CHUBB®

Cyberrisiken immer einen Schritt voraus.

Stärken Sie Ihren
Cyber-Schutz mit Chubb.

Inhalt

Die Entwicklung von Chubb 3

Cyber-Risikoumfeld 4

Aktuelle Trends 5

Drängende Fragen zum Datenschutz und mehr 6

Dienstleistungen zur Schadensbegrenzung 7

Threat Intelligence und Cyber Risk Advisory Team 8

Incident Response Team und Schadenfälle 9

DIE ENTWICKLUNG VON CHUBB

Ihre Cyber-Infrastruktur braucht ein solides Fundament. Am besten von einem globalen Marktführer.

Durch die Globalisierung und Digitalisierung der Wirtschaft sind starke gegenseitige Abhängigkeiten entstanden, die zahlreiche Risiken bergen.

Chubb unterstützt seit mehr als 25 Jahren Unternehmen beim Management von Cyberrisiken. Heute sind wir der weltweit führende Anbieter von Cyberversicherungen[1] – eine Position, die wir uns durch kontinuierliche Innovation, die Einführung neuer Deckungsoptionen und die Entwicklung wegweisender Dienstleistungen im Bereich Cyber-Risikomanagement angesichts einer sich ständig verändernden Bedrohungslage erarbeitet haben. Unsere Cyber-Schadenexperten haben weltweit mehr als 32.500 Cyber-Schadenfälle bearbeitet. Sie pflegen enge Beziehungen zu erstklassigen Incident-Response-Spezialisten, die Versicherungsnehmer bei der Minderung und Bewältigung von Cyber-Vorfällen unterstützen.

Ob durch Definitionen, die die neuesten Datenschutz- und Cybergesetze berücksichtigen, die intelligente Einbeziehung von Deckungserweiterungen oder die gezielte Auswahl von Cyber Risk Services zur Risikominderung – Chubb bietet, was Kunden heute und in Zukunft benötigen.

Unsere Cyber-Schadenexperten haben mehr als **32.500 Schadenfälle bearbeitet**.

UNSERE GESCHICHTE

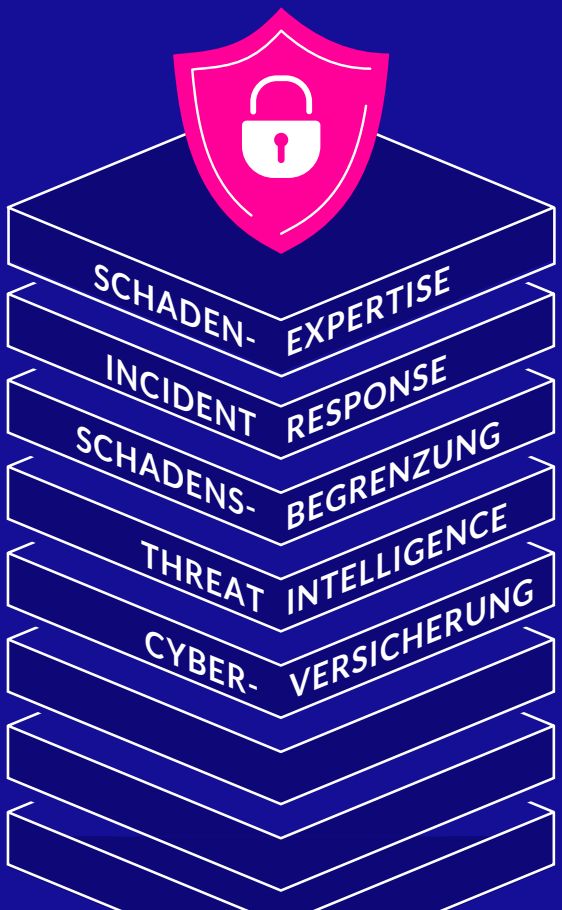
1998

Lancierung des ersten Cyber-Produkts.

2016

Lancierung von Cyber ERM und des Technology Master Package, fast 20 Jahre nach der Entwicklung unseres ersten Produkts.

