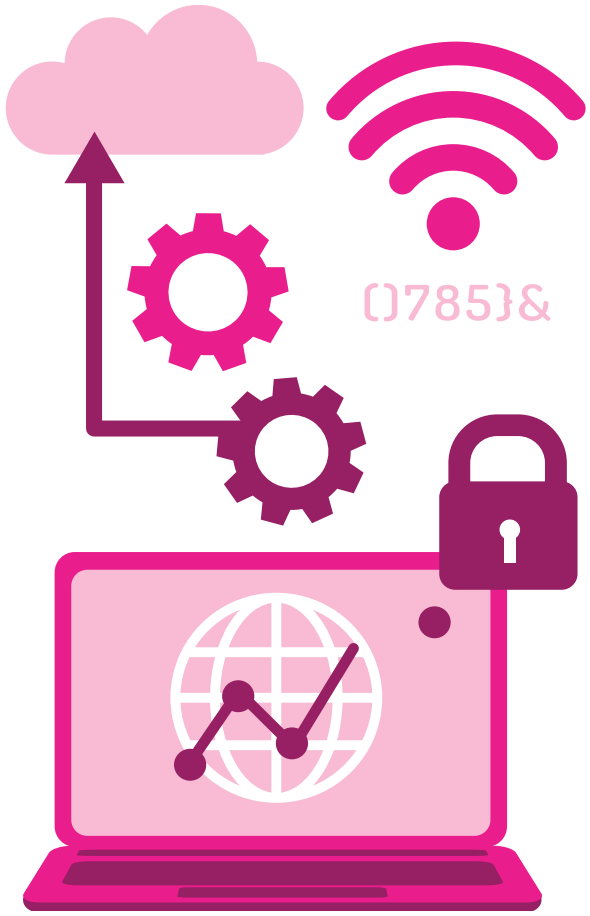
CHUBB®

Cyber Risk Management Leitfaden für Broker

Dieser Leitfaden enthält Informationen zu folgenden Themen:

Warum sind Cyberversicherungen so wichtig?



Im heutigen Informations- und Digitalzeitalter sind wir in der Lage, mehr Daten als je zuvor zu sammeln, effizienter mit anderen zusammenzuarbeiten, Geschäftsprozesse zu rationalisieren und Informationen jederzeit weltweit abzurufen.

Durch eine hohe Abhängigkeit von Computersystemen und Datenzugriffen kann das Cyberbedrohungsrisiko von Unternehmen in erheblichem Masse steigen. Systemausfälle, Fehler und Angriffe auf die neuen Prozesse können so kostspielig werden, dass die Unternehmensbilanz gefährdet wird. Die Frage ist nicht, ob es zu Datenpannen oder Verletzungen der Privatsphäre kommen könnte, sondern wann. Im Fall der Fälle benötigen Sie einen umfassenden Deckungsschutz von einem auf Cyberrisiken spezialisierten Versicherer, der eine vollständige Palette integrierter Versicherungslösungen anbieten kann, mit denen Deckungslücken auf ein Mindestmass begrenzt werden, und der sich darauf versteht, einen massgeschneiderten Deckungsschutz für Ihr Unternehmen zu gestalten. **Chubb ist seit 1998 in der Lage, seinen Versicherten Cyberlösungen anzubieten.**

Deckungslücken klassischer Versicherungen

Viele Unternehmen sind sich sicher, dass sie über ihre bestehenden Policen ausreichend gegen Risiken versichert sind, die die Sicherheit ihrer Daten und den Schutz der Privatsphäre betreffen. Genau dies ist leider nicht der Fall. Herkömmliche Versicherungspolicen können sich angesichts der Bedrohungen, denen Unternehmen heute ausgesetzt sind, als völlig unzureichend erweisen. Zum Vergleich die folgenden klassischen Policen:

Haftpflichtversicherungen	Sachversicherungen	Vertrauensschadenversicherungen
Haftpflichtpolicen greifen normalerweise im Falle von Personen- und Sachschäden. Bei einem Cybervorfall werden aber in aller Regel weder Personen verletzt, noch entsteht ein Sachschaden. Haftpflichtpolicen bieten im Normalfall ohnehin keinen Deckungsschutz für die, dem Versicherten entstehenden, Kosten.	Sachpolicen bieten üblicherweise bei Zerstörungen und Beschädigungen von Sacheigentum Deckungsschutz, wenn diese auf eine physische Gefahr zurückzuführen sind. Aufgrund des verursachten Sachschadens greift die Deckung für Betriebsunterbrechung und entstehende Mehrkosten. Ein Cybervorfall muss nicht in einem Sachschaden resultieren, kann für ein Unternehmen aber erhebliche Kosten und Einkommenseinbussen bedeuten.	Vertrauensschadenpolicen bieten im Falle unmittelbarer Schäden Versicherungsschutz, die durch den Diebstahl von Geldern, Wertpapieren oder Sachgütern durch Mitarbeiter entstehen. Deckungserweiterungen auf Computerstraftaten beinhalten in der Regel keine Schadenersatzansprüche Dritter und bieten unter Umständen keinen ausreichenden Schutz beim Verlust vertraulicher Daten.

Branchenspezifische Risiken

Finanzinstitute

Insbesondere Finanzinstitute sind in grossem Masse gegenüber Cyberrisiken exponiert, weil bei ihnen mehrere Faktoren zusammen wirken. Cyber-kriminalität, Hacktivismus und **hochgradig spezialisierte Angreifer,** die Systeme für andere Nutzniesser ausspionieren, sind nur einige Beispiele. Die Angreifbarkeit von Finanzinstituten kann sehr ausgeprägt sein, da viele von ihnen von stark vernetzten Systemen und **kritischen Infrastrukturen** abhängig sind. Aufgrund ihrer hohen Abhängigkeit von Technologien wird die Mehrzahl der Finanzinstitute auch künftig in erheblichem Masse Cyberrisken ausgesetzt sein.

Häufige Schadenfälle:
Social - Phishing und menschliches Versagen

Gesundheitswesen

Die zunehmende Trend, Krankenakten zu digitalisieren, hat bewirkt, dass Unternehmen aus dem Gesundheits-wesen immer stärker von Computer-systemen abhängig sind, auf denen **hochsensible persönliche Gesund-heitsdaten und Krankenakten** erfasst und übermittelt werden. Es besteht ein erhebliches Risiko administrativer Fehler, da sich die Unternehmen auf fehlerfreie System-eingaben ihrer Mitarbeiter verlassen müssen. Ältere Computersysteme sind häufig nicht segregiert, sodass ein höheres Risiko besteht, dass sich ein Vorfall gravierend auf den gesamten Geschäftsbetrieb auswirkt.

Häufige Schadenfälle:
Mitarbeiterfehler und Missbrauch

Einzelhandel

Die von Chubb gesammelten Schaden-daten zeigen, dass Einzelhändler, gleich ob sie Betreiber von Online-Shops oder von Filialgeschäften sind, über hohes Cyberschadenrisiko verfügen. Einzelhandelsfirmen haben oft **viele Standorte** und betreiben ihr Geschäft über zentralisierte IT-Systeme. Ihr Netzwerk unternehmenskritischer IT-Dienstleister kann sehr **komplex** sein und aufgrund des zunehmenden Internetabsatzes kann eine starke Abhängigkeit von **Websites** bestehen. Auch haben sie einen vergleichsweise hohen Bestand an **sensiblen persönlichen Daten,** der auf die hohe Zahl an Finanztransaktionen und Kundenbindungsprogramme zurückzuführen ist.

Häufige Schadenfälle:
Hacking und Social Engineering - Phishing

Gastronomie

Die Gastronomie umfasst eine Vielzahl unterschiedlicher Betriebe wie Hotels, Bars und Restaurants. Die gesamte Branche sieht sich mit Cyberrisiken konfrontiert, die von **der hohen Menge an Gäste- und Mitarbeiter-daten,** einer oftmals starken Abhängigkeit von Websites, über die Kunden ihre Buchungen vornehmen, sowie ihren **Loyalty-Programm-Datenbeständen** ausgehen und zu Datenschutzverstössen führen können, da sie Social Engineering- und Phishing-Angriffen ausgesetzt ist.

Häufige Schadenfälle:
Social Engineering - Phishing und Hacking

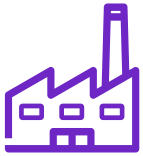
Professionelle Dienstleister

Angesichts der grossen Menge vertraulicher Daten, die bei professionellen Dienstleistungen erfasst werden, ist die Branche ein beliebtes Ziel für Cyberangriffe. So können die Informationen und Gelder, über die bspw. eine Anwaltskanzlei oder eine Steuerberatung verfügt, ein lukratives Ziel für Angreifer werden und der **Reputationsschaden,** den ein Unternehmen infolge eines Daten-verstosses erleidet, kann beträchtlich sein. Das hohe Volumen sensibler Kundendaten hat in den letzten Jahren dazu geführt, dass professionelle Dienstleister immer häufiger zum Ziel von Cyberangriffen wurde.

