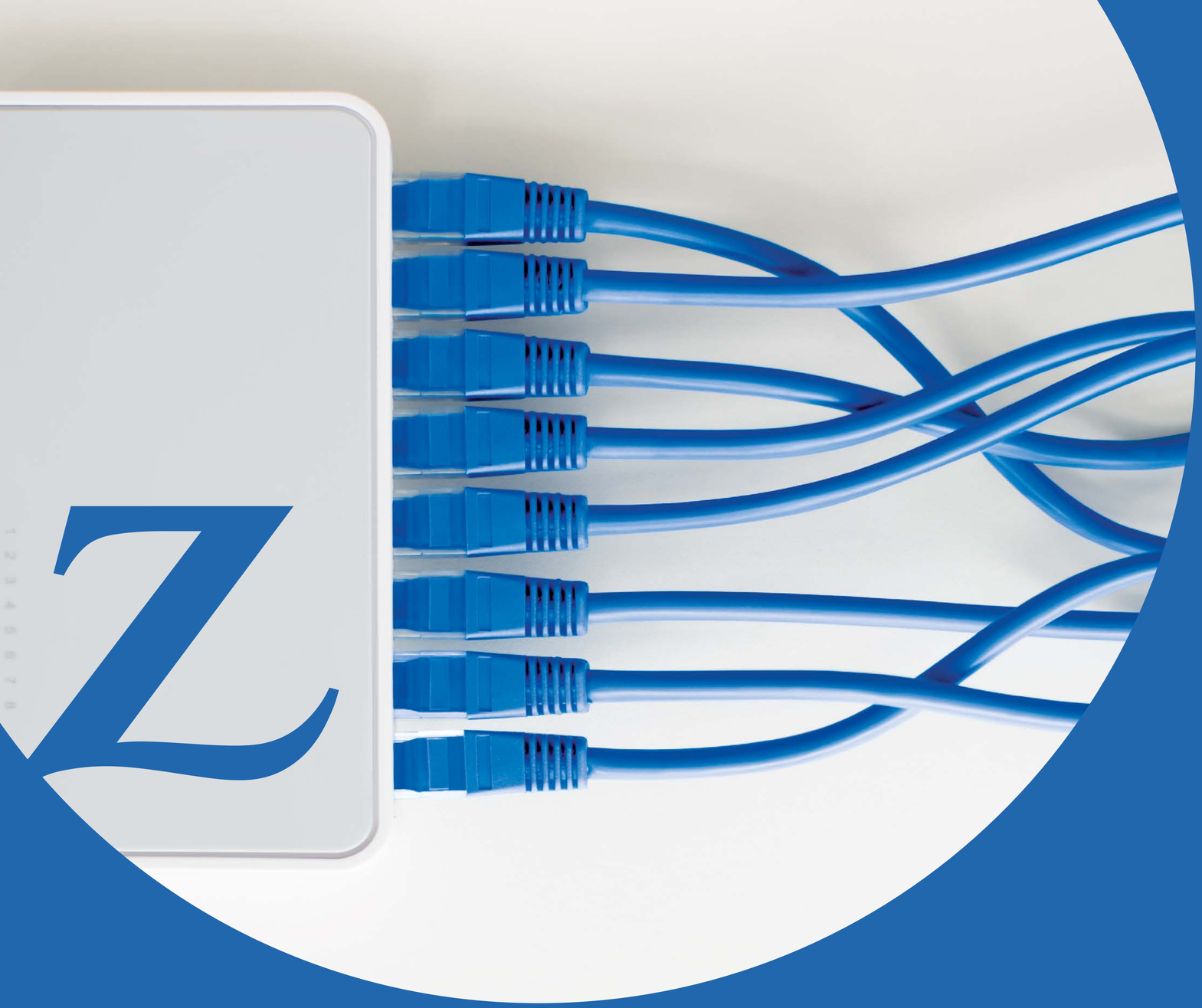


ZURICH

Broschüre Cyberversicherung

Inhaltsverzeichnis

Digitalisierung – Chance und Risiko zugleich

Der digitale Wandel bietet Schweizer KMUs enorme Chancen: Sie können bestehende Prozesse vereinfachen, Produkte und Dienstleistungen optimieren und so Mehrwert für ihre Kunden schaffen. Dieser Wandel beansprucht oft die volle Aufmerksamkeit der Unternehmensführung. Cyberrisiken rücken dabei oft in den Hintergrund und werden vernachlässigt. Dabei ist es immens wichtig, sich vor Cyberrisiken zu schützen – damit die Unternehmerinnen und Unternehmer das Potenzial der Digitalisierung nutzen können und von unliebsamen Nebenwirkungen verschont bleiben.

Nationalrätin Doris Fiala, Präsidentin der Swiss Cyber Security Days, ist überzeugt: «Die Digitalisierung ist eine riesige Chance, birgt aber auch einige Risiken.» Laut Hochrechnungen entstehen gemäss Fiala alleine in der Schweiz jährlich Kosten in Höhe von 5 Mrd. Franken durch Cyberkriminalität: «Das ist mehr als das Armeebudget.» Vielen Schweizer KMU ist noch gar nicht bewusst, dass auch sie betroffen sein können, hat Doris Fiala beobachtet. «Die KMU müssen im täglichen Wettbewerb stark auf die Kosten achten und scheuen deshalb oft die Ausgaben für Informationssicherheit. Doch ein guter Schutz auf allen Stufen lohnt sich.»

Die hohe Relevanz von Cyber-Risiken für KMUs belegt auch eine aktuelle Umfrage des Instituts gfs-zürich. Von über 500 befragten Geschäftsführenden gab jeder vierte an, schon Opfer eines folgenschweren Cyberangriffs gewesen zu sein.

Digitalisierung – Chance und Risiko zugleich

Die Digitalisierung umfasst alle Branchen: In fast allen Unternehmen findet der Grossteil der täglichen Kommunikation und Büroarbeit computergestützt statt. Je nach Tätigkeit bieten Unternehmen darüber hinaus weitere Angriffsflächen:

Freie Berufe wie Architekten oder Ingenieure
Entwurf, Planung und Berechnung sind heute vollständig computerisiert, z.B. durch den Einsatz von CAD-Programmen. Ohne funktionierende IT-Infrastruktur kommen sämtliche Arbeiten zum Erliegen.

