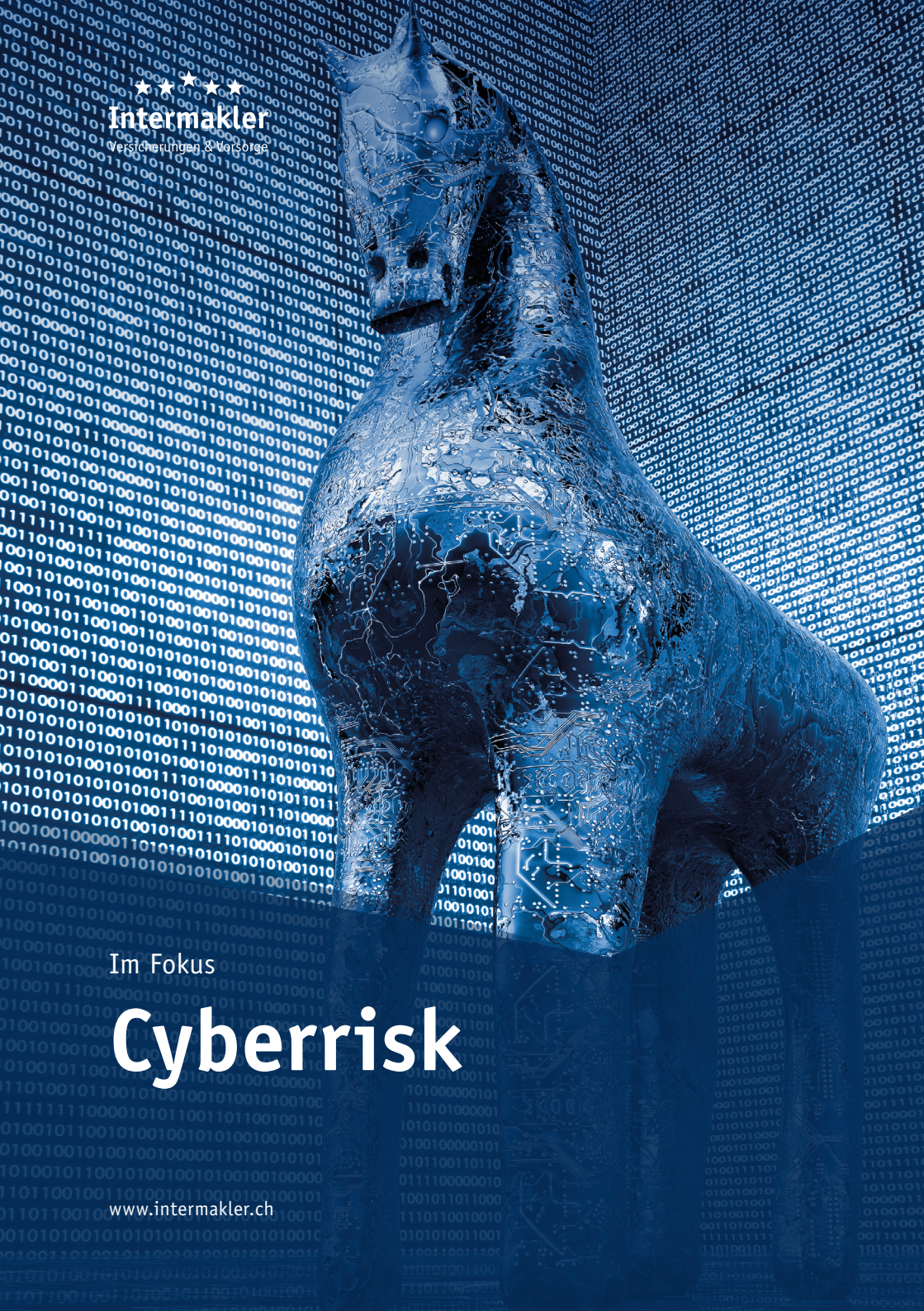

Intermakler
Versicherungen & Vorsorge
Im Fokus
Cyberrisk
www.intermakler.ch

Die Digitalisierung von betrieblichen Prozessen schreitet voran. «Cyber» hat als Eintrittstor in Organisationen die Verwundbarkeit von Unternehmen erhöht.