Chubb ist einer der weltweit führenden Anbieter von Cyberversicherungen, gemessen an den Bruttoprämien.[1]



5,4 Milliarden

Internetnutzer im Vergleich zu 2,6 Milliarden vor 10 Jahren.[2]

Mehr als 280.000

bekannte Schwachstellen (Common Vulnerabilities and Exposures, CVEs); **täglich kommen mehr als 100 neue hinzu.**[3]

Cyber-Unsicherheit

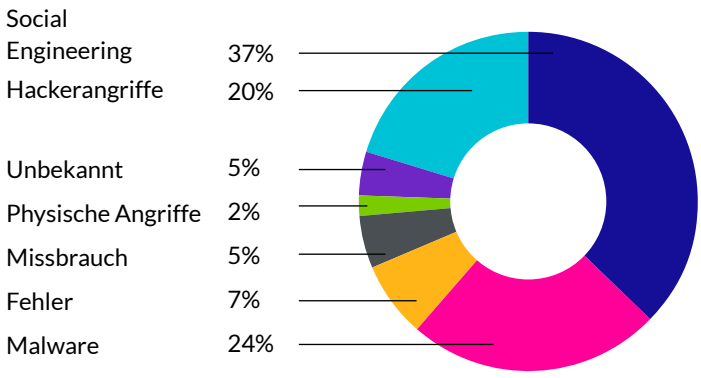
rangiert auf Platz 4 der 10 größten Risiken für die Gesellschaft.[4]

Wenn alle Zeichen gegen Sie stehen, ist es an der Zeit, Ihre Cyber-Infrastruktur zu stärken.

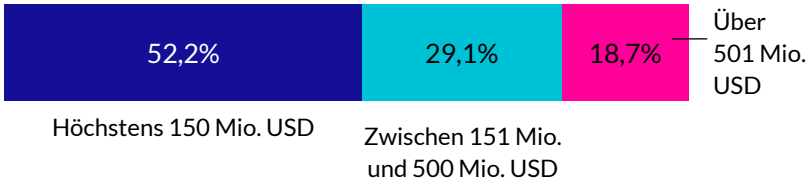
Trends bei Cyberschäden

Unternehmen jeder Größe sehen sich mit immer raffinierteren Social-Engineering-Angriffen konfrontiert, die zu Datenschutzverletzungen, Ransomware-Ereignissen und Reputationsschäden führen können. Unser **Cyber Index** berücksichtigt die verschiedenen Auslöser von Cybervorfällen und zeigt, warum Unternehmen die Cyber Services von Chubb nutzen sollten, darunter auch viele Services für kleine Unternehmen mit bis zu 100 Mitarbeitern.

Handlungen, die zu Cybervorfällen führen – gleitender 12-Monatszeitraum, USA, alle Branchen, Umsatz unter 150 Mio. USD



Anteil der jährlichen Schadenfälle nach Jahresumsatz seit 2023



Chubb Cyber Index

Bietet Echtzeit-Zugriff auf Schadendaten von Chubb sowie Einblicke in aktuelle Cyber-Bedrohungen, Trends und Kosten. Nutzer können Bereiche definieren und sich historische Trends nach Art der Bedrohung, Unternehmensgröße und Branche anzeigen lassen.

Unfälle passieren:

Laut dem Verizon Data Breach Investigations Report (DBIR)[5]

68% der Sicherheitsverletzungen waren auf nicht böswillige menschliche Handlungen zurückzuführen

28% der Sicherheitsverletzungen waren auf Fehler zurückzuführen

15% der Sicherheitsverletzungen waren auf Dritte zurückzuführen

DRÄNGENDE FRAGEN ZU DATENSCHUTZ UND MEHR

Eine gute Cyber-Infrastruktur umfasst auch den Schutz vor unbeabsichtigten Datenschutzverletzungen.

Nicht alle Cyber-Risiken sind auf Hacker zurückzuführen. Im Zuge des technischen Fortschritts entwickeln sich auch die Vorschriften weiter. Mit Niederlassungen in mehr als 50 Ländern und einem der größten Cyber Underwriting Teams der Welt unterstützen wir unsere Kunden dabei, die neuesten Risiken zu erkennen und zu steuern.

Wir bei Chubb unterstützen unsere Kunden nicht nur bei der Identifikation und Steuerung von Risiken, sondern bieten ihnen auch einen umfassenden Versicherungsschutz für eine Vielzahl von Risiken. Wir bieten umfassende Versicherungslösungen, die auf die individuellen Bedürfnisse der Unternehmen zugeschnitten sind.