Handel und Logistik
Bestellungen, Lagerbewirtschaftung und Vertrieb werden durch ERP-Systeme abgebildet. Auch Verkaufsprozesse zu den Endkunden verlagern sich immer mehr ins Internet.

Beherbergung, Gastronomie und Unterhaltung
Bestellungen und Personaleinsatzplanung sowie sämtliche Administration werden über spezialisierte Software abgewickelt. Buchungen und Bestellungen finden mehr und mehr online statt, zum Teil auch per App.

Finanzdienstleistungen
Praktisch sämtliche Transaktionen sind vollständig digitalisiert – Einzahlungen, Wertschriftenhandel, sogar Hypotheken werden immer häufiger online abgeschlossen oder erneuert.

Gesundheit, Betreuung und Soziales
Behandlungen und Patientenmanagement werden durch zentrale Informationssysteme geplant und gestützt. Patientendossiers sind zunehmend digital und erleichtern die Arbeit des behandelnden Personals. Ohne diese Systeme funktioniert heute wenig.

Produktion
Die Herstellungsprozesse sind – je nach Branche und Firma – bereits zu einem grossen Teil durch automatisierte Anlagen und Robotik gestützt. Ohne funktionierende Steuerung dieser Anlagen steht die Produktion still.

Typische Tricks der Hacker

Angriffsmuster

Bankraub war gestern. Wer heute schnell ans grosse Geld kommen will, braucht dafür kein Stemmeisen, keine Pistole und kein Fluchtauto. Sondern eine gute Internetverbindung, einen scharfen Verstand und viel kriminelle Energie. Die häufigsten «Angriffsmuster» von Cyberkriminellen sind:

- Blockierung von IT-Infrastrukturen
- Datendiebstahl
- Denial of Service
- Cyber-Betrug

Einfallstore

Doch wie verschaffen sich Cyber-Kriminelle Zugang zu IT-Infrastrukturen, um einen Angriff auszuführen? Obwohl die gängigen Methoden von Cyber-Angreifern bekannt sind, haben sie immer noch mit vielen Angriffen Erfolg. Zu den gängigsten «Einfallstoren» zählen:

- Fernzugriffe
- Phishing
- Drive-by-Infektionen
- Nicht aktualisierte Systeme oder Fehlkonfigurationen
- Drittparteien (z.B. externe Dienstleister)

Typische Tricks der Hacker

Angriffsmuster Einfallstore

Bankraub war gestern. Wer heute schnell ans grosse Geld kommen will, braucht dafür kein Stemmeisen, keine Pistole und kein Fluchtauto. Sondern eine gute Internetverbindung, einen scharfen Verstand und viel kriminelle Energie. Doch wie kommen Hacker konkret zu ihrem Ziel? Trotz der Vielfalt und Raffinesse der Cyber-Attacken entspricht ein Grossteil der tagtäglich stattfindenden Schadenfälle wenigen gängigen Mustern:

Blockierung von IT-Infrastrukturen
Cyber-Angreifer verschaffen sich Zugang zu IT-Infrastrukturen und blockieren diese. Gängiges Mittel hierfür ist sogenannte «Ransomware», zu Deutsch «Lösegeldsoftware» – und genau darum geht es auch. Der Angreifer schleust ein Programm zur Verschlüsselung von Daten und Programmen auf zentrale IT-Infrastrukturen (z.B. Windows-Domaincontroller, ERP-System) ein. Dann kontaktiert er sein Opfer und informiert es, dass er ihm nur gegen ein Lösegeld den digitalen Schlüssel für die Entschlüsselung und Entsperrung der Daten und Programme wieder zur Verfügung stellt. Oft hat der Angreifer neben den operativen Systemen auch Backup-Systeme verschlüsselt – deshalb ist die Situation für viele Betroffene alternativlos und sie kommen der Lösegeldforderung nach.

Datendiebstahl
Cyber-Angreifer verschaffen sich Zugang zu IT-Infrastrukturen mit sensitivem Datenmaterial und entwenden eine Kopie dieser Daten. Besonders wertvoll für die Hacker sind Kundendaten – sie können für diverse Betrugsversuche verwendet werden. Das gilt vor allem für Kreditkartendaten oder Informationen, mit welchen Identitäten gefälscht werden können (z.B. Passkopien).

Typische Tricks der Hacker

Angriffsmuster Einfallstore

Denial of Service

Cyber-Angreifer überfluten die elektronischen Kommunikationskanäle von Firmen mit Millionen elektronischen Anfragen. Die betroffenen Systeme, etwa Webseiten oder Voice-over-IP-Telefonsysteme, werden dadurch überlastet und versagen ihren Dienst. Üblicherweise nutzen die Hacker für solche Angriffe Botnetze – tausende im Vorfeld gehackte private Computer oder auch Haushaltsgeräte – welche auf Kommando gleichzeitig auf ebendiese Kommunikationskanäle des Opfers zugreifen. Meistens folgt anschliessend eine Lösegeldforderung: Wenn das betroffene Unternehmen keinen weiteren Angriff erleben will, muss es zahlen.

Cyber-Betrug

Hacker nutzen elektronische Kommunikationskanäle, um Mitarbeitende zu Geldüberweisungen zu verleiten und sich dadurch selbst zu bereichern. Dabei werden üblicherweise Krisenszenarien vorgegaukelt – der Angreifer gibt sich z.B. als CEO, CFO oder eine andere Führungskraft des Unternehmens aus. Oft werden dabei kompromittierte E-Mail-Konten verwendet. Dies sind E-Mail-Konten, welche die Angreifer mittels gestohlener Benutzernamen und Passwörter gekapert haben. Diese Masche wird gemeinhin auch als Business Email Compromise (BEC) bezeichnet.