Häufige Schadenfälle:
menschliches Versagen und Hacking

*Die häufigsten Ursachen für Cyberschäden gemäss dem von Chubb veröffentlichten Cyber Risk Index℠

Branchenspezifische Risiken



Produzierende Unternehmen

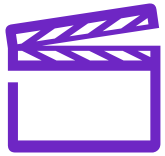
Eine der am häufigsten von **Cyber-Kriminellen** angegriffenen Branchen ist der Industriesektor, denn der umfassende Einsatz von Technologien bringt hier starke Veränderungen der Arbeitsabläufe in den Unternehmen mit sich. Zur Steigerung ihrer Produktivität und Kosteneffektivität nutzen viele Hersteller das Internet der Dinge, Cloud-Dienste und die Digitalisierung, weshalb die Auswirkungen bestimmter Cybervorfälle hier noch viel gravierender sein können. Vorfälle der letzten Zeit betrafen Industrial Control Systems (ICS) sowie Supervisory Control and Data Acquisition (SCADA)-Systeme und hatten verheerende Folgen für die betrieblichen Abläufe.

Häufige Schadenfälle:
Malware und Social Engineering

Bildungssektor

Bildungseinrichtungen sind aufgrund der **sensiblen Daten** ihrer Schüler, Studierenden und Mitarbeiter besonderen Risiken ausgesetzt. Häufig sind die IT-Budgets und Ressourcen von Schulen und Universitäten begrenzt. Es bestehen interne und äussere Bedrohungen, z. B. aufgrund von Malware, die von Studenten vorsätzlich oder unbeabsichtigt in Netzwerke eingeschleust wird oder durch Mitarbeiter, die Vorschriften missachten und dadurch Datenpannen verursachen.

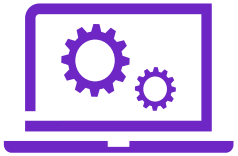
Häufige Schadenfälle:
Social Engineering - Phishing und Hacking



Medien / Unterhaltung

Unternehmen der Medien- und Unterhaltungsbranche sind oftmals dem Risiko von **Cybererpressung** ausgesetzt, die auf schützenswertes Material und Inhalte ausgerichtet ist. Distributed **Denial of Service (DDoS)-Angriffe** oder Ausfälle von Computersystemen können den Sendebetrieb erheblich stören und die pünktliche Lieferung von Inhalten unmöglich machen. Der Besitz **sensibler personenbezogener** Daten vergrössert das Risiko umso mehr.

Häufige Schadenfälle:
menschliches Versagen und Social



Technologiebranche

Technologieunternehmen gelten bei ihren Kunden und Geschäftspartnern als Branchenführer für Cybersicherheit und Datenschutz. Aus diesem Grund haben sie ein besonders hohes Risiko, bei Cybervorfällen **Reputationsschäden** zu erleiden. Cybervorfälle bei Technologieanbietern können aber auch eine spezifische Technology **Errors and Omissions-Deckung** erfordern. Bitte wenden Sie sich an den zuständigen Chubb-Underwriter, der Ihnen nähere Informationen über unsere branchenführende kombinierte Versicherung Tech E&O und Cyber geben kann.

Schadenfälle:
Hacking und menschliches Versagen

*Die häufigsten Ursachen für Cyberschäden gemäss dem von Chubb veröffentlichten Cyber Risk Index℠

Hier sehen Sie Chubbs Angebotsspektrum für die Risiken kleiner, mittelständischer und grosser Unternehmen:

KMUs/Kleine Firmen | Mittelstand | Grossunternehmen

KMUs/Kleine Firmen – Übersicht

Trotz der zunehmenden medialen Aufmerksamkeit, die Cybervorfälle in Grossunternehmen auf sich ziehen, sind vor allem KMUs/Kleine Firmen aufgrund ihrer spezifischen Schwachstellen von Angriffen bedroht. KMUs/Kleine Firmen sind für Cyber-Kriminelle oftmals leichtere Ziele, da sie nicht selten nur in begrenztem Mass über IT-Ressourcen und Mittel für Investitionen verfügen.

Ausserdem werden in KMUs/kleinen Firmen Massnahmen wie Mitarbeiterschulungen zum Thema Datenschutz, Passwortregelungen und die Zwei-Faktor-Authentifizierung schneller vernachlässigt. KMU bieten Cyber-Kriminellen häufig lukrativere Möglichkeiten als grössere Unternehmen, die nicht so leicht „zu hacken“ sind. Ausserdem sollten KMUs/kleine Firmen bedenken, dass sie nicht unbedingt das eigentliche Angriffsziel sein müssen, sondern möglicherweise nur Mitbetroffene von Vorfällen sind, die sich bei ihren IT-Anbietern oder Geschäftspartnern ereignen.

Schadenfälle von KMUs/kleinen Unternehmen - Chubb Cyber Index℠

Cyberrisiken von KMUs/kleinen Betrieben lassen sich am besten am Beispiel der Datenbestände aufzeigen. Inzwischen reguliert Chubb seit mehr als zwei Jahrzehnten Cyberschäden. Bei der Schadenbearbeitung zeichnen wir wichtige Metriken auf, so z. B. Aktivitäten, die zu Cyberschäden führen, ob ein Cybervorfall von einer firmeninternen oder -externen Person ausging, die Anzahl der betroffenen Datensätze und die Grösse sowie die Branche des betroffenen Versicherten. Damit unsere Kunden und Vermittler Einblick in diese nützlichen Cyberschaden-Daten nehmen können, veröffentlicht Chubb den Cyber Index℠.

Anhand des Cyber Index℠ von Chubb und seiner Beispiele für Cyberangriffe und Datenpannen aus der Praxis können Nutzer die für ihre Unternehmen grössten Cyberrisiken identifizieren. Dies gibt ihnen die Möglichkeit, auf der Grundlage der Bedrohungsart, der Firmengrösse und der Branche Parameter aufzustellen und historische Trends zu verfolgen.

Weitere Informationen zu Chubbs Cyber Index℠ finden Sie hier:
https://chubbcyberindex.com

KMUs/Kleine Firmen – Schadenszenarien

Ransomware

Ein bei Chubb versichertes Unternehmen aus der Baubranche wurde Ziel eines Ransomware-Angriffs. In die Systeme des Versicherten konnte eingedrungen werden, weil ein Mitarbeiter auf einen infizierten Link einer E-Mail geklickt hatte. Die Systeme und Server des Versicherten wurden daraufhin verschlüsselt und es folgte eine Lösegeldforderung in Höhe von 800.000 € in Bitcoins. Das versicherte Unternehmen wandte sich an die Incident Response Manager von Chubb, um die IT-Forensiker mit der Feststellung der Angriffsmethode und des Umfangs des Vorfalls zu beauftragten. Auch wenn letztlich keine Lösegeldzahlung erfolgte, war der gesamte Geschäftsbetrieb mehr als sechs Monate lang unterbrochen.

Anwendbare Versicherungsgegenstände:

Daten- und Systemwiederherstellungen, Betriebsunterbrechung, Incident Response-Kosten und Cyber-Erpressung.

Risikoprävention:

Regelmässige Überprüfung der IT-Sicherheit, Mitarbeiterschulungen, regelmässige Datensicherungen sowie Desaster Recovery- und Business Continuity Pläne.

Unzufriedene Mitarbeiter

Einer unserer Versicherten wurde Opfer eines kriminellen Mitarbeiters, der die Datensätze von mehr als 700 Kunden einschliesslich deren Namen, Adressen und Kontaktdaten entwendete. Die Daten wurden dem neuen Arbeitgeber des Mitarbeiters zu dessen Verwendung überlassen. Da sich der Vorfall nach Einführung der DSGVO ereignete, musste er den lokalen Aufsichtsbehörden und auch den betroffenen Personen gemeldet werden.

Anwendbare Versicherungsgegenstände:

Haftung bei Datenschutz- und Netzwerksicherheitsverletzungen und Incident Response-Kosten.

Risikoprävention:

Sich vor kriminellen Mitarbeiten zu schützen, die dem Unternehmen schaden wollen, ist äusserst schwierig. In vielen Fällen verfügen sie über den erforderlichen Systemzugriff, der es ihnen ermöglicht, schützenswerte persönliche oder Unternehmensdaten zu entwenden. Nach aktueller Rechtsprechung tragen Unternehmen gegenüber ihren Kunden ein hohes Haftungsrisiko. Die Cyberversicherungslösungen von Chubb beinhalten Instrumente, mit denen im Ernstfall die richtigen Massnahmen getroffen werden können.

Menschliches Versagen

Eine bei uns versicherte britische Wohnungsgesellschaft wurde aufgrund eines Mitarbeiterfehlers unversehens Opfer einer Datenpanne. Bei der Veröffentlichung einer Immobilienanzeige hatte der Angestellte versehentlich ein Foto in das Internet-Exposé der Immobilie aufgenommen, auf dem Behandlungsinformationen eines Kunden zu sehen waren.

Anwendbare Versicherungsgegenstände:

Haftung bei Datenschutz- und Netzwerksicherheitsverletzungen und Incident Response-Kosten.