In den letzten zwei Jahren sind die Schadenfälle aufgrund von Datenschutz-verletzungen um 210%[6] gestiegen

DSGVO und BIPA

Die Datenschutz-Grundverordnung (DSGVO) trat 2018 in Kraft. Sie regelt die Erhebung, Verwendung, Speicherung und Löschung von Daten. In vielen Ländern gibt es Gesetze, die es Opfern von Datenschutzverletzungen ermöglichen, private Schadenersatzklagen zu erheben, auch wenn kein finanzieller Verlust oder objektiv nachweisbarer Schaden vorliegt.

Biometrische Daten bleiben als besondere Datenkategorie im Fokus der DSGVO, wobei für die Erhebung, Verwendung und Verarbeitung biometrischer Daten häufig eine Einwilligung erforderlich ist. Für Unternehmen mit US-Bezug war der 2008 in Illinois verabschiedete Biometric Information Privacy Act (BIPA) das erste Gesetz, das einen zunehmend populären Standard für private Klagen gegen Organisationen festlegte – mit Bußgeldern bei Nichteinhaltung.

Cookies, Web Beacons und Pixel

Cookies, Web Beacons und Pixel sind Codes, die auf Websites verwendet werden, um das Nutzerverhalten für Kundenprofile, gezielte Werbung oder Datenanalysen zu verfolgen. Für die Erfassung von Daten mithilfe solcher Tracking-Technologien ist die Einwilligung der Nutzer erforderlich. Wird diese Einwilligung nicht eingeholt, stellt dies einen Verstoß gegen Datenschutzbestimmungen wie die DSGVO dar.

Bei Versicherungsnehmern mit Nutzern in den USA sehen wir weiterhin Klagen wegen Datenschutzverletzungen nach dem Video Privacy Protection Act (1988). Weltweit häufen sich Klagen wegen unzulässiger Nutzung dieser Technologie oder der Offenlegung von Videonutzungs-gewohnheiten. Die Kläger führen an, dass personenbezogene Daten ohne Einwilligung der Nutzer weitergegeben wurden. Dieses Risiko ist allgegenwärtig, und die Strafen können erheblich sein.

Künstliche Intelligenz (KI)

Während die Ausschöpfung des vollen Potenzials von KI für Organisationen auf der ganzen Welt oberste Priorität hat, ist eine wirksame Regulierung von KI trotz der Bemühungen der Regierungen nach wie vor schwierig. Die Minderung von Sicherheitsrisiken im Zusammenhang mit KI hat sich als ein Prozess von Versuch und Irrtum erwiesen. KI ist in einige Abwehrtools integriert, wird aber auch von Angreifern als Waffe eingesetzt.

Digitale operationale Resilienz

Die Vorschriften zur Stärkung der digitalen operationalen Resilienz entwickeln sich rasch weiter. In der EU sind in den letzten Monaten die Verordnung zur digitalen operationalen Resilienz (DORA) und die NIS-2-Richtlinie in Kraft getreten. Die Vorschriften konzentrieren sich auf den Finanzsektor und kritische Infrastrukturen. Sie sehen strenge Fristen für die Berichterstattung und Geldstrafen bei Nichteinhaltung vor.

SERVICES ZUR SCHADENSBEGRENZUNG

Auf eine starke Cyber-Infrastruktur sollten sie als Unternehmen nicht verzichten.

Alle Versicherungsnehmer, die eine Cyber-Deckung abschließen, haben Zugang zu kostenlosen oder vergünstigten* Services zur Schadensbegrenzung. Diese können dazu beitragen, sich gegen die wichtigsten Cyberrisiken zu wappnen und die Risiken zu mindern, bevor es zu einem Vorfall kommt.

Die Chubb Cyber Services sind eine Reihe von Dienstleistungen, die auf den Threat-Intelligence-Erkenntnissen und der Schadenexpertise von Chubb basieren:

1. **Cyber Incident Response**
   Erstellung, Optimierung oder Umsetzung eines Reaktionsplans für Cybervorfälle mit allen relevanten Stakeholdern.