Typische Tricks der Hacker

Angriffsmuster **Einfallstore**

Egal, welcher der genannten Angriffe geschieht – schnelles Handeln ist gefragt, um den Schaden zu begrenzen. Darüber hinaus gilt es, das Risiko künftiger Vorfälle zu reduzieren, mit technischen oder organisatorischen Massnahmen. Obwohl die gängigen Methoden von Cyber-Angreifern bekannt sind, haben sie immer noch mit vielen Angriffen Erfolg. Im nächsten Abschnitt sind die gängigsten «Einfallstore» der Cyber-Kriminellen beschrieben. Sie ermöglichen oft sogar mehrere Angriffsmuster:

Fernzugriffe

In der Coronazeit haben viele Unternehmen Möglichkeiten für ihre Mitarbeitenden geschaffen, damit diese sich aus dem Homeoffice ins Firmensystem einloggen können. Das war ein Highlight für die Cyberkriminellen weltweit. Denn eine hohe Sicherheit bieten nur solche Fernzugriff-Technologien, die einen Passwortschutz mit einer Multifaktor-Authentisierungslösung kombinieren. Das ist oft bei VPN der Fall. Doch viele Firmen scheuen die Kosten dafür und haben stattdessen auf ein ausschliesslich passwortgeschütztes System gesetzt. Besonders häufig anzutreffen ist hierbei das Remote Desktop Protokoll (RDP). Cyber-Angreifer erkennen diese RDP-Schnittstellen relativ rasch und vielen ist es durch Ausprobieren von Benutzername und Passwort-Kombinationen gelungen, eine Remote-Desktopsitzung aufzubauen. Ab diesem Moment ist es dem Hacker möglich, weiter ins Netz vorzudringen, um Daten zu stehlen oder eben auch Ransomware-Angriffe durchzuführen.

Phishing

Beim Phishing steht der Faktor «Mensch» im Zentrum, denn der Mitarbeitende übernimmt unfreiwillig eine aktive Rolle in der Cyber-Attacke. «Phishing» ist eine spezielle Art des Social Engineering, also der sozialen Manipulation. Social Engineering will Menschen zu Handlungen verleiten, die für sie selbst schädlich sind. Geschieht diese Manipulation per E-Mail, spricht man üblicherweise von Phishing. Per Phishing-E-Mails werden Mitarbeitende beispielsweise dazu verleitet, vertrauliche Informationen preiszugeben oder Schadsoftware auf ihren Computern zu aktivieren, etwa per Anhang oder Link auf eine Webseite. Anschliessend können die Angreifer weiter ins Netz vordringen und Daten stehlen oder Ransomware-Angriffe starten.

Typische Tricks der Hacker

Angriffsmuster **Einfallstore**

Drive-by-Infektionen

In vielen Unternehmen werden Anwendungen zu selten aktualisiert. Oft sind Browser mit bekannten Schwachstellen im Einsatz, z.B. in sogenannten «Plugins». In diesem Fall reicht es, dass ein Mitarbeitender eine gehackte oder «bösartige» Webseite besucht. Diese erkennt die Schwachstelle im Browser und nistet sich ins Computersystem des Opfers ein. Der Besuch einer falschen Webseite kann also ausreichen, um Schadsoftware ins Unternehmen zu transportieren.

Nicht aktualisierte Systeme oder Fehlkonfigurationen

Praktisch jedes Unternehmen betreibt heute eine Vielzahl von IT-Systemen, welche direkt mit dem Internet verbunden und dadurch von überall auf der Welt erreichbar sind. Diese Systeme bestehen aus der Betriebssystemschicht sowie üblicherweise einer Vielzahl von Applikationen. Die meisten Unternehmen sind damit überfordert, sämtliche Systeme ständig aktuell zu halten – zumal praktisch täglich neue Updates und «Sicherheitspatches» der Softwarehersteller erscheinen. Deshalb kommt es vor, dass Sicherheitslücken über Monate oder gar Jahre nicht geschlossen werden. Sobald ein Cyber-Angreifer solche Sicherheitslücken erkennt, kann er sie ausnutzen (z.B. via sogenanntem «Exploit») und sich Zugang zu Daten verschaffen oder gar die Kontrolle über die Systeme erlangen.

Drittparteien (z.B. externe Dienstleister)

Bei den «Einfallstoren» via Fernzugriff, Phishing, Drive-by-Infektionen oder nicht aktualisierte Systeme erfolgt ein direkter Angriff auf das Unternehmen. Doch Cyber-Kriminelle können auch Schwachstellen von Drittparteien nutzen. Teilt ein Unternehmen sensitive Daten mit einem Dienstleister oder bezieht es Software-Dienstleistungen von Dienstleistern, ist dieses Unternehmen nämlich nicht nur den eigenen Sicherheitsrisiken ausgesetzt, sondern auch denjenigen des Dienstleisters.

Wappnen Sie sich und reduzieren Sie Ihre Risiken

Die 8 wichtigsten Tipps Weitere Informationen zum Thema

Auch wenn jedes Unternehmen einzigartig ist, haben wir für Sie die wichtigsten Tipps aufgelistet:

1. Risikoanalyse als Managementaufgabe: Welche sind meine «Kronjuwelen» und wie kann ich diese schützen? Dazu gehört auch ein professionelles Krisenmanagement mit Notfallplan für Cyber-Angriffe.

2. Schulen Sie Ihre Mitarbeitenden im Umgang mit Daten und E-Mails, da diese das häufigste Einfallstor für Schadsoftware und somit auch Angriffe darstellen.

3. Nutzerrechte jährlich und bei Funktionswechsel überprüfen – so verhindern Sie, dass beispielsweise ehemalige Mitarbeitende aufs Netzwerk zugreifen.

4. Intelligente Passwörter verwenden, die zum Beispiel Sonderzeichen enthalten, Zahlen und Buchstaben kombinieren, mindestens acht Zeichen haben und in denen der eigene Name nicht vorkommt. Verwenden Sie Passwörter nicht mehrfach, wechseln Sie diese regelmässig und teilen Sie Ihre Passwörter nicht mit Dritten.

5. Stellen Sie sicher, dass auch Fernzugänge gut geschützt sind und mit einer Multifaktor-Authentisierungslösung gepaart werden. Sinnvoll ist es auch, externe Zugriffe zeitlich und räumlich zu begrenzen, z.B. nur von bestimmten IP-Adressen aus und zu gewissen Zeiten (z.B. Wartungsfenster).

6. Das Betriebssystem auf dem aktuellsten Stand halten – weil Hacker auf Schwachstellen in der Software zugreifen. Dazu gehört auch, alte Betriebssysteme (z.B. Windows XP, Windows 7) zu beseitigen, weil sie keine Updates mehr erhalten. Sinnvoll ist ausserdem, ein Inventar aller Computer und Applikationen des Unternehmens anzulegen, um eine Übersicht über alle IT-Systeme im Einsatz zu behalten.