Risikominderung:

Es kommt entscheidend darauf an, über eine unternehmensübergreifende Datenschutzrichtlinie zu verfügen, in der detailliert beschrieben ist, wie mit sensiblen Informationen umzugehen ist. Mitarbeiter müssen verpflichtet sein, die Kenntnis der Richtlinie und deren Einhaltung mindestens einmal jährlich zu bestätigen.

KMUs/Kleine Firmen – Schadenszenarien

Unberechtigter Zugriff - Phishing

Bei einem bei uns versicherten Logistikunternehmen ist es zu einem Malware-Phishing-Angriff gekommen. Einem Mitarbeiter des HR-Teams des Versicherten wurde auf seinem Rechner ein Pop-Up-Fenster angezeigt, nachdem er in einer E-Mail auf einen infizierten Link geklickt hatte. In dem Fenster wurde ihm mitgeteilt, dass der Computer infiziert sei und er die angegebene Telefonnummer anrufen solle. Indem die Betrüger den Angestellten während des Telefonats weiter täuschten, erlangten sie schliesslich den Fernzugriff auf dessen PC.

Anwendbare Versicherungsgegenstände:

Haftung bei Datenschutz- und Netzwerksicherheitsverletzungen und Incident Response-Kosten.

Risikoprävention:

Ein Unternehmen mag über die besten Sicherheitstechnologien und -systeme verfügen, seine verwundbarste Stelle sind oft die eigenen Mitarbeiter, denn Angestellte können dazu verleitet werden, Passwörter preiszugeben oder Systemzugriffe zuzulassen. Regelmässige Phishing-Schulungen sind daher empfehlenswert, aber auch eine Versicherungspolice, die die entsprechende Expertise beinhaltet.

Physischer Verlust von Datensätzen

Eine bei uns versicherte Anwaltskanzlei wandte sich an die Incident Response-Hotline von Chubb, als sich herausstellte, dass ein Mitarbeiter des Unternehmens gegen die Firmenrichtlinien verstossen hatte, indem er Klientenakten aus der Kanzlei mitgenommen und diese in seinem Auto aufbewahrt hatte. Als der Wagen gestohlen wurde, befanden sich die Akten im Fahrzeug und wurden ebenfalls entwendet.

Anwendbare Versicherungsgegenstände:

Haftung bei Datenschutz- und Netzwerksicherheitsverletzungen und Incident Response-Kosten.

Risikoprävention:

Festgelegte klare Prozesse für die Aufbewahrung digitaler und physischer Daten. Regelmässige Datensicherungen sind entscheidend, wenn es darauf ankommt,Daten schnell wiederherzustellen. Festlegung einer unternehmensübergreifenden Datenschutzrichtlinie, deren Kenntnis und Einhaltung für Mitarbeiter verbindlich ist.

KMUs/Kleine Firmen – Eine massgeschneiderte Cyberlösung

1 Schadenpräventionsdienstleistungen für KMUs/kleine Firmens

Chubb ist Anbieter zahlreicher kostenloser bzw. äusserst kostengünstiger Serviceleistungen, mit denen versicherte KMUs/kleine Firmen häufig auftretende Cyberschäden auf ein Mindestmass begrenzen können.

Passwortverwaltungslösungen, die pro Policeninhaber für bis zu 500 Mitarbeiter kostenlos sind.

- Eine effiziente Passwortverwaltung kann dazu beitragen, die unbefugte Nutzung gestohlener Anmeldedaten auf ein Mindestmass zu begrenzen.

Phishing-Simulationen und -Schulungen stehen allen Policeninhabern zur Verfügung.

- Phishing ist eine der am häufigsten vorkommenden Ursachen für Cyberschäden. Einfache Mitarbeitertrainings-massnahmen können sich als sehr effektiv erweisen, um Phishing-Angriffe auf KMUs/kleine Firmen einzudämmen.

2 Incident Response-Service für KMUs/kleine Firmens

Wir wissen, dass es unmöglich ist, jeden Vorfall zu unterbinden. Im Fall der Fälle **bieten unsere Cyberpolicen Zugang zu unserem Expertenpool von Incident Response-Anbietern und das ganz ohne Selbstbehalt für unsere KMU-Kunden.**

Wir wissen, dass es unmöglich ist, jeden Vorfall zu unterbinden. Im Fall der Fälle bieten unsere Cyberpolicen Zugang zu unserem Expertenpool von Incident Response-Anbietern und das ganz ohne Selbstbehalt für unsere KMU-Kunden.

- Der Expertenpool umfasst u. a. Incident Response Manager, IT-Forensiker sowie Rechts- und PR-Berater.
- Die Police beinhaltet den Zugang zum Anbieternetzwerk.
- 24/7/365-Erreichbarkeit über die Cyber Alert App®, die kostenlose Hotline und das Internet.
- Die Police bietet Unterstützung nach einem tatsächlichen oder **vermuteten** Cybervorfall – im Notfall erhalten Sie Hilfe.

3 Plattformen für KMUs/kleine Firmen

Chubbs Webplattformen (nicht in allen Ländern verfügbar) wurden eigens dazu entwickelt, Vermittlern die Möglichkeit zu geben, Versicherungsangebote für KMUs/kleine Firmen über das Internet abzugeben und deren Verträge online abzuschliessen. Das intuitive Design des Portals in Verbindung mit seiner kundenfreundlichen Gestaltung ermöglicht es Vermittlern, in nur wenigen Minuten Cyberdeckungen für ihre Kunden zu vereinbaren und sofort die entsprechenden Unterlagen auszustellen.

Schnelle und einfache Abschlussstrecke; dieselben Policenleistungen wie bei Offline-Abschlüssen:

- Einfacher Fragenkatalog.
- Hohe Risikoappetit in Bezug auf KMUs/kleine Unternehmen.
- Gleiches Cyberpolicen-Wording wie bei Offline-Abschlüssen.
- Zugang zu Chubbs Cyber-Schadenpräventionsdienstleistungen.
- Bearbeitung von Policendaten, Versicherungssummen, Provisionshöhen und Kontaktdaten ohne das Erfordernis, einen Underwriter kontaktieren zu müssen.
- Angebotserstellung und Abschluss von Risiken in nur wenigen Minuten.

Hier finden Sie weitere Informationen über unser gesamtes Angebot an Cyberdienstleistungen, einschliesslich Cybersicherheit und vieles mehr.

Hier erfahren Sie, welche Vorteile Chubbs Incident Response-Lösung im Einzelnen bietet.

Bitte wenden Sie sich bei Fragen zu unseren Online-Cyberversicherungslösungen und einfachen Lösungen für KMU an den für Ihre Region zuständigen Chubb-Underwriter.

Mittelstand – Übersicht

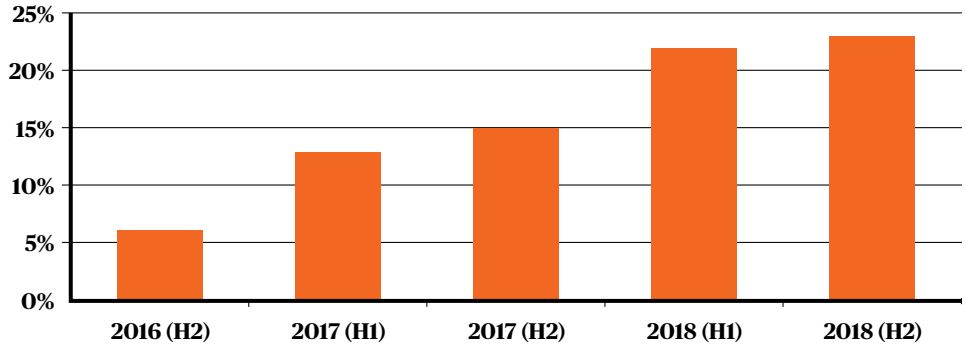
Mittelständische Firmen sehen sich mit denselben Cybersicherheitsproblemen konfrontiert wie Grossunternehmen, haben aber geringere Budgets und weniger auf den Umgang mit Cyberrisiken spezialisierte Mitarbeiter. Wie viele KMUs/kleine Firmen sind sie oft der Auffassung, dass nur grosse, global agierende Unternehmen ein hohes Gefahrenpotenzial aufweisen. Da böswillige Cyberaktivitäten immer ausgeklügelter werden, müssen sich Firmen aus dem mittleren Marktsegment so gut wappnen wie nie zuvor.

Chubb Cyber Index℠

Anhand des Index und seiner Beispiele für Cyberangriffe und Datenpannen aus der Praxis können Nutzer die für ihre Unternehmen grössten Cyberrisiken identifizieren. Dies gibt ihnen die Möglichkeit, auf der Grundlage der Bedrohungsart, der Firmengrösse und der Branche Parameter aufzustellen und historische Trends zu verfolgen.