2. **Schwachstellenmanagement**
   Identifizierung von Schwachstellen im Netzwerk einer Organisation, um Fehlkonfigurationen und Sicherheitslücken proaktiv zu beheben.

3. **Endpoint Security**
   Antivirus-Software sowie Endpoint Detection and Response Software (EDR) der nächsten Generation, die darauf abzielen, das Eindringen von Cyberkriminellen in das Netzwerk einer Organisation zu verhindern.

4. **Nutzersicherheit und Risikobewusstsein**
   Tools und Schulungen, die die Mitarbeiter in die Lage versetzen, die erste Verteidigungslinie zu bilden.

5. **Datenschutzrisik**
   Management von Datenschutzrisiken und Compliance im gesamten Ökosystem eines Unternehmens.

**Soweit gesetzlich zulässig.*

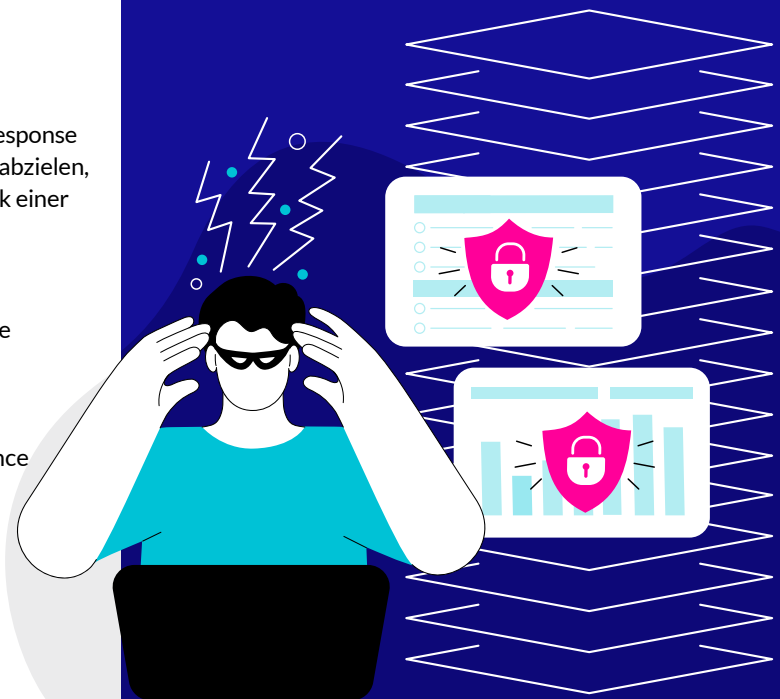
52%

der Cyberangriffe richten sich gegen kleine und mittlere Unternehmen.[6]

KOSTENLOSER CYBER-SCHUTZ FÜR KLEINE UNTERNEHMEN

Chubb Cyber Infrastruktur

Ausgewählte Services, die von einem Netzwerk vertrauenswürdiger Cybersicherheitsanbieter bereitgestellt werden und Kosteneinsparungen in Höhe von bis zu 27.000 Euro pro Jahr ermöglichen. Die Dienstleistungen wurden speziell für kleine Unternehmen mit bis zu 100 Mitarbeitern entwickelt. Sie zielen darauf ab, Cyber-Vorfälle zu verhindern, ein effektives Cyber-Risikomanagement sicherzustellen und eine effiziente Reaktion auf Vorfälle zu ermöglichen.[7]



THREAT INTELLIGENCE UND CYBER RISK ADVISORY TEAM

Cyberexperten, die sich darauf konzentrieren, Ihre Abwehr zu stärken.

Vulnerability Management Outreach

Unser Cyber Intelligence Team überwacht und identifiziert regelmäßig Schwachstellen und neue kritische Sicherheitslücken, um unsere Versicherungsnehmer zu schützen.

Informationen für Versicherungsnehmer

Outreach Program
Versicherungsnehmer einer Cyberversicherung von Chubb und ihre Makler werden benachrichtigt, wenn während der Vertragslaufzeit kritische Sicherheitslücken mit hoher Ausnutzungswahrscheinlichkeit in ihrer Umgebung entdeckt werden.

Warnmeldungen
Warnmeldungen werden an die Versicherungsnehmer einer Cyberversicherung und ihre Makler verschickt, wenn Sicherheitslücken mit hoher Ausnutzungswahrscheinlichkeit entdeckt werden, die ihre IT-Umgebung beeinträchtigen könnten.