Kriminelle Aktivitäten basierend auf Cyber-Technologien zielen darauf ab, die Infrastruktur und die Daten einer Organisation anzugreifen, woraus insbesondere finanzielle Schäden entstehen, aber ebenso ein schwerwiegender Reputationsverlust und negative Auswirkungen auf die Kunden und Dienstleistungen resultieren können.

Mobilität

Gesundheit & Alter

Politik & Ökonomie

Infrastruktur

Reputation

Kunden & Lieferanten

Produkte & Dienstleistungen

Finanzen

Mitarbeitende

Natur & Umwelt

Technologie

Kriminalität

Die Achillesferse des 21. Jahrhunderts

Cyberrisiken zählen zu den momentan grössten sowie unberechenbarsten Risiken und Bedrohungen für Unternehmen.

95%
aller Cyber-Sicherheitsverletzungen werden durch menschliches Fehlverhalten verursacht.
Quelle: Cybint

207
Tage dauert es durchschnittlich, um einen Cybervorfall zu entdecken.
Quelle: IBM

37%
aller schädlichen Mail-Anhänge sind Word-Dokumente (.doc/.dot).
Quelle: Symantec

86%
aller Cyberangriffe sind finanziell motiviert.
Quelle: Verizon

> 300'000'000'000
Passwörter wurden im Jahr 2020 weltweit von Menschen und Maschinen verwendet.
Quelle: Cybersecurity Media

Kaum eine Woche vergeht, in der die Medien nicht über Hackerangriffe, Datenlecks oder die Gefahren der Cyberkriminalität berichten. Begriffe wie «DDoS», «Phishing» und «Ransomware» haben Aufnahme in den üblichen Wortschatz der Wirtschaftspresse gefunden. Als Verständnishilfe haben wir für Sie einige der wichtigsten Cyberrisk-Begriffe in einem Glossar zusammengefasst und erklärt.

Botnet
Eine Gruppierung automatisierter Computerprogramme, die auf vernetzten Rechnern laufen («bot» =a Roboter, «net» = Netz). Der Roboter wird dabei unbemerkt auf fremden Geräten installiert und erlaubt es den Angreifern, Kontrolle über das Gerät zu erlangen. Alle Geräte zusammen funktionieren bei einem Angriff als «Botnet». Unter anderem werden DDoS-Attacken über solche Botnets durchgeführt.

Brute-Force-Attacke
Ein Cyberangriff, bei dem leistungsfähige Computer und Software genutzt werden, um die bestehenden Sicherheitsmassnahmen

mit einer hohen Angriffsgeschwindigkeit und -häufigkeit zu überwältigen. Von einer Brute-Force-Attacke spricht man beispielsweise, wenn ein Passwort mittels eines Algorithmus, der sämtliche möglichen Kombinationen versucht, erraten wird.

Datenleck / Data breach
Ist der Fall, wenn Daten von einem Computersystem gestohlen wurden (z.B. Kundendaten, Login- oder Zahlungsinformationen).

DDoS(-Attacke)
Steht für «Distributed Denial of Service» (= Verweigerung des Dienstes). Ein Cyberangriff, der darauf ausgelegt ist, auf einem Server durch Überlastung einen Ausfall zu verursachen. Der Angriff erfolgt von vielen verteilten Rechnern aus. Diese befeuern das angegriffene System mit Anfragen und führen so zur Überlastung.

DNS-Attacke
Der DNS-Eintrag («Domain Name System») einer Webseite definiert, auf welche IP-Adresse der Benutzer beim Eingeben einer URL (z.B. www.intermakler.ch) geleitet wird. Bei einer DNS-Attacke wird dieser Eintrag geändert und der Datenverkehr auf eine andere IP-Adresse respektive Webseite umgeleitet.