Weitere Informationen über den Chubb Cyber Index℠ finden Sie hier:
https://chubbcyberindex.com

Chubbs Schadenaufkommen i. Vgl. z. 1. HJ 2016 (prozentuale Zunahme)
Mittleres Marktsegment - Alle Branchen



Mittelstand – Schadenszenarien

Ransomware

In einer Einrichtung für betreutes Wohnen kam es zu einem Brute-Force-Ransomwareangriff, bei dem mehrere Dateien verschlüsselt wurden. Die Täter verlangten ein Lösegeld in Höhe von rund 26.000 EUR. Nachdem die betroffene Gesellschaft zunächst einen kleinen Teilbetrag gezahlt hatte, um das Entschlüsselungstool testen zu können, entschied sie sich, ihre Systeme lieber anhand der vorhandenen Sicherheitskopien wiederherzustellen.

Anwendbare Versicherungsgegenstände:

Daten- und Systemwiederherstellung, Betriebsunterbrechung, Incident Response-Kosten und Cyber-Erpressung.

Risikoprävention:

Investitionen in Sicherheitstechnologie sind unverzichtbar, um unberechtigten Systemzugriffen vorzubeugen, eine hundert-prozentige Sicherheit bieten sie jedoch nicht. Die Täter bedienen sich immer ausgefeilterer Angriffsmethoden, sodass Unternehmen ihre Schutzmassnahmen und Verfahrensweisen kontinuierlich auf den Prüfstand stellen müssen, um mit den Bedrohungen Schritt halten zu können.

Mitarbeiterfehler

Ein Mitarbeiter einer Baumarktkette liess interne Richtlinien und Verfahrensweisen ausser Acht und öffnete einen scheinbar harmlosen Dateianhang einer E-Mail. Ab dem folgenden Tag funktionierten das Lagerbestandssystem und die Kassen nicht mehr einwandfrei und aufgrund der Störung des Netzwerks musste der Geschäftsbetrieb schliesslich eingestellt werden.

Anwendbare Versicherungsgegenständ:

Daten- und Systemwiederherstellungen, Haftung bei Daten- und Netzwerksicherheitsverletzungen, Betriebsunterbrechung und Incident Response-Kosten.

Risikoprävention:

Regelmässige Schulungen, um sicherzustellen, dass die Mitarbeiter wissen, auf was sie bei verdächtigen E-Mail-Anhängen achten müssen und welche Verfahrensweisen im Verdachtsfall zu befolgen sind. Die sofortige Erreichbarkeit eines Incident Managers und ein Notfallhilfe-Netzwerk ermöglichen eine schnelle Reaktion.

Datenpanne

Nach einem Hackerangriff auf das Netzwerk eines Hotelbetriebs musste davon ausgegangen werden, dass alle Datensätze der Mitarbeiter und Gäste manipuliert wurden, hierin eingeschlossen die Zahlungskartendaten der Kunden.

Anwendbare Versicherungsgegenstände:

Incident Response-Kosten, Daten- und Systemwiederherstellung sowie Haftung bei Datenschutz und Netzwerksicherheits-verletzungen.

Risikoprävention:

Detection Awareness Security ist eine gutes Instrument , um Hacker abzuwehren. Auf diese Weise können alle verdächtigen Vorgänge schnell erkannt werden. Auch die Verschlüsselung von Daten ist unverzichtbar, um sicherzustellen, dass gehackte Daten nicht ohne Weiteres entfernt und verwendet werden können.

Mittelstand – Schadenszenarien

Kryptomining

Bei einem Ransomware-Angriff auf ein produzierendes Unternehmen wurden mehrere Dateien des Unternehmens verschlüsselt. Nachdem der Versicherte Chubb über die 24/7-Incident Response-Hotline verständigt hatte, boten wir ihm ein Gespräch mit einem Incident Response Manager und Forensikern aus unserem Cyber-Expertenpool an. Nach Rücksprache mit diesen entschied sich der Versicherte, kein Lösegeld zu zahlen. Als das Forensikunternehmen dann mit seinen Arbeiten begann, wurde festgestellt, dass nicht nur ein Ransomware-Angriff erfolgt war, sondern der Versicherte auch Opfer eines Kryptominings geworden war. Die Täter hatten auf dem System Software zum Schürfen von Bitcoins installiert. Kryptomining erfolgt, wenn das Computersystem einer Person ohne deren Wissen für das Schürfen von Kryptowährungen benutzt wird.

Anwendbare Versicherungsgegenstände:

Incident Response-Kosten, Betriebsunterbrechung, Daten- und Systemwiederherstellung sowie Haftung bei Datenschutz- und Netzwerksicherheitsverletzungen.

Risikoprävention:

Hersteller sollten regelmässig IT-Security-Prüfungen vornehmen, um angriffsbedingte Produktionsunterbrechungen zu verhindern. Auch ein Desaster Recovery- und Business-Continuity-Plan sind in Erwägung zu ziehen, um im Falle eines Angriffs die Unterbrechung auf ein Mindestmass zu begrenzen. Unberechtigte Zugriffe lassen sich allerdings nicht immer vermeiden. Die Täter bedienen sich immer ausgefeilterer Angriffsmethoden, sodass Unternehmen ihre Schutzmassnahmen und Verfahrensweisen kontinuierlich auf den Prüfstand stellen müssen, um mit den Bedrohungen Schritt halten zu können.

Datendiebstahl und seine Folgen: Erpressung, Betriebsunterbrechungen und Mehrkosten

Das Netzwerk einer Anwaltskanzlei wurde von einer unbekannten Organisation gehackt, die sich vermuteterweise Zugriff auf sensible Kundendaten verschaffte, darunter das Übernahmeziel einer Aktiengesellschaft, die Patentanmeldung einer Technologie eines weiteren börsennotierten Unternehmens, der Prospektentwurf eines Venture Capital-Kunden sowie eine grössere Anzahl von Massenklagen-Listen mit Daten, über die die Kläger persönlich identifizierbar waren. Ein von der Kanzlei beauftragter Forensikdienstleister stellte fest, dass Malware in das Firmennetzwerk eingeschleust worden war. Kurz darauf erhielt das Unternehmen einen Anruf der Eindringlinge, die 10 Mio. EUR verlangen, anderenfalls würden die gestohlenen Daten ins Internet gestellt. Der Anwaltskanzlei entstanden im Zusammenhang mit der forensischen Untersuchung, den Verhandlungen mit den Erpressern, der Lösegeldzahlung, Benachrichtigungen, der Kredit- und Identitätsüberwachung, Wiederherstellungsarbeiten und Honoraren externer Berater Kosten in Höhe von 2 Mio. EUR.

Anwendbare Versicherungsgegenstände:

Cybererpressung, Haftung bei Datenschutz- und Netzwerksicherheitsverletzungen, Betriebsunterbrechung und Incident Response-Kosten.

Risikoprävention:

Schulung von Mitarbeitern, damit infizierte E-Mails nicht geöffnet werden. Zusätzlich IT-Security Systeme, um Malware sofort erkennen zu können und im Falle der Aktivierung eine weitere Ausbreitung im Netzwerk zu verhindern.

Mittelstand – Eine massgeschneiderte Cyberlösung

1 Schadenpräventionsdienstleistungen für den Mittelstand

Um unsere Kunden aus dem mittleren Marktsegment bei der Abwehr tendenziell häufiger Cyberschäden unterstützen zu können, bietet Chubb seinen Versicherungsnehmern verschiedene kostenlose bzw. äusserst kostengünstige Serviceleistungen an.

Passwortverwaltungslösungen, die pro Policeninhaber für bis zu 500 Mitarbeiter kostenlos sind.

- Eine effektive Passwortverwaltung kann dazu beitragen, die unberechtigte Nutzung gestohlener Anmeldedaten auf eine Mindestmass begrenzen.

Phishing-Simulationen als Schulungsmassnahmen stehen allen Policeninhabern zur Verfügung.

- Phishing ist immer häufiger die Ursache von Cyberschäden. Mit einfachen Schulungsmassnahmen für Mitarbeiter können Phishing-Angriffe in mittelständischen Unternehmen weitgehend verhindert werden.

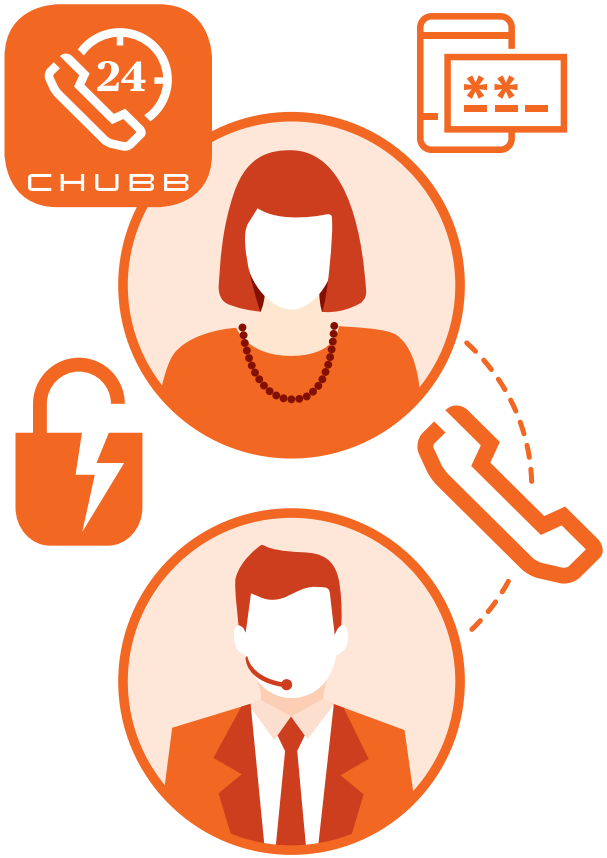
Hier finden Sie weitere Informationen über unser gesamtes Angebot an Cyberdienstleistungen, einschliesslich Cybersicherheit und vieles mehr.