Cyber Risk Advisory Team
Unsere Cyber Risk Advisor können Versicherungsnehmern die richtigen Services zur Risikominderung empfehlen und sie bei der Integration dieser Dienstleistungen in ihr Risikomanagement unterstützen. Termine können auf unserer **Website** vereinbart werden.

Eine gute Cyber-Infrastruktur schützt nicht nur, sondern gewährleistet auch eine schnelle Reaktion.

Incident Response Teams

Sollte es zu einem Cybervorfall kommen, wird Sie unser kompetentes **Incident Response Team** schnell und effizient unterstützen. Unsere Teams umfassen erfahrene externe Dienstleister in den Bereichen Rechtsberatung, Computerforensik, Benachrichtigung, Call Center, Öffentlichkeitsarbeit, Krisenkommunikation, Betrugsberatung, Kreditüberwachung und Identitätswiederherstellung.

Chubb Cyber Alert℠

Unsere kostenlose Incident Response Mobile App verbindet Versicherungsnehmer rund um die Uhr mit einem Chubb Incident Response Coach. Die App ermöglicht es ihnen, Fotos zur Unterstützung der Bewertung des Vorfalls hochzuladen, ihren Makler zu benachrichtigen und vieles mehr.

Jetzt die App herunterladen:

Download on the App Store

GET IT ON Google Play

Der Chubb Unterschied

Unsere erfahrenen Schadenexperten wissen, dass der Umgang mit jedem einzelnen Versicherungsschaden für die Bewertung unserer Leistung, unseres Supports und unseres Ansehens ins Gewicht fällt.

Unsere Expertise berücksichtigt die Unternehmenskultur der Kunden und hat die Märkte sowie die dort geltenden Vorschriften im Blick.

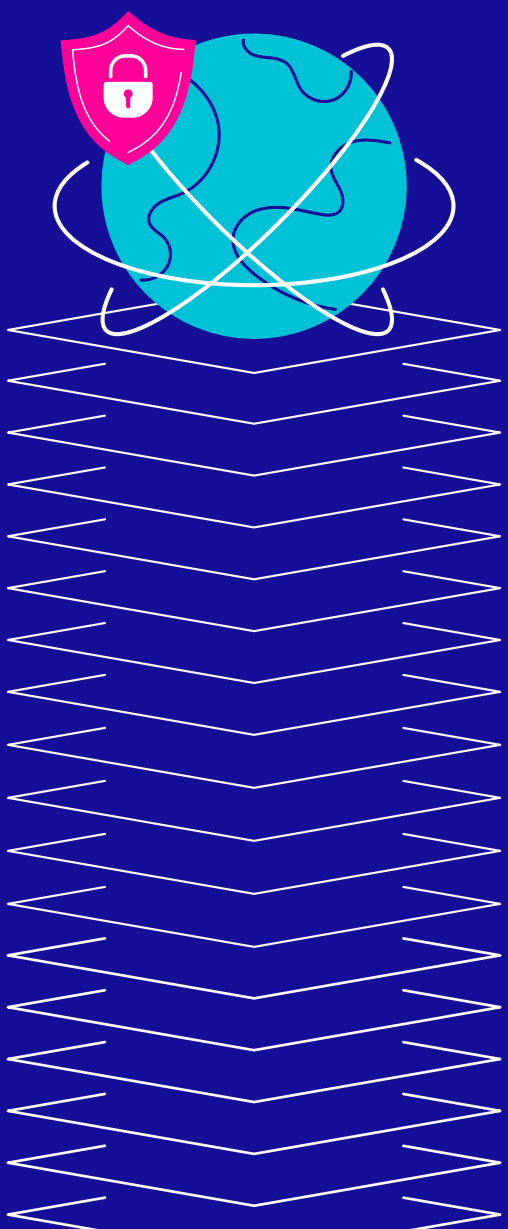
Flexibilität, wenn Sie sie am meisten brauchen

Ob Sie einen Vorfall über die Hotline oder die Cyber Alert App melden, Sie können selbst entscheiden, ob der Vorfall von Chubb als Schadenmeldung behandelt werden soll.