Exploit
Von einem «Exploit» spricht man, wenn die Schwachstelle einer Software ausgenutzt wird («exploit» = ausnutzen). Die Angreifer nutzen Sicherheitslücken im Programmiercode, um Zugriff auf das Computersystem zu erlangen.

Firewall
Hardware oder Software, die vor Cyberangriffen schützen soll.

Malware
Überbegriff für verschiedene Formen von schädlicher Software, die darauf programmiert sind auf dem angegriffenen System oder Gerät einen Schaden anzurichten.

Phishing
Eine illegale Methode, bei der persönliche Daten (z.B. Kreditkarten, Logindaten) über gefälschte Webseiten, E-Mails oder Kurznachrichten erlangt und anschliessend auf kriminelle Weise missbraucht werden.

Ransomware
Schädliche Software (Malware), die auf einem Gerät eingeschleust wurde und die darauf gespeicherten Daten verschlüsselt oder blockiert. Zur Freigabe oder Entschlüsselung fordern die Angreifer eine Lösegeldzahlung («ransom» = Lösegeld).

Spyware
Schädliche Software (Malware), die bei aktiver Internetverbindung Informationen über den Benutzer und dessen Aktivitäten (z.B. Besuch von Webseiten) aufzeichnet. Im Gegensatz zu einem Virus verbleibt die Spyware jedoch auf dem Gerät und hat nicht das Ziel, sich weiterzuverbreiten.

Trojanisches Pferd
Schädliche Software (Malware), die es dem Hacker erlaubt, Zugriff auf ein am Internet angeschlossenes Gerät zu erlangen.

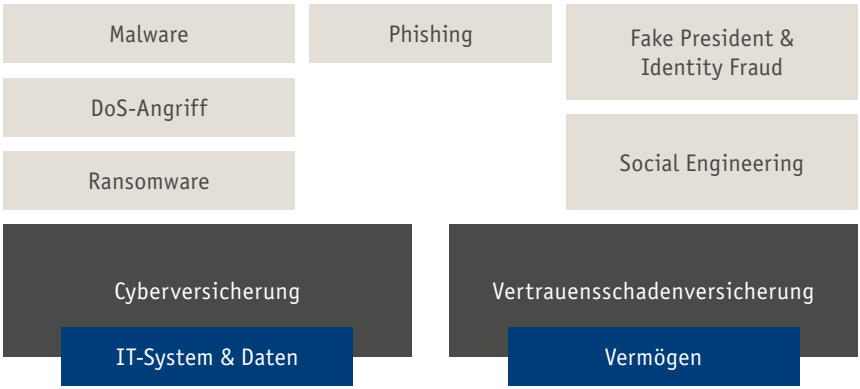
Virus
Schädliche Software (Malware), die auf einem Gerät eingeschleust wurde und dort ohne Wissen des Benutzers läuft, mit dem Ziel Schaden anzurichten.

Worm / Wurm
Schädliche Software (Malware), die sich selbst repliziert und so andere Geräte im gleichen Netzwerk infiltriert.

Dieses Glossar umfasst ausgewählte Begriffe rund um das Thema Cyberrisk. Die Begriffe werden zur besseren Verständlichkeit vereinfacht erklärt.

Cyberrisiken: Gefahren und Versicherungen

Der Verlust von wichtigen Daten, ein Betriebsunterbruch aufgrund blockierter IT-Systeme, Lösegeldforderungen, hohe Wiederherstellungskosten sowie ein Vermögensdiebstahl aufgrund eines unerlaubten Zugriffs auf das Zahlungssystem: Diese Schadenszenarien wecken bei Unternehmen oft die grössten Befürchtungen hinsichtlich Cyberrisiken. Aus versicherungstechnischer Sicht gilt es dabei zwischen zwei Versicherungen zu unterscheiden.