2 Incident Response-Service für den Mittelstand

Bei Cybervorfällen kommt es auf schnelles Handeln an, um weitere Auswirkungen und Schäden möglichst gering zu halten. Denn im Fall der Fälle bieten unsere Cyber-Policen Zugang zu unserem Expertenpool von Incident Response-Anbietern für Kunden aus dem Mittelstand. Die Spezialisten sind an allen Tagen im Jahr rund um die Uhr erreichbar (24/7/365) und erläutern Ihnen alle erforderlichen Schritte, um den Geschäftsbetrieb nach einem Cybervorfall wiederaufnehmen zu können.

- Zum Kreis der Experten gehören Incident Response Manager, IT-Forensiker, Rechtsberater, PR-Spezialisten und Cyber-Erpressungs-Verhandlungsführer.
- Der Kunde kann frei entscheiden, ob er die Dienste unserer Anbieter in Anspruch nehmen möchte oder Anbieter, mit denen er bereits im Rahmen eines Cyber-Incident Response-Plans zusammenarbeitet.
- 24/7/365-Verfügbarkeit über die Cyber Alert® App, die kostenlose Telefonnummer oder das Internet.
- „Emergency Incident Response" bietet Unterstützung nach stattgefundenen oder **anzunehmenden** Cybervorfällen – das entsprechende Team steht bereit, in allen Cyber-Notfällen zu helfen, und das über einen Zeitraum von 48 Stunden und **ohne Selbstbehalt.**

Weitere Informationen darüber, welche Vorteile die Incident Response-Lösung von Chubb im Einzelnen bietet.



Mittelstand – Eine massgeschneiderte Cyberlösung

3 Risk Engineering Services

Die betrieblichen Abläufe der jeweiligen Kunden und die von ihnen eingesetzten Technologien können sehr verschieden sein. Unsere Cyber Risk Engineers helfen unseren Kunden, ihre technischen Schwachstellen zu identifizieren und ein Verständnis hierüber zu gewinnen und unterstützen sie bei der Vermeidung künftiger Cybervorfälle und das bereits vor Versicherungsbeginn.

Die wichtigsten Vorteile

Direkter Kontakt zum Kunden, um eine fundierte Kenntnis seiner Risiken und etwaigen Schwachstellen zu gewinnen

Dies kann bereits vor Vertragsschluss oder während der Vertragslaufzeit erfolgen

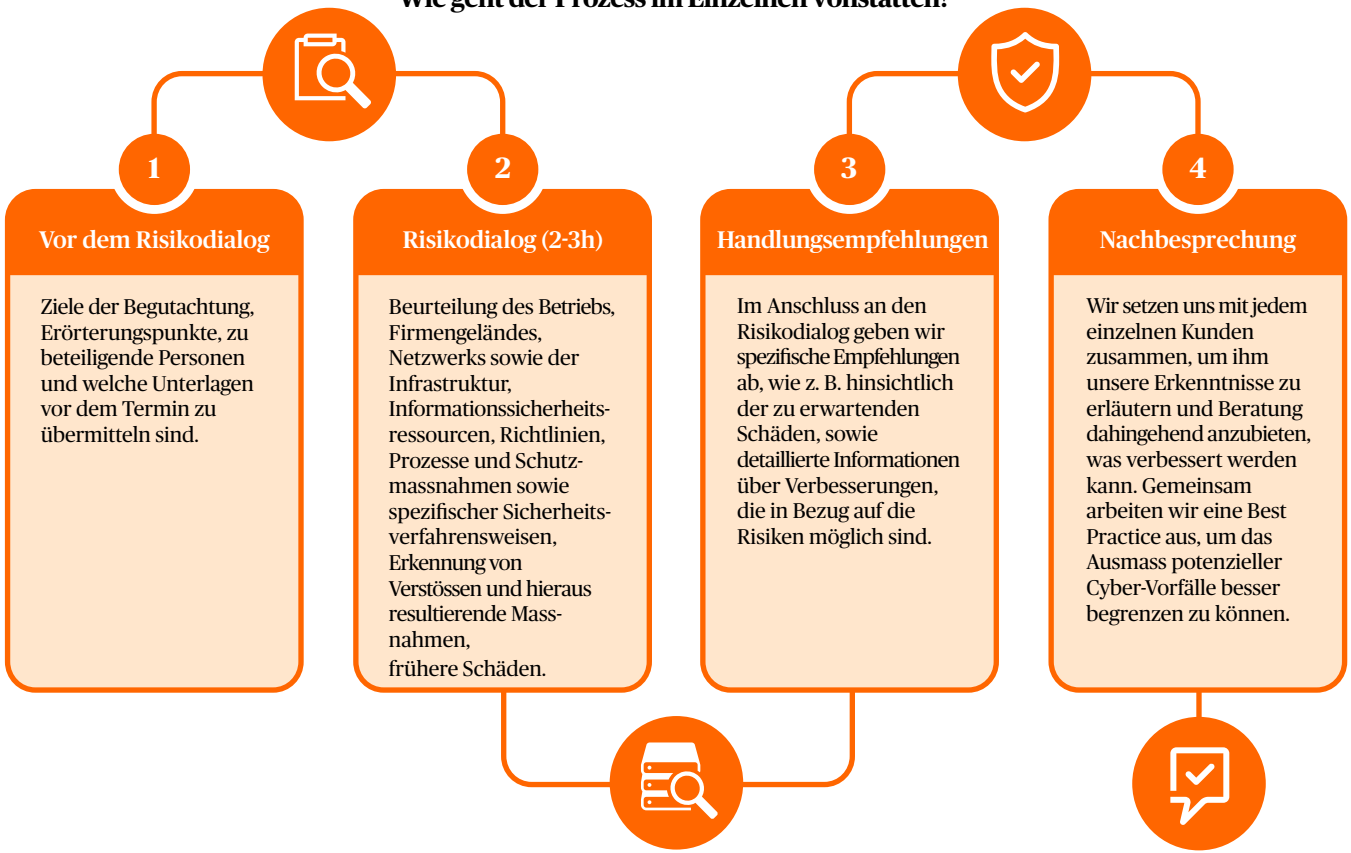
Die Kunden erhalten Risikoempfehlungen und Ratschläge, wie sie ihr Cyberrisikomanagement-Profil insgesamt verbessern können

Zusätzliche fachliche Schulungen sind für Kunden und Makler verfügbar

Dieser Service ist auf unsere Kunden aus dem mittleren Marktsegment zugeschnitten, ist aber für Firmen jeder Grösse von Vorteil.

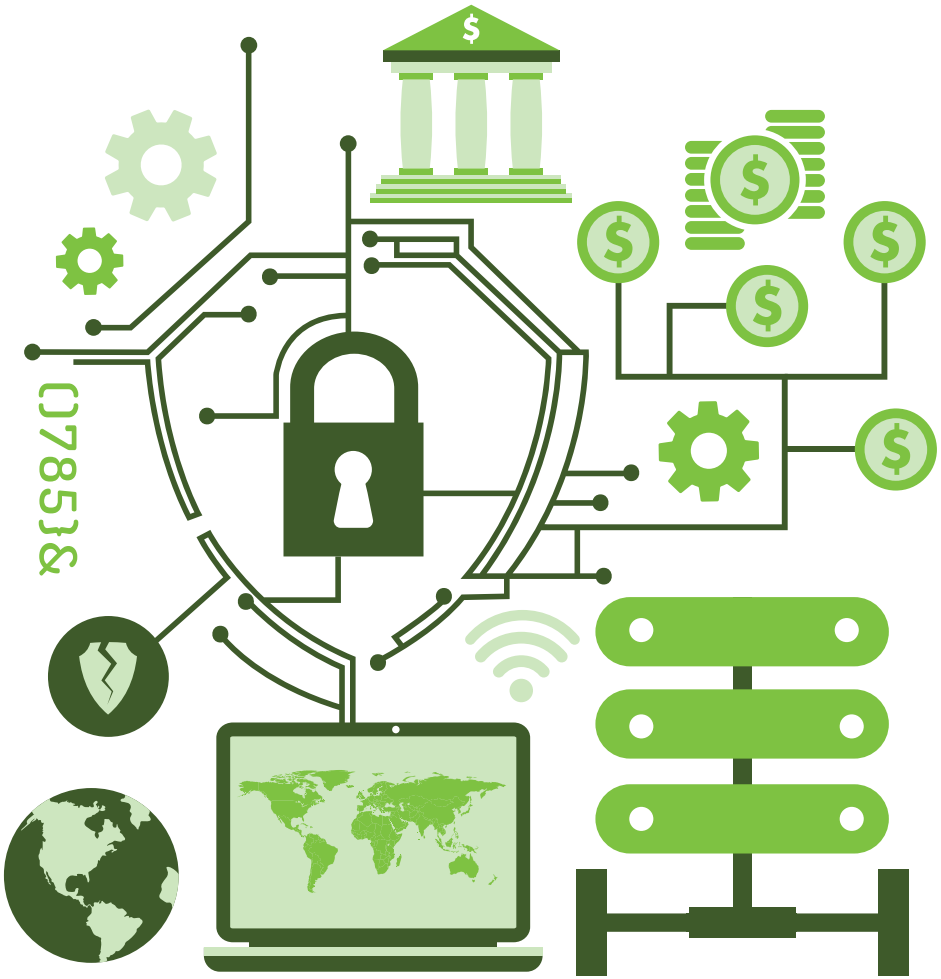
Vorgehensweise

Wie geht der Prozess im Einzelnen vonstatten?



Grossunternehmen – Übersicht

Da sich die Anzahl der in den Medien veröffentlichten Cyber-Angriffe auf grosse und multinationale Unternehmen in den letzten Jahren erhöht hat, ist auch die Nachfrage nach Cyber-Versicherungen drastisch gestiegen. Die höhere Nachfrage ging vor allem auf den auf Vorstände ausgeübten Druck zurück, angemessene Cyberrisiko-Einschätzungen zu treffen, sowie auf eine strengere Beaufsichtigung durch die Behörden und die Zunahme des Informationsaustauschbedarfs unter Mitarbeitern und Geschäftspartnern. Vorstände und Risikomanager wissen, dass Cyber-versicherungen mehr bieten müssen als einen blossen Risikotransfer. Chubbs Angebote für Grossunternehmen beinhalten eine globale und dennoch flexible Incident Response-Lösung, ein breites Spektrum an multinationalen Programmen, Captive-Fronting-Optionen und bedeutende Kapazitäten über unsere Global Cyber Facility.



Incident Response-Dienstleistungen für Grossunternehmen

Grossunternehmen verfügen sehr häufig über Cyber-Incident Response-Pläne, die kontinuierlichen Tests unterzogen werden. Chubbs Cyber Incident Response-Service ist als Ergänzung hierzu gedacht. Unser Incident Response Manager-Team ist gerne bereit, mit den vom Versicherten bevorzugten Anbietern zusammenzuarbeiten, auch wenn diese nicht unserem Pool angehören.

- Die Police beinhaltet die Inanspruchnahme von Anbietern, die von unseren Kunden bereits in deren Cyber-Incident Response-Plan aufgenommen wurden.
- Mit unserem weltweiten Netz lokaler Incident Response-Teams können wir die Anforderungen multinationaler Risiken erfüllen.
- Chubbs für Risiko- und IT-Manager konzipierte Cyber Alert® App ist an unser Incident Response- und Schadenteam angeschlossen, wo die Unterstützung durch Experten und die zu treffenden Massnahmen koordiniert werden.
- „Emergency Incident Response“ bietet Unterstützung nach einem Cybervorfall.

Hier sehen Sie, wie Chubbs Incident Response-Lösung in der Praxis funktioniert.

Grossunternehmen

1 Multinationale Programme

Die Globalität der Cyberrisiken bringt es mit sich, dass Unternehmen wissen müssen, was ihre Versicherungspolicen bei Vorfällen internationalen Ausmasses leisten und ob etwaige Einschränkungen bestehen. Die Gestaltung eines effektiven, kostengünstigen multinationalen Versicherungsprogramms setzt die genaue Kenntnis des veränderlichen regulatorischen Umfelds im Cyberbereich voraus.

Hier einige wichtige Fragen, die sich jeder vor dem Abschluss eines multinationalen Versicherungsprogramms stellen sollte:

- In welchen Ländern befinden sich die Gesellschaften und Niederlassungen? Etwaige Einschränkungen können von Land zu Land verschieden sein.
- Ist es Non-Admitted-Versicherern in den jeweiligen Ländern gestattet, direkte Schadenzahlungen an die dort ansässigen Gesellschaften zu leisten? Welche spezifischen Länderbeschränkungen gibt es?
- Möchte der Kunde die Versicherten vor Ort absichern? Vorteile einer lokalen Police sind u. a.: lokale Schadenzahlungen, Policen-Wordings in Landessprache und Schadenbearbeitung vor Ort.

Chubbs multinationale Cyber-Kompetenzen:

Chubb ist in der Lage, multinationale Cyber-Programme anzubieten, die in 35 Ländern einen lokalen und verlässlichen Deckungsschutz bieten. Die Programme werden von Chubbs umfassend besetztem Global Services- Team betreut, das über die entsprechende Expertise sowie Spezialisten verfügt, die bei jeglichem Bedarf an multinationalem Versicherungs-schutz helfen können.

2 Global Cyber Facility

Die umfassende Cyber-Risikomanagementlösung für Grossunternehmen:

Mit wem arbeiten wir zusammen?

- Unternehmen mit einem Jahresumsatz von über 1 Mrd. USD.
- Allen Branchen, u. a. Einzelhandel, Finanzinstitute und produzierende Industrie.

Bestandteile unseres Angebots:

- Schadenpräventionsdienstleistungen vor dem Schadenfall seitens international anerkannten, auf die Abwehr von Cyber-Angriffen spezialisierten Unternehmen, um Cyber-Schwachstellen zu beseitigen, die im Rahmen der Risikobeurteilung erkannt wurden.
- Massgeschneiderte Risikotransfer-Police.
- Post-Event-Massnahmen und Schadenmanagement.

Wesentliche Elemente des Deckungsschutzes:

- Grundvertragskapazitäten von 30 Mio. bis 100 Mio. EUR, von Chubb bereitgestelltes Kapital zur Unterstützung grosser Versicherungsprogramme.
- DIC/DIL-Deckung zur Schliessung von Lücken zwischen den Cyber-, Haftpflicht- und Sachversicherungspolicen eines Unternehmens.
- Massgeschneiderte, flexible Policenformen verfügbar.

Wie gestaltet sich der Prozess im Einzelnen?

- Proaktive Anbahnung drei Monate vor der Ausschreibung am Markt.
- Chubb-eigene Beurteilung zur Analyse des Risikoprofils des Unternehmens.
- Direkter Kontakt zwischen dem Kunden und dem Underwritingteam von Chubb (auch Risk Engineering verfügbar).

Grossunternehmen

3 Captives

Die Handhabung von Cyberrisiken über ein Captive kommt für immer mehr multinationale Unternehmen in Frage, für die eine Kombination aus Risikotransfer und Selbstbehalt sinnvoll ist. Captives sind immer häufiger die Lösung, um adäquate, aber dennoch bezahlbare Prämien aufrechtzuerhalten oder lokale Policen-Selbstbehalte in eine konsolidierte Struktur auszugliedern.

Ein Captive kann aber auch einen umfassenderen Deckungsschutz bieten als er am Gewerbeversicherungsmarkt für die Muttergesellschaft erhältlich wäre. Unternehmen können auf diese Weise ein eingehendes Verständnis ihrer Risiken gewinnen und Schadendaten sammeln, sodass ein Versicherer oder Rückversicherer das Risiko anschliessend zu einem angemessenen Limit und Beitrag übernehmen kann.

Warum?

- Optimierung des Risikotransfers
- Diversifizierungsmöglichkeit
- Bildung eines Datenpools
- Möglichkeit der späteren Erweiterung der Services

Wie?

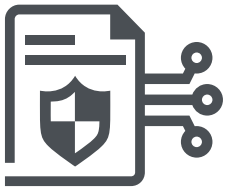
- Verschiedene Strukturen möglich
- kleine Grundverträge/ Grosse Selbstbehalts-Layer
- Prozentuale Beteiligung an grossen Programmen
- Gefahrenspezifisch

Herausforderungen

- Verständnis der Risiken und Unwägbarkeiten
- Preisgestaltung des Selbstbehalts-Layers
- Aggregierung mit anderen Sparten

Haupt-Verkaufsargumente

Nicht alle unsere Kunden verstehen, wie wichtig Cyber-Policen sind und wie viele Vorteile sie bieten können. Wir haben deshalb einige wichtige Fakten zusammengestellt, damit Sie Ihren Kunden die wesentlichen Vorteile besser erläutern können.



Affirmativer Deckungsschutz

Klassische Versicherungspolicen bieten nicht immer ausreichenden Schutz vor Cyberrisiken. Cyber-Versicherungen hingegen sind eigens dafür konzipiert, solche Lücken zu schliessen und Deckung für Risiken bereit zu stellen, die schwer einzuschätzen sind.

Man muss nicht das direkte Ziel eines Cyber-Angriffs sein, um hiervon betroffen zu werden

Cyber-Angriffe können sich über Ihre Lieferanten oder externe Technologie-anbieter ausbreiten und erhebliche Folgen haben, auch wenn Sie selbst nicht das Angriffsziel waren. Chubb konnte in der Vergangenheit hohe Kollateralschäden feststellen, die aus Vorfällen in anderen Unternehmen resultierten. Stellen Sie sich vor, was passiert, wenn Ihr Data-Storage-Anbieter Ziel eines Angriffs wird und Ihre Daten manipuliert werden.

