen außerordentliche Umstände vor.

5. IT-Sicherheit ist Vertrauenssache

ESET bietet Informationssicherheit für Unternehmen jeder Größe

ESET Made in EU IT-Security

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:

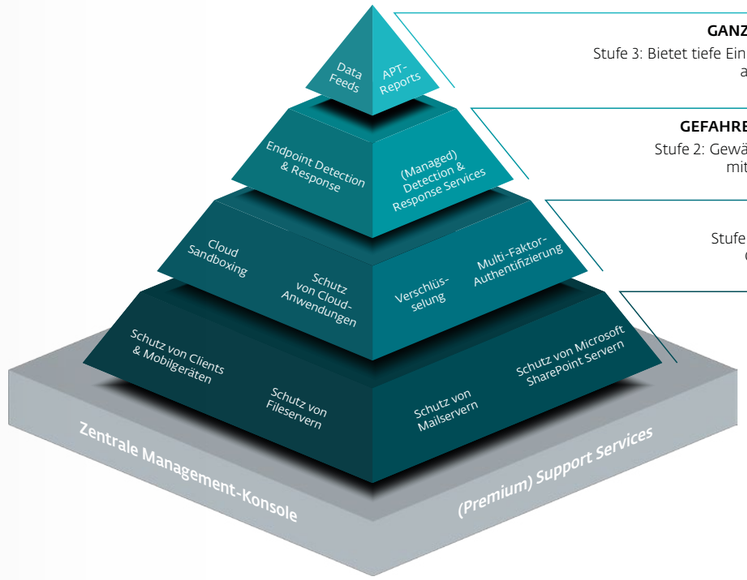
- Passgenaue IT-Sicherheit für alle Unternehmensgrößen und -anforderungen
- Mitarbeiter entlasten und (Hardware-) Ressourcen schonen
- Compliance und Sicherheitsstandards erweitern
- Verwaltung der Schutzlösungen für alle gängigen Betriebssysteme via ESET PROTECT (Cloud oder On-Premises)
- Lizenzvielfalt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

„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

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 Prozent 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.

Quellenverzeichnis

Abbildungsverzeichnis

Abbildung 1: Kosten durch Cyberkriminalität: Entstandene Schäden und erwartete Kosten; Dr Michael McGuire, World Economic Forum; CyberVentures; Statista

Abbildung 2: Laut Forsa-Umfrage ist das Risiko hoch, aber nur für andere.; https://app.23degrees.io/view/Y2STXQ8RwIw23SJg-bar-stacked-horizontal-cyber-2024-1-risikowahrnehmung

Abbildung 3: Nur 31% erfüllen die Anforderungen an den kompletten Basisschutz.; https://app.23degrees.io/view/SICGTpOUXYy2pWYz-bar-stacked-horizontal-pk-cyber-2024-x-basissicherheit

Abbildung 4: Der wirtschaftliche Schaden ist zum Vorjahr erneut gestiegen.; https://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf, Seite 4

Abbildung 5: Cybervorfälle halten Schweizer Unternehmen für die größte Gefahr.; https://app.23degrees.io/view/IA6ULwiBYfetWPuI-bar-horizontal-top-10-geschaeftsrisiken-in

Abbildung 6: Betriebsunterbrechungen waren 2024 häufigste Folge nach einem Angriff auf Schweizer Unternehmen.; https://www.onlinesicherheit.gv.at/Services/News/Cyberversicherungen-Ueberblick-Infografiken.html

Abbildung 7: In Österreich konnten 2024 Unternehmensdaten weniger gerettet werden.; https://www.onlinesicherheit.gv.at/Services/News/Cyberversicherungen-Ueberblick-Infografiken.html

Abbildung 8: Gesamtkosten einer Datenschutzverletzung in Mio.; https://www.ibm.com/reports/data-breach

Abbildung 9: Verteilung der Kosten für Krisendienste; https://netdiligence.com/cyber-claims-study-2023-report/

Abbildung 10: Durchschnittliche Kosten für Ransomware; https://netdiligence.com/cyber-insurance-claims-study/

Abbildung 11: Gesamtmeldungen von Ansprüchen nach Ereignistyp; https://info.coalitioninc.com/download-2024-cyber-claims-report.html

Abbildung 12: Geschäftsentwicklung in der Cyber-Riskoversicherungsbranche; https://app.23degrees.eu/view/l6OjbPgz3yGO-TuWD-table-tab-85-s-86-or

Abbildung 13: Cyberversicherungen in Österreich; https://www.onlinesicherheit.gv.at/Services/News/Cyberversicherungen-Ueberblick-Infografiken.html

Abbildung 14: Entwicklung der Cyberversicherungen in der Schweiz von 2020 bis 2023; https://www.svv.ch/de/steigerung-des-cyber-praemienvolumens-um-185-prozent

Literaturverzeichnis

1 kmu.admin.ch

2 NetDiligence Cyber Claims Study 2023; https://netdiligence.com/cyber-claims-study-2023-report/

3 Aktuelle Untersuchungen; https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business

4 Durchschnitt bei 850.000 US-Dollar; https://netdiligence.com/wp-content/uploads/2023/10/2023-NetDiligence-Cyber-Claims-Study_v1.1.pdf

5 In Großbritannien haben jedoch nur 10 % der KMU eine Cyber-Risiko-Versicherung; https://www.abi.org.uk/globalassets/files/subject/public/cyber/the-value-of-cyber-insurance-to-the-uk-economy-november.pdf

6 In Deutschland liegt dieser Anteil bei 12 % und in den USA bei 21 % – allesamt niedriger als erwartet angesichts der Vorteile einer Cyberversicherung; https://www.abi.org.uk/globalassets/files/subject/public/cyber/the-value-of-cyber-insurance-to-the-uk-economy-november.pdf

7 Whitepaper Stand der Technik; https://go.eset.com/eset-dach/eset-whitepaper-stand-der-technik

8 https://unternehmen-cybersicherheit.de/vdma-studie-signifikante-cybersicherheitsvorfaelle-in-jedem-vierten-unternehmen/

9 https://midrange.de/mehr-als-die-haelfte-der-dach-unternehmen-haben-mittlerweile-eine-police/

10 „Statistiken zur deutschen Versicherungswirtschaft 2024“, Gesamtverband der Deutschen Versicherungswirtschaft (GDV)

11 ausführliche Analyse von über 90 Cyberversicherungsfällen von Schweizer Unternehmen; https://www.it-markt.ch/cybersecurity/2021-05-31/wie-schweizer-versicherer-mit-ransomware-opfern-umgehen/0It0

↗www.eset.com/de/business/small-and-medium/

3 VON ÜBER 500.000 ZUFRIEDENEN KUNDEN

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

Secur|Ty 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 Informations-sicherheitsstandards ISO 9001:2015 und ISO/IEC 27001:2022 zertifiziert

ESET IN ZAHLEN

110.000.000+
Geschützte Nutzer weltweit

176
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