7. Antivirenprogramme installieren, die Schadsoftware erkennen und blockieren, sowie eine Firewall nutzen, die nicht erlaubte Zugriffe verhindert. Die Programme sollten täglich auf den aktuellsten Stand gebracht werden.

8. Nehmen Sie regelmässige Daten-Backups vor, je nach Wichtigkeit täglich oder gar noch häufiger. Das neueste Backup sollte nicht das vorherige überschreiben, weil sonst die historischen Daten verloren gehen können. Banal, aber wichtig: Eine Kopie des Backups sollte stets vom Netz genommen werden, damit es einem Angreifer im Ereignisfall nicht auch zum Opfer fällt. Und man muss regelmässig testen, ob die Datensicherung funktioniert hat.

Wappnen Sie sich und reduzieren Sie Ihre Risiken

Möchten Sie sich detaillierter darüber informieren, wie Sie die Cyberrisiken Ihres Unternehmens minimieren können? Dann empfehlen wir Ihnen folgende weiterführende Informationen:

Mit der digitalen Plattform **Zurich Risk Advisor** können Sie eine Selbst-Einschätzung ihrer Cyberrisiken vornehmen. Die Einschätzung umfasst fünf Module und gibt Ihnen konkrete Verbesserungsvorschläge. Informieren Sie sich auf unserer Website (auf Englisch) und laden Sie die App herunter: **Link**

Das **Nationale Zentrum für Cybersicherheit (NCSC)** ist das Kompetenzzentrum des Bundes für Cybersicherheit. Das Ziel dieser Behörde ist der Schutz der Schweiz vor Cyberrisiken. Auf der Informationsseite für Unternehmen warnt das NCSC vor aktuellen Gefahren und gibt einen umfassenden Überblick, wie sich Unternehmen vor Cyberrisiken schützen können: **Link**

Auch der Dachverband der **ICT Wirtschaft** in der Schweiz, ICT Switzerland, möchte Schweizer KMUs dabei unterstützen, Cyberrisiken zu minimieren und hat dazu einen Leitfaden erstellt: **Link**

Das Versicherungskonzept von Zurich

1 Prävention

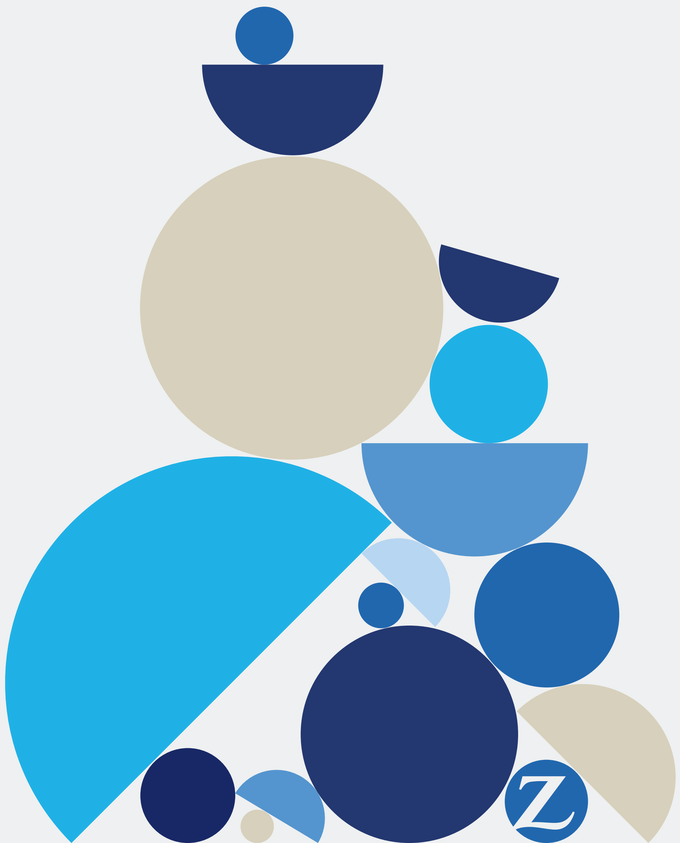
Das Zurich-Cyberversicherungskonzept hilft Ihnen dabei, Ihre Risiken zu verstehen und sich gegen Cyber-Attacken zu schützen.

2 Schutz vor finanziellen Risiken

Unsere modularen Deckungsbausteine bieten Ihnen genau die passende Versicherungslösung.

3 Schaden-management

Eine schnelle und adäquate Intervention im Ernstfall ist ausschlaggebend für den Erfolg der Massnahmen.



Das Versicherungskonzept von Zurich

1. Prävention 2. Schutz vor finanziellen Risiken 3. Schadenmanagement

Das Zurich-Cyberversicherungskonzept hilft Ihnen dabei, Ihre Risiken zu verstehen und sich gegen Cyber-Attacken zu schützen. Zusammen mit unserem Partner unterstützen wir Sie dabei, Cyberrisiken für Ihren Betrieb zu minimieren.

Sensibilisierungstraining – damit Mitarbeitende nicht zu Mittätern werden
Der Mensch ist beim Thema Cyber-Sicherheit das schwächste Glied. Bei allen Unternehmenstypen sind unerkannte Hacker-E-Mails das häufigste Einfallstor für gezielte Cyber-Angriffe. Genau hier setzt Zurich mit dem kostenlosen Cyber-Sicherheitstraining für Zurich Cyber-Kunden und deren Mitarbeitenden an. Das Online-Training wurde von unserer Partnerfirma SoSafe entwickelt – sie ist auf E-Learning und Cyber-Sicherheit spezialisiert. Die fünf E-Learning-Module und die Phishing-Simulation sensibilisieren die Mitarbeitenden für die Risiken im Internet und verhindern so, dass Mitarbeitende ungewollt zu Mittätern werden.

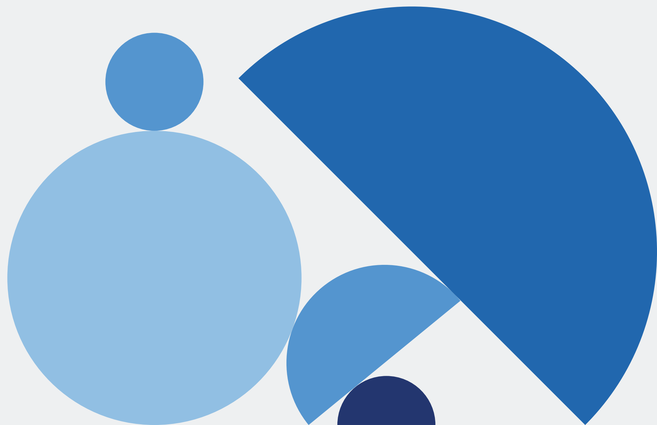
Risiko-Assessment
Zusammen mit Spie ICS, einem der führenden Dienstleister für Informations- und Kommunikationstechnologie in der Schweiz, hat Zurich einen Security-Check und ein Security-Assessment entwickelt. Die beiden Analysen sind darauf ausgerichtet, Ihre Cyber-Sicherheitsrisiken zu identifizieren, zu bewerten und umsetzbare Empfehlungen abzugeben. Durchgeführt werden sie von den Spie-Experten.

Security Check (1 Stunde Aufwand für Sie)
Die Analyse findet bei Ihnen vor Ort statt. Mit Tool-Unterstützung werden Ihre Systeme und Anwendungen auf Schwachstellen geprüft.
Sie erhalten einen Bericht, der die Dringlichkeit der Schwachstellen einschliesslich der Behebung/Mitigation erläutert.

Security Assessment (2 Stunden Aufwand für Sie)
Die umfassende Analyse der Sicherheitsprozesse und Kontrollen der Vertraulichkeit, Integrität und Verfügbarkeit der Systeme/Anwendungen wird bei Ihnen vor Ort durchgeführt. Dazu findet ein strukturiertes Interview mit Ihnen statt.

Sie erhalten einen detaillierten Bericht mit folgenden Inhalten:
– Zustand der Sicherheitskontrollen
– identifizierte Schwachstellen
– Empfehlungen zur Reduzierung von Risiken

Als Cyber-Kunde von Zurich profitieren Sie bei Spie ICS von Spezialkonditionen für die Durchführung eines Security Checks oder Security Assessments. Die Kosten berechnen sich anhand der Anzahl an Computer-Arbeitsplätzen: Der Security Check kostet ab 630 Schweizer Franken (bis zu 10 Arbeitsplätze), das Security Assessment erhalten Sie ab 1’600 Franken (bis zu 10 Arbeitsplätze).



Das Versicherungskonzept von Zurich

1. Prävention **2. Schutz vor finanziellen Risiken** 3. Schadenmanagement

Unsere modularen Deckungsbausteine bieten Ihnen genau die passende Versicherungslösung.

Auch ein solides Cyber-Sicherheitskonzept garantiert leider keinen absoluten Schutz vor Cyber-Attacken. Falls es dennoch zu einem Cyber-Vorfall kommt, bietet Zurich den optimalen Versicherungsschutz und unterstützt Sie beim Bewältigen der Folgen.

Wählen Sie das passende Paket für Ihr Unternehmen:

Basic ab CHF 410	Cyber-Daten- und Systemwiederherstellung Cyber-Krisenmanagement Cyber-Haftpflicht Cyber-Rechtsschutz
Optimum ab CHF 690	+ Cyber-Betriebsunterbruch
Premium ab CHF 845	+ Cyber-Crime

Das Versicherungskonzept von Zurich

1. Prävention **2. Schutz vor finanziellen Risiken** 3. Schadenmanagement

Cyber-Daten- und Systemwiederherstellung

- technische Abklärungen und IT-forensische Analysen: Was ist genau passiert?
- Wiederherstellung oder Wiederbeschaffung von Daten und Informationen
- Wiederbeschaffung von beschädigter Hardware (Bricking)
- Identifikation von Software-Schwachstellen und Massnahmen zur Sicherheitsverbesserung (Betterment)
- Cyber-Erpressungszahlungen und Kosten für die Abwehr von Cyber-Erpressungen
- Kostenübernahme bei Telefon-Hacking

Basic Optimum Premium

Cyber-Krisenmanagement

- Prüfung von Meldepflichten und Benachrichtigungspflichten
- Benachrichtigung von betroffenen Personen auf freiwilliger Basis
- behördliche Verfahren sowie (versicherbare) Strafen und Bussen
- Vertragsstrafen bei einem Verstoss gegen PCI DSS-Standards
- Call Center, Kreditkarten-Monitoring und Identity-Monitoring für betroffene Personen
- Goodwill-Aktionen wie beispielsweise Rabattaktionen und Preisnachlässe für betroffene Personen
- Planung und Umsetzung von Public Relations-Kampagnen bei negativer Medienberichterstattung

Basic Optimum Premium

Cyber-Haftpflicht

Schadenersatz und Abwehr von ungerechtfertigten Ansprüchen bei/im Zusammenhang mit:

- Verlust, Diebstahl oder Veröffentlichung von Daten – unabhängig von einem Cybervorfall
- Verletzung des Datenschutzrechts (inklusive GDPR)
- Verletzung von Namens-, Urheber- und Markenrechten
- Verfahrenskosten und Verteidigungskosten

Basic Optimum Premium

Cyber-Rechtsschutz

- Beratung zu juristischen Sofortmassnahmen
- Geltendmachung von Schadenersatzansprüchen
- Strafverteidigung bei fahrlässiger Verletzung von Datenschutzbestimmungen

Basic Optimum Premium

Cyber-Betriebsunterbruch und Mehrkosten

- aufgrund eines Cybervorfalls oder einer Fehlbedienung
- aufgrund einer behördlichen Anordnung infolge einer Datenschutzverletzung
- Deckung von Nettogewinnausfall sowie Mehrkosten zur Aufrechterhaltung des Betriebs

Optimum Premium

Cyber-Crime

- Cyber-Betrug aufgrund von aktiven Täuschungshandlungen durch Dritte (Social Engineering)
- Cyber-Diebstahl durch Manipulation der Computersysteme durch Dritte (E-Banking Hacking)

Premium

Das Versicherungskonzept von Zurich

Eine schnelle und adäquate Intervention im Ernstfall ist ausschlaggebend für den Erfolg der Massnahmen.

Im Schadenfall muss es schnell gehen. Unsere Hotline erreichen Sie deshalb 24/7. Während der Bürozeiten kümmern sich unsere spezialisierten Mitarbeitenden für Cyberschäden um Ihren Fall. Ausserhalb der Bürozeiten wird Ihr Anruf direkt an unseren IT-Partner Compass Security weitergeleitet.

Je nach Bedarf organisieren wir für Sie die Experten. Dazu arbeiten wir ebenfalls mit dem IT-Security-Unternehmen Compass Security zusammen. Durch seine Erfahrung und Expertise ist unser Partner bestens dafür gerüstet, eine schnelle und nachhaltige Lösung für Ihren Cyber-Vorfall zu finden. Basierend auf der Ursachenanalyse werden Ihnen ausserdem Massnahmen für einen nachhaltigen Cyber-Schutz empfohlen. So können Sie Ihr Unternehmen in Zukunft umfassend schützen.

Wir helfen nicht nur bei IT-Problemen, sondern verfügen auch über die richtigen Partner, wenn es um rechtliche Themen geht, sei es bei der Prüfung der Informationspflicht, Abwehr von Schadenersatzansprüchen oder beim Stellen von Strafanzeigen. Ebenso kann die Reputation des Unternehmens schnell auf dem Spiel stehen. Deshalb organisieren wir im Fall der Fälle Spezialisten für die Kommunikation gegenüber externen Parteien und helfen Ihnen so, Ihr Image zu schützen.

Das Versicherungskonzept von Zurich

1. Prävention 2. Schutz vor finanziellen Risiken **3. Schadenmanagement**

Schadenprozess Cyber: Der Schadenfall ist der «Moment der Wahrheit» – getreu nach dem Versprechen «Wir sind für Sie da, wenn es darauf ankommt.»

Vertragsabschluss

Herzliche Gratulation zum Abschluss Ihrer Cyber-Versicherung von Zurich. Gerne stehen wir Ihnen bei Fragen zur Verfügung und bieten Ihnen ein kostenloses Sensibilisierungstraining für Ihre Mitarbeitenden sowie als optionalen Service ein Cyber Risk Assessment an.

Ereignis

Sie stellen Unregelmässigkeiten in Ihrem IT-System fest oder wurden Opfer einer Cyberattacke.

Meldung

Melden Sie uns das Ereignis unkompliziert 24 / 7 an:

044 629 10 40

zurich.ch/schadenmelden

Gerne klären wir gemeinsam mit Ihnen den Sachverhalt ab und besprechen das weitere Vorgehen.

Massnahme

Bei Bedarf vermittelt Zurich Ihnen einen IT-Spezialisten, der die Sofortmassnahmen einleitet und/oder die vollständige Behebung der Störung sicherstellt. Andernfalls können Sie Ihren eigenen IT-Partner für die Problemlösung beauftragen.

Abwicklung

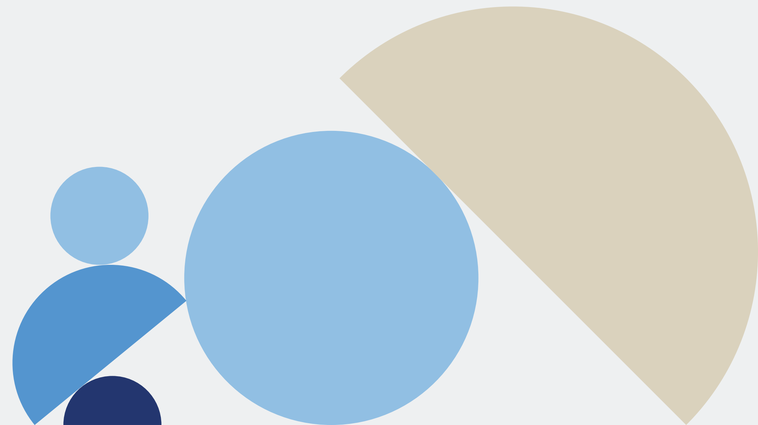
Zurich prüft den Analyse-Bericht des IT-Spezialisten. Zurich prüft die Entschädigung.

Erledigung

Wir besprechen mit Ihnen gemeinsam die Schadenerledigung. Sie erhalten mit der Erledigungsmeldung eine Kostenzusammenstellung und die Bestätigung der Schadenzahlung.

Nach-Schaden

Als optionalen Service können unsere IT-Spezialisten Ihnen Tipps für die Prävention geben.



Schadenbeispiel Arztpraxis (1/2)

Datendiebstahl in einer Arztpraxis durch einen Hackerangriff auf dessen IT-Dienstleister

1 Die Ausgangslage

Die **Arztpraxis** Arzt-Muster GmbH ist eine Praxisgemeinschaft von mehreren Kinderärzten.

Jahresumsatz: CHF 1’500’000
Anzahl Mitarbeitende: 6

Die **IT-Infrastruktur** (inklusive Patientenmanagementsystem) wird von einem IT-Dienstleister zur Verfügung gestellt. Die Mitarbeitenden verwenden Notebooks, welche mit dem Server vernetzt sind. Die Daten werden direkt auf dem Server abgespeichert.

2 Schadenszenario

Über einen gezielten Hackerangriff gegen den IT-Dienstleister der Arztpraxis Arzt-Muster GmbH erlangen unbefugte Personen Zugriff auf die Patientendaten. Die Ärztinnen und Ärzte sind im Ungewissen, welche Daten betroffen sind und welchen Schaden der Hacker damit verursachen kann.

3 So hilft Zurich

Paket Basic

Schadenmanagement

- Zurich informiert sich beim Versicherungsnehmer, ob sein IT-Dienstleister Unterstützung benötigt, um den Schaden zu beheben. Dieser ist bereits daran, den Vorfall aufzuklären sowie die IT-Infrastruktur wieder funktionsfähig zu machen. Bald stellt sich jedoch heraus, dass für die Einschätzung des Schadenausmasses Experten eingeschaltet werden müssen. Zurich organisiert zügig die nötige Unterstützung, um aufzuklären, welche Patientendaten vom Cyber-Vorfall betroffen sind.
- Durch ihren Partner bietet Zurich ausserdem den Ärztinnen und Ärzten eine kompetente Rechtsberatung zur Informationspflicht und Haftung. Gerade mit der geplanten Revision des Datenschutzgesetzes und der damit verbundenen erhöhten Rechtsrisiken aufgrund der strengeren Regulierung gewinnt die spezialisierte Expertise an Bedeutung.
- Als Teil des Schadenmanagements unterstützen Experten von Zurichs PR-Partner die Arztpraxis dabei, alle Personen angemessen zu informieren.

Schadenbeispiel Arztpraxis (2/2)

Schutz vor den finanziellen Risiken

- Baustein Cyber-Daten- und Systemwiederherstellung
  Der IT-Forensik-Partner von Zurich analysiert den Sachverhalt auf das Schadenausmass und überprüft, welche Daten und Patienten betroffen sind. Aufgrund der Analyse kann der IT-Experte abschätzen, welchen Schaden der Hacker mit den Daten verursachen kann. Falls die Daten nicht hinreichend geschützt waren, kann davon ausgegangen werden, dass der Hacker sie im Darknet zu Geld machen wird. Falls Daten und Systeme der Arztpraxis korrumpiert wurden, übernimmt Zurich die Kosten für die Wiederherstellung der Daten und der IT-Infrastruktur.

- Baustein Cyber-Rechtsschutz
  Es ist zu prüfen, inwiefern die betroffenen Patienten oder Behörden über den Diebstahl der Daten informiert werden müssen. Die Initialanalyse ist im Rechtsschutz versichert.

- Baustein Cyber-Haftpflicht
  Sollte sich in der rechtlichen Initialanalyse herausstellen, dass keine Rechtsverletzung vorliegt, wehrt Zurich unbegründete Haftpflichtansprüche ab. Falls die Personendaten nicht hinreichend geschützt wurden, besteht das Risiko, dass berechtigte Haftpflichtansprüche erhoben werden. In diesen Fällen leistet Zurich Schadenersatz

- Baustein Cyber-Krisenmanagement
  Basierend auf den Erkenntnissen der Schadenanalyse wird eine angemessene Kommunikationsstrategie entwickelt. Die Kosten für die Kommunikation übernimmt Zurich. Sollte sich in der rechtlichen Initialanalyse herausstellen, dass eine Rechtsverletzung vorliegt, sind auch die Kosten im Zusammenhang mit der Kommunikation gegenüber den Behörden versichert.

- Übersicht der versicherten Kosten in diesem Beispiel:
  Kosten für IT-Forensik und Kommunikationsberater sowie eventuell weitere Kosten für Rechtsberatung/Rechtsstreit abhängig von der Sachlage (Abzug von Selbstbehalt je nach Vereinbarung vorbehalten)

Schadenbeispiel Hersteller (1/2)

Produktionsstillstand bei einem Hersteller von Metallteilen durch einen Fernzugriff

1 Die Ausgangslage

Der **Hersteller** Metallteile-Muster AG bietet ein universelles Angebot an Metallteilen und schnelle Lieferfristen.

Jahresumsatz: CHF 3’000’000
Anzahl Mitarbeitende: 15

Die komplette **IT-Infrastruktur** befindet sich auf dem Gelände; neben dem Firmennetzwerk aus der Administration verfügt die Firma über ein Netzwerk für die Produktionsmaschinen. Diese sind für den Fernzugriff über das Internet freigeschaltet, damit der Hersteller die Wartung der Maschinen rund um die Uhr gewährleisten kann.

2 Schadenszenario

Ein Hacker hat sich am Sonntag durch ein gestohlenes Passwort aus der Ferne Zugriff auf das firmeninterne Netzwerk verschafft. Er blockiert die gesamte IT-Infrastruktur und legt damit alle Produktionsmaschinen still. Folglich hat die Firma während 5 Tagen keine Möglichkeit, Metallteile zu produzieren. Während der lokale IT-Dienstleister in Zusammenarbeit mit dem Maschinenhersteller versucht, das Netzwerk vom Virus zu befreien und die Produktionsmaschinen wieder zu starten, erhält der Unternehmer einen Anruf von einem wichtigen Kunden. Dieser möchte einen dringenden Auftrag mit einem Volumen von CHF 80’000 CHF und Fertigstellungsdatum innert 7 Tagen erteilen. Da der Auftrag nicht verschoben werden kann, muss der Unternehmer aufgrund des Cybervorfalls absagen. Zudem muss ein bereits bestehender Auftrag in den nächsten 10 Tagen fertiggestellt werden. Um dies zu gewährleisten, müssen alle Mitarbeitenden der Produktion am Wochenende zusätzlich arbeiten.

Da der IT-Dienstleister der Firma die für die Schadenanalyse und -behebung notwendigen Fähigkeiten nicht selbst hat, braucht die Firma externe Unterstützung. Der Unternehmer fordert sogleich Hilfe bei Zurich an.

3 So hilft Zurich

Paket Optimum

Schadenmanagement
Die Schadenhotline für Cybervorfälle ist 24/7 erreichbar, sodass der Hersteller den Schaden noch am Sonntagabend bei Zurich melden kann. Während den Bürozeiten kümmern sich spezialisierte Mitarbeiter für Cyber-Schäden um die Vorfälle. Ausserhalb der Bürozeiten wird der Anruf direkt an unseren IT-Partner weitergeleitet, der sich dann sogleich um die Problemlösung kümmert. Nach dem Anruf stellt der Partner sogleich sicher, dass ein Incident-Response-Team beim Kunden vor Ort ist und sich um die Problemlösung kümmert.

Schadenbeispiel Hersteller (2/2)

Schutz vor den finanziellen Risiken

- Baustein Cyber-Daten- und Systemwiederherstellung
  Der Cybervorfall verursacht Kosten in Höhe von 4'000 Schweizer Franken für den lokalen IT-Dienstleister. Weitere 7’000 Schweizer Franken fallen für die Wartungsarbeiten des Maschinenherstellers aufgrund des Cyber-angriffs an. Die Kosten für die rasche Intervention des Incident-Response-Teams, um die IT-Infrastruktur wiederherzustellen sowie die Schwachstelle zu beseitigen, belaufen sich auf 13’000 Schweizer Franken.

- Baustein Cyber-Betriebsunterbruch
  Die im Firmennetzwerk eingespeiste Schadsoftware blockiert den Zugriff auf die Produktionsmaschinen während fünf Tagen. Aufgrund des Auftrages, der nicht angenommen werden konnte, beläuft sich der entgangene Umsatz auf 60'000 Schweizer Franken (80'000 Franken für den Auftrag abzüglich 20'000 Franken für eingesparte Kosten wie z.B. Rohmaterial, Strom, etc.). Ebenfalls gedeckt ist der Mehraufwand für den zweiten Auftrag, welcher nur dank der Mehrarbeit am Wochenende ausgeführt werden konnte. Zusätzliche 5'000 Schweizer Franken wurden dem Produktionspersonal für die Sonderschichten ausbezahlt.

- Übersicht der versicherten Kosten in diesem Beispiel:
  CHF 89’000 (Abzug von Selbstbehalt je nach Vereinbarung vorbehalten)

Schadenbeispiel Treuhänder (1/2)

Diebstahl von Kundenkonten einer Treuhandfirma durch eine Phishing-Attacke

1 Die Ausgangslage

Die **Treuhandfirma** Treuhand-Muster AG führt im Auftrag ihrer Kunden Zahlungen aus.

Jahresumsatz: CHF 6’500’000
Anzahl Mitarbeitende: 22

Die **IT-Infrastruktur** wird von einem IT-Dienstleister zur Verfügung gestellt. Die Mitarbeitenden verwenden Notebooks, welche sich mit dem Server in Verbindung setzen. Die Daten werden direkt auf dem Server abgespeichert.

2 Schadenszenario

Ein Mitarbeitender wird Opfer einer Phishingattacke. Er erhält eine angebliche Spontan-Bewerbung und klickt deren Anhang an, das vorgebliche Bewerbungsdossier. So lädt er unabsichtlich eine Schadsoftware auf das Endgerät. Mit dieser Software kann der Hacker beim Einloggen der Mitarbeitenden ins E-Banking-Portal die Kontrolle übernehmen und Gelder von den Bankkonten der Kunden abzweigen.

3 So hilft Zurich

Paket Premium

Schadenmanagement
Nachdem der Treuhänder den Schaden bei Zurich gemeldet hat, nehmen die Zurich-Cyberspezialisten sofort Kontakt mit dem IT-Dienstleister der Firma auf. Ausserdem unterstützen sie den Treuhänder bei der Kommunikation mit den Behörden. Der IT-Dienstleister hat die Situation relativ schnell unter Kontrolle und kann innerhalb von drei Arbeitstagen die Systeme von der Schadsoftware bereinigen. Um sicherzustellen, dass der Hacker keinen Zugriff mehr auf die Systeme hat, bietet Zurich zusätzlich die IT-Forensiker der Zurich-Partnerfirma auf. Sie überprüfen sämtliche Systeme auf Spuren des Angriffs. Die Analyse ergibt, dass der Hacker keinen weiteren Zugriff mehr hat und keine Kundendaten gestohlen wurden.

Schadenbeispiel Treuhänder (2/2)

Schutz vor den finanziellen Risiken

- Baustein Cyber-Daten- und Systemwiederherstellung
  Die Kosten für die Bereinigung der Systeme und Behebung der Schwachstelle belaufen sich auf 12'000 Schweizer Franken (Kosten für den IT-Dienstleister sowie die IT-Forensiker).

- Baustein Cyber-Krisenmanagement
  Zurich und deren Partner unterstützen den Kunden bei der Kommunikation gegenüber den Behörden.

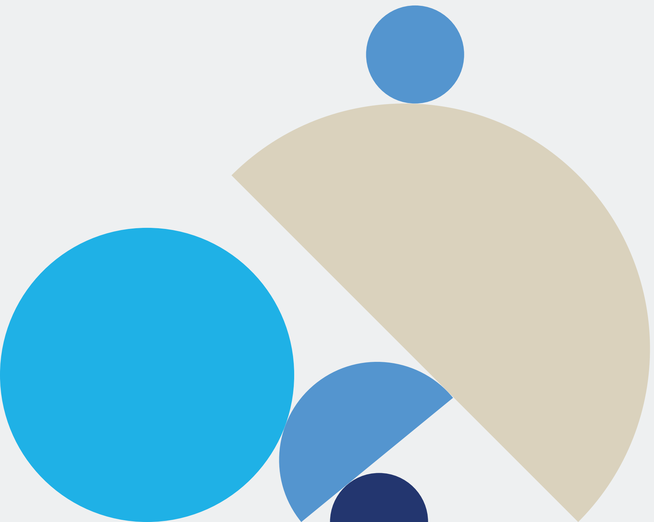
- Baustein Cyber-Crime
  Den Kunden vom Treuhandbüro wurden insgesamt 130’000 Schweizer Franken gestohlen, aus einem vom Versicherten verwalteten Konto. Dem Treuhänder fällt ein Stein vom Herzen, als er feststellt, dass der Schaden seine Versicherungssumme nicht überschreitet.

- Übersicht der versicherten Kosten in diesem Beispiel:
  CHF 142’000 (Abzug von Selbstbehalt je nach Vereinbarung vorbehalten)

Zurich Cyberversicherung

Kontakt und Vorteile

Die Digitalisierung bietet Unternehmen viele Wachstumsmöglichkeiten. Mit Zurich sind Sie bestens aufgestellt, um dieses Potenzial zu nutzen – dank präventiven Massnahmen, einer umfassenden Absicherung der finanziellen Risiken sowie einem kompetenten Schadenmanagement.



Für mehr Informationen zur **Zurich Cyberversicherung** besuchen Sie **unsere Website.** Gerne beraten wir Sie persönlich und individuell.

Kontaktieren Sie einfach Ihre nächste Zurich-Agentur,
Rufen Sie uns kostenlos an unter **0800 80 80 80** oder nehmen Sie direkt Kontakt auf mit Ihrem Makler/Broker.

Vorteile der Zurich Cyberversicherung

- Wir unterstützen Sie dabei, Ihre Firma gegen Cyberrisiken zu schützen – mit einem kostenlosen Sensibilisierungstraining für Ihre Mitarbeitenden sowie einem detaillierten Risiko-Assessment durch unsere Partnerfirma Spie mit Vorzugskonditionen für Zurich-Kunden.
- Die Deckungen sind klar und einfach beschrieben. So wissen Sie zu jedem Zeitpunkt, was versichert ist und was nicht.
- Die umfassenden Zusatzdeckungen berücksichtigen branchenspezifische Bedürfnisse und auch neue Risiken.
  Durch unsere Zurich-Spezialisten sowie unser professionelles Partnernetzwerk kann Ihnen Zurich im Schadenfall kompetent zur Seite stehen und dennoch haben Sie freie Dienstleisterwahl.
- Wir kümmern uns nicht nur um die Behebung des Vorfalls, sondern untersuchen die Ursachen und helfen Ihnen, die Schwachstelle auch für die Zukunft zu beseitigen.
- Das Angebot wurde für mittlere wie auch für kleine Unternehmen konzipiert.