Die Versicherung kommt für Aufwendungen für Abhilfe-massnahmen und Wiederher-stellungskosten auf, nicht nur die Datenmanipulation.

Die Haftung aufgrund des Verlusts oder Missbrauchs sensibler Daten ist nur eine der Folgen, die ein Cybervorfall haben kann. Betriebsunterbrechung, Incident Response und Wieder-herstellungskosten machen auch ohne Berücksichtigung von Haftpflicht-ansprüche einen erheblichen Teil der von Chubb geleisteten Schaden-zahlungen aus.

Ergänzung bestehender IT-Teams

Cyber-Versicherungen „unterminieren“ keinesfalls die Effizienz von IT-Sicherheitsteams, sondern ergänzen vielmehr deren Kompetenz und schützen Unternehmen vor dem Unbekannten.

Haupt-Verkaufsargumente

Multinationale Bedrohungen

Cyber-Schäden entstehen nicht nur in den Vereinigten Staaten. Chubb hilft Unternehmen dabei, nach einem Cybervorfall, ganz gleich, wo dieser sich ereignet, zur normalen Geschäftsbetrieb zurückzukehren, hierin eingeschlossen Vorfälle wie Datenpannen und die Einschleusung von Ransomware.

Jedes Unternehmen kann betroffen sein

Cybervorfälle können jedes Unternehmen treffen, unabhängig von seiner Grösse und Branche. Es kann sich um zielgerichtete Angriffe handeln, Fehler von Mitarbeitern oder Kollateralschäden von Angriffen, die sich anderswo ereignet haben. Chubb verfügt über flexible Lösungen für Ihre spezifischen Anforderungen, die dem Reifegrad und der jeweiligen Grösse Ihres Unternehmens entsprechen.

Reaktion auf regulatorische Veränderungen

Neue Datenschutzbestimmungen erfüllen immer höhere Standards und sehen auch immer höhere Strafen vor - genau hier können Ihnen Cyber-versicherungen helfen. Die von Chubb angebotenen Policen passen sich den neuen Bestimmungen an.

Anpassung an neue Cyberrisiken

Chubb informiert Sie vierteljährlich über aktuelle Trends, die wir bei neuartigen Cyber-Schadenfällen erkennen, damit Sie stets auf dem Stand der Dinge sind. Zudem bietet Ihnen der Cyber IndexSM von Chubb aktuelle Information über historische Trends und neueste Entwicklungen.

Hacksagon!

Kennen Sie schon Chubbs Cyber-Brettspiel Hacksagon? Hacksagon ist ein sehr gutes Verkaufs- und Trainings-Tool, mit dem Sie Ihren Kunden ein besseres Verständnis über Cyberbedrohungen und die vom Unternehmen zu ergreifenden Massnahmen vermitteln können. Bitte wenden Sie sich zwecks näherer Informationen hierzu an den für Ihre Region zuständigen Underwriter.

Schadenpräventionsdienstleistungen

Die allgemeine Schadenentwicklung hat gezeigt, dass es Themen gibt, die viele Branchen und Kundensegmente betreffen. Mitarbeiterfehler, missbräuchliche Verwendung und soziale Angriffe wie Phishing sind häufige Ursachen für Cyberschäden, können aber durch das entsprechende Bewusstsein und Schulungsmassnahmen verhindert oder auf ein Mindestmass begrenzt werden.

Im Umfang der Cyber-Versicherungslösung von Chubb sind Schadenpräventionsdienstleistungen enthalten, die darauf ausgerichtet sind, häufige Ursachen für Cyberschäden weitestgehend zu unterbinden. Unseren Versicherungsnehmern steht eine Vielzahl an Serviceleistungen wie **Passwortschutz, Phishing-Schulungen und die Verbesserung des Mitarbeiterbewusstseins** zur Verfügung.

Unsere Unternehmensrisikophilosophie zeigt, wie wichtig es uns ist, dass unsere Kunden ihr Cyber Risk Management weiter verbessern. Durch unsere Zusammenarbeit mit externen Experten haben Kunden Zugang zu Serviceleistungen, die der Verbesserung des Cyberschutzes dienen, sich leicht umsetzen lassen und oftmals sogar kostenlos sind.

Die **Registrierung** für diesen Service ist über Chubbs Cyber Services-Website möglich, auf der Sie auch viele weitere Informationen finden:

www.chubb.com/cyber-services

Schadenpräventionsdienstleistungen

1. Passwortverwaltung von Dashlane

Passwörter sind die Grundlage solider Online-Sicherheitsmassnahmen. Die von Chubb gesammelten Schadendaten zeigen, dass eine defizitäre Passwortverwaltung zu gravierenden Cyberschäden führen kann. Aus diesem Grund stellt Chubb das Passwort-Management-Tool von Dashlane allen seinen Cyber-Versicherungskunden als Ergänzung zur Verfügung.

2. Phishing-Sensibilisierung von Cofense

Mit dem Phishing-Schulungsprogramm von Cofense können Schwachstellen und Risiken im Zusammenhang mit Phishing-Angriffen ermittelt werden, eine der Hauptursachen vieler Cyberschäden in der Vergangenheit.

3. Cyber Alert®-App von Chubb

Richtig auf einen Cybervorfall zu reagieren ist nicht immer einfach. Stehen in dieser Situationen keine Spezialisten zur Verfügung, kann der Schaden noch grösser werden. Über Chubbs kostenlose Cyber Alert®-App können Versicherte einen Schaden umgehend melden und unsere Experten im Umgang mit Cybervorfällen sofort erreichen.

4. Weitere Serviceleistungen

Policeninhabern bestimmter Länder stehen Cybersicherheitsschulungen, Risikobeurteilungen, Planungsübungen und weitere Services zur Begrenzung von Cyberschäden zur Verfügung. Hier können Sie sehen, welche Serviceleistungen in Ihrem Land angeboten werden:

www.chubb.com/uk-en/business/cyber-services-registration.aspx

Erfahren Sie mehr über unseren Incident Response-Service in einer Zeit, in der sich Cyber-Ereignisse nicht vermeiden lassen.

Weitere Informationen

Incident Response-Services – Übersicht

Die von Chubb angebotenen Dienstleistungen zur Prävention von Cyberschäden können die Wahrscheinlichkeit von Cybervorfällen verringern, generell muss aber gesagt werden, dass es keinen perfekten Schutz vor Cyberbedrohungen gibt. Die Cyberpolicen von Chubb umfassen ein Netzwerk von Incident Response-Experten, die täglich rund um die Uhr erreichbar sind und die unsere Versicherten nach einem Cybervorfall bei der Wiederaufnahme des Geschäftsbetriebs unterstützen können.

Highlights

Chubb hilft weltweit drei bis fünf Unternehmen pro Tag, ihren Geschäftsbetrieb nach einem Cybervorfall wieder aufzunehmen.

Versicherte, die das Cyber Incident Response Centre von Chubb verständigen, erhalten **umgehend Unterstützung** von einem Cyber Reporting-Experten, der die wichtigsten Angaben abfragt, um das entsprechende Expertenteam zusammenzustellen.
90 % der Versicherten erhalten innerhalb von 15 Minuten ein Rückruf von einem Cyber Incident Response Manager.

Freie Auswahl der Anbieter - uns ist bewusst, dass manche Unternehmen Anbieter vorziehen, die bereits zu ihren festen Dienstleistern gehören. Chubb bietet sein Versicherten in vielen Ländern die Möglichkeit, Spezialisten ihrer Wahl zu beauftragen, die dann nahtlos in unser Incident Response-Netzwerk integriert werden können.

Sehen Sie hier den Ablauf unserer Incident Response-Massnahmen:

Weiter

Incident Response-Services – So funktioniert es

In diesem Leitfaden erfahren Sie, wie Sie sich mit dem Incident Response-Team von Chubb in Verbindung setzen können, einen Schaden melden und was Sie von unserer Incident Response Plattform erwarten können.

1 Bei einem Kunden kommt es zu einem Cybervorfall

Chubbs Incident Response Platform ist rund um die Uhr an allen Tagen im Jahr erreichbar. Sie bietet Zugang zum Cyber Incident Response Centre von Chubb sowie unserem Cyber Incident Response Team. Auf diese Weise können Cybervorfälle holistisch gemanagt werden.

2 Er meldet diesen entweder über:

Chubbs Cyber Alert® Mobil-App

Im Apple Store und Google Play Store erhältlich:

Download on the App Store | ANDROID APP ON Google play

das Internet

Zugriff auf unsere Plattform: **www.chubbcyberalert.com**

oder die Telefon-Hotline

Rufnummern der einzelnen Länder siehe unten:

Gebührenfreie lokale Rufnummern

Argentinien	**800 666 1967**
Australien	**1 800 027428**
Belgien	**800 49 405**
Brasilien	**0800 095 7346**
Chile	**1 230 020 1212**
China	**400 120 5310**
Dänemark	**80 250 571**
Deutschland	**0800 589 3743**
Finnland	**0 800 1 12382**
Frankreich	**08 05 10 12 80**
Grossbritannien	**0800 279 7004**
Hongkong	**800 900 659**
Indonesien	**001 803 011 2974**
Irland	**1 80 093 7331**
Israel	**1 80 921 3812**
Italien	**80 019 4721**
Japan	**00531 1 21575**
Kanada	**1 866 561 8612**
Kolumbien	**01 800 518 2642**
Malaysia	**1 800 8 12541**
Mexiko	**001 855 250 4580**
Neuseeland	**0800 441402**
Niederlande	**0800 020 3267**
Norwegen	**800 12554**
Österreich	**0800 005 376**
Panama	**001 800 507 3360**
Peru	**0800 56006**
Polen	**00 800 121 4960**
Portugal	**800 8 14130**
Schweden	**020 088 3181**
Schweiz	**080 016 6223**
Singapore	**800 120 6727**
Spanien	**800 810 089**
Südafrika	**080 09 82340**
Südkorea	**00798 14 800 6017**
Taiwan	**00801 13 6828**
Tschechien	**800 142 853**
Türkei	**0811 213 0171 (Festland)**
Türkei	**0812 213 0043 (Mobil)**
USA	**1 844 740 9227**
Vereinigte Arabische Emirate	**8000 444 4411**
Vietnam	**1203 2353 (VNPT)**
Vietnam	**1228 0688 (Viettel)**

Incident Response-Services – So funktioniert es

3 Anruf vom Incident Response Centre von Chubb

Innerhalb 1 Minute nach der Meldung des Vorfalls wird der Kunde mit einem Berater verbunden, der folgende Daten abfragt:

- Name des Versicherten
- Land, in dem die Police abgeschlossen wurde
- Kontaktdaten
- Ort des Vorfall

Informationen werden an das lokale Incident Response Management übermittelt und können an die Schaden-abteilung von Chubb weitergeleitet werden. Die effektivste Massnahme ist es, Chubb jederzeit auf dem Stand der Dinge zu halten.

4 Incident Response Management

Innerhalb 1 Stunde nach der Meldung erhält der Kunde einen Rückruf vom für den Schadenort zuständigen Incident Response Manager. Die nächsten Schritte sind:

- Durchführung einer ersten Untersuchung
- Ausarbeitung eines Massnahmenplans, um die Auswirkungen des Vorfalls zu begrenzen
- die Beauftragung von Spezialisten, die beratend und bei der Wiederherstellung mitwirken:

IT Forensik | Rechts-Beratung | Public Relations | Regulatorische Compliance | Identitäts-schutz | Bonitäts-über-wachung | Forensic Accountancy

5 Wiederherstellung

Mit einem Expertenteam von Anbietern, das daran arbeitet, das Ereignis einzudämmen, unterstützt Sie das Cyber Incident Response Team bei der Wiederherstellung Ihrer Geschäftsaktivitäten.

6 Nachbearbeitung

Die spezialisierten Anbieter von Chubb werden anschliessend die Bereitstellung zusätzlicher Dienste mit Ihnen besprechen, um Sie bei der Analyse der Vorfalls zu unterstützen, künftige Abhilfemassnahmen festzulegen, die gewonnenen Erkenntnisse mit Ihnen zu besprechen und Ihnen Ratschläge für die Risikominderung zu geben.

Deckungsschutz - Cyber Enterprise Risk Management *(Version 2)*

Der Deckungsschutz

Eigenschaden

- **Incident Response** - nach einem stattgefundenen oder vermuteten Cybervorfall - häufig ohne Selbstbehalt
- **Betriebsunterbrechung** - Nettogewinneinbussen und weiter entstehender zusätzlicher Betriebsaufwand
- **Daten- und Systemwiederherstellung** - erhöhte Arbeitskosten, Datenwiederherstellungskosten, Mehrkosten für die Minimierung der Betriebsunterbrechung

Drittschaden

- Haftung bei **Datenschutz- und Netzwerksicherheitshaftung** nach einer Daten- oder Netzwerksicherheitspanne:
- **PCI DSS**-Vertragsstrafen und Geldbussen
- **Verbraucherentschädigungsfonds**
- **Aufsichtsbehördliche Geldbussen und Strafen** (wo gesetzlich versicherbar) - DSGVO
- **Medienhaftung** - Haftpflicht aufgrund von Diffamierungen oder Rechtsverstössen im Internet

Die Deckungshighlights

- **Betriebsunterbrechung durch Rückwirkungsschäden** bei externen Technologieanbietern
- Auslöser von **Systemausfällen** - menschliches Versagen, Programmierfehler, Stromausfälle
- **Standarderweiterungen:**
  - **Nofallbedingte Incident Response-Kosten** innerhalb 48 Stunden für KMU und Unternehmen aus dem mittleren Marktsegment - **ohne Selbstbehalt**
  - **Verbesserungskosten** - Verbesserungen von Software und Applikationen
  - **Cyber- Kriminalität** - unmittelbare finanzielle Einbussen aufgrund eines Cyberdiebstahls
  - **Belohnungsaufwendungen**
  - **Telekommunikationsbetrug**
- Übernahme der Incident Response-Kosten im Namen der Versicherten
- **Freie Wahl der Incident Response-Anbieter**
- **Schäden durch böswillige Mitarbeiter**
- **Freiwillige Meldungen**
- **Freiwillige Abschaltung**
- **Cyberterrorismus**
- **Weltweite** Deckung
- Per Zusatzvereinbarung: **Reputationsschaden**-Erweiterung, **Social Engineering** Betrug

Risikoappetit

Die folgende Liste soll Ihnen und Ihren Kunden einen allgemeinen Überblick darüber geben, welche Risiken wir eingehen. Die Auflistung ist nicht vollständig und dient lediglichder allgemeinen Orientierung. Bitte wenden Sie sich hinsichtlich spezieller Risiken und Branchen, die im Folgenden nicht aufgeführt sind, an unser Underwriting-Team, das Ihre Anforderungen mit Ihnen besprechen wird.

Bevorzugt

- Werbung*
- Landwirtschaft
- Architekten und Ingenieure
- Kunstgalerien und Museen
- Autohandel / Kfz-Werkstätten und Tankstellen
- Kommunikation* Bauwesen
- Ingenieur-, Management- und Industriedienst-leistungen
- Staatlicher Sektor
- Gemeinnützige Organisationen
- Druck- und Verlagswesen*
- Öffentliche Verwaltung
- Immobilien
- Kleinere Schulen / Schuldirektorien, Vorschulen, primärer und sekundärer Bildungsbereich
- TV-/Radio-/Film-produktion*
- Grosshandel

Akzeptiert

- Steuerberater / Wirtschaftsprüfer
- Gesundheitsdienst-leister
- Vermögensverwalter Hochschulen und Universitäten
- Computer-Hardware / Software
- Arzt-/Zahnarztpraxen
- Büros
- Arbeits- / Personalvermittlungen
- Beratungsfirmen allgemein
- Wirtschaftskanzleien
- Chemikalien und verwandte Produkte
- Managementberater
- Marketingberater
- Bergbau
- Baufinanzierungsmakler
- Darstellende Künste und Theater*
- Persönliche Dienstleistungen
- Fachdienstleistungen - Sonstige
- Technische Berater Wirtschaftsverbände Transportdienst-leistungen - Sonstige
- Lebensmittelherstellung
- Industrielle Fertigung
- Erzeugnisse
- Herstellendes Gewerbe

Selektiv

- Einrichtungen für betreutes Wohnen
- Rundfunk* Callcenter
- Inkassounternehmen
- Rohstoffhändler
- Rohstoffbörsen
- Verwahrstellen
- Institutionen
- Finanzinstitute - Sonstige
- Krankenhäuser
- Versicherungen - ohne Personal Lines
- Investment- / Fondsmanager
- Notariate
- Pflege- / Seniorenheime
- Behörden / Spezialbereiche
- Restaurants / Gastgewerbe
- Einzelhandel
- Sparkassen / Retail-Banking
- Wertpapier- und Rohstoffmakler
- Telekommunikation
- Telemarketingdienst-leistungen*
- Rechtstitel-versicherungsagent
- Versorgungs-unternehmen

Opportunistisch

- Kasinos
- Kritische Infrastruktur
- Datenverarbeitung
- Direktmarketing*
- EMR-Storage Factoring-Unternehmen
- Gesundheitssysteme
- Versicherungsträger - Personal Lines
- Internet-Spieleplatt-formen
- Online-Medien-Streaming*
- Zahlungskarten-verar-beitung
- Lohnbuchhaltungs-dienstleistungen

Nicht zulässig

- Nicht jugendfreie Inhalte
- Fluggesellschaften
- Kryptowährungsbörsen
- Initial Coin Offerings
- Datenaggregatoren
- Onlinebörsen
- Websites/Applikationen sozialer Netzwerke
- Handelsplattformen

*Ohne Medien-E&O-Deckung

CHUBB®

Weitere Informationen

Nähere Informationen zu unseren Cyber-Angeboten erhalten Sie von unseren Underwritern und auf unserer Website **www.chubb.com/ch**

Zurück zur Startseite