Wichtigste Deckung (Beispiele):

- ✓ Systemwiederherstellung & Datenrekonstruktion
- ✓ Ertragsausfall bei Betriebsunterbruch
- ✓ Ansprüche aufgrund von Datenschutzverletzungen und Schadenersatz

Wichtigste Deckung (Beispiele):

- ✓ Vermögensverlust infolge Betrug oder Diebstahl durch Vertrauenspersonen oder Hacker
- ✓ Vermögensverlust infolge von Social-Engineering-Angriffe von Dritten

Die marktüblichen Cyberversicherungen decken in erster Linie Schäden an den IT-Systemen sowie den Daten eines Unternehmens, welche durch Hackerangriffe oder Schadsoftware (Malware) entstehen. Ebenso sind Ertragsausfälle, die aus einem allfälligen Betriebsunterbruch resultieren, sowie Haftungsansprüche (z.B. aufgrund einer Datenschutzverletzung) eingeschlosseneingeschlossen. Sofern benötigt, können gegen eine zusätzliche Prämie auch Lösegeldzahlungen mitversichert werden.

Cyberversicherung Schadenszenario (Beispiel):
Eine Ransomware ist auf unbekannte Weise auf den Firmenserver gelangt und verschlüsselt die gespeicherten Daten. Die Mitarbeitenden haben keinen Zugriff mehr auf betriebsnotwendige Dokumente. Eine Cyberversicherung deckt in diesem Fall die Wiederherstellungskosten sowie je nach Vertragsbedingungen und versicherten Bausteinen den entstandenen Ertragsausfall, Unterstützung im Krisenmanagement mit externen Experten sowie die Verhandlungskosten mit den Erpressern. Teurere Lösungen versichern im Notfall die Lösegeldzahlung.

Cyberversicherung Schadenszenario (Beispiel):
Ein Hacker erlangt Zugriff auf sensible Kundendaten und veröffentlicht diese im Internet. Eine Cyberversicherung deckt in diesem Fall allfällige Schadenersatzforderungen Dritter.

Mit einer Cyberversicherung sind dagegen in der Regel Vermögensschäden, die auf Diebstahl, Betrug oder Erpressung zurückzuführen sind (z.B. fehlgeleitete Zahlungen aufgrund vorgespielter Identität), nicht gedeckt. Dazu dient die Vertrauensschadenversicherung.

Vertrauensschadenversicherung Schadenszenario (Beispiel):
Der Mitarbeiter eines Industriebetriebs, der für die Finanzen des Unternehmens zuständig ist, erhält eine E-Mail des Inhabers mit der Anweisung eine mittelgrosse Geldsumme auf ein Bankkonto in China zu überweisen. Der Inhaber weilt zu dieser Zeit tatsächlich in China und hat bereits in der Vergangenheit Zahlungsanweisungen per E-Mail gesendet. Der Mitarbeiter überweist den Geldbetrag. Erst nachdem der Inhaber die Überweisung in den Finanzunterlagen entdeckt, fliegt der Schwindel auf. Die E-Mail war gefälscht. Die Vermögensschadenversicherung deckt in diesem Fall den finanziellen Schaden.

Zwischen den beiden Versicherungen bestehen Überschneidungen, beispielsweise hinsichtlich Phishing, bei dem persönliche Daten (z.B. Kreditkarten, Logindaten) über gefälschte Webseiten, E-Mails oder Kurznachrichten erlangt und anschliessend auf kriminelle Weise missbraucht werden. Dieser Fall kann sowohl durch eine Cyber- oder eine Vertrauensschadenversicherung gedeckt sein. Es empfiehlt sich daher, bei einer Versicherungsstrategie für Cyberrisken die nötigen Deckungen genau zu analysieren und beispielsweise eine Cyberversicherung um Zusatzversicherungen aus dem Bereich der Vertrauensschadenversicherung zu ergänzen. Bei hohen Vermögensverlustrisiken ist eine zusätzliche Vertrauensschaden-/Cybercrimeversicherung prüfenswert.

Evaluationsmodell Cyberversicherung