Dieses Team hat mehr als

32.500 Cyber-Schadenfälle

bearbeitet und wird Sie bei einem Schadenvorfall unterstützen.



CHUBB®

Fußnoten

[1] Beinsure (https://beinsure.com/global-ranking-cyber-insurers)

[2] Forbes (www.forbes.com/home-improvement/internet/internet-statistics)

[3] NIST National Vulnerability Database (nvd.nist.gov/general/nvd-dashboard) (Stand: März 2025)

[4] World Economic Forum - Global Risks Perception Survey, 2024 (https://www.weforum.org/publications/global-risks-report-2024)

[5] Verizon Data Breach Investigations Report (www.verizon.com/business/resources/reports/dbir/)

[6] Chubb Cyber Index (chubbcyberindex.com)

[7] Die Bedingungen können sich ändern. Die Kostenfreiheit gilt für einen Zeitraum von einem Jahr und nur für Versicherungsnehmer, die Neukunden der jeweiligen Dienste sind. Darüber hinaus müssen berechtigte Versicherungsnehmer die Größenbeschränkung von maximal 100 Mitarbeitern erfüllen, um bestimmte Services in Anspruch nehmen zu können.

Schützen Sie Ihr Unternehmen mit Chubb.

Um mehr über Chubb Cyber zu erfahren, klicken Sie bitte auf den Link oder scannen Sie den QR-Code:

Alle Cyber-Services können sich ändern. Änderungen des Serviceangebots werden im lokalen Cyber-Services-Webformular abgebildet. Die Versicherungsnehmer sind dafür verantwortlich, die spezifischen Bedingungen und Konditionen jedes Cyber-Service-Anbieters zu überprüfen, um die Berechtigung zu gewährleisten und über eventuelle Änderungen informiert zu bleiben.

RABATTIERTE CYBER-SERVICES VON DRITTPARTNER-ANBIETERN:
Externe Schwachstellenüberwachung, Sicherer Passwort-Manager.

Die oben genannten Cyber-Services werden von Drittanbietern für Chubb-Versicherungsnehmer während des angegebenen Anfangszeitraums kostenfrei angeboten, sofern der Versicherungsnehmer ein neuer Abonnent/Kunde der angebotenen Cyber-Services des ausgewählten Drittanbieters ist und die angegebenen Berechtigungsvoraussetzungen erfüllt. Nach Ablauf des angegebenen Anfangszeitraums können Versicherungsnehmer die Möglichkeit haben, ihre Cyber-Services zu einem ermäßigten Preis bei der Verlängerung fortzuführen. Bitte beachten Sie, dass der spezifische Rabatt je nach Produkt und Service variieren kann. Rabatte auf Produkte und Services, die von Cyber-Services-Anbietern angeboten werden, stehen nur Chubb-Versicherungsnehmern mit laufenden Versicherungsverträgen zur Verfügung und unterliegen den geltenden Versicherungsgesetzen. Die von Drittanbietern bereitgestellten Produkte und Dienstleistungen unterliegen den Vertragsbedingungen, die der Versicherungsnehmer mit dem Drittanbieter eingeht. Chubb ist nicht an der Entscheidung des Versicherungsnehmers beteiligt, Services zu erwerben, und übernimmt keine Verantwortung für Produkte oder Dienstleistungen von Drittanbietern.

Diese Inhalte dienen ausschliesslich der allgemeinen Information. Es handelt sich dabei nicht um eine persönliche Beratung oder Empfehlung für Privatpersonen oder Unternehmen hinsichtlich eines Produkts oder einer Leistung. Die exakten Deckungsbedingungen entnehmen Sie bitte den Versicherungsunterlagen. Insbesondere ist das vorliegende Dokument nicht als Rechts-, Finanz- oder Anlageberatung zu verstehen.

Wir verwenden personenbezogene Daten, die Sie uns direkt oder durch Ihren Makler zur Verfügung stellen, für die Ausstellung und Verwaltung Ihrer Versicherung, einschließlich der Bearbeitung im Zusammenhang damit anfallender Schadenfälle. Weitere Informationen finden Sie in unserer Rahmendatenschutzrichtlinie unter www.chubb.com/de-de/datenschutz.html

DE0434-HS 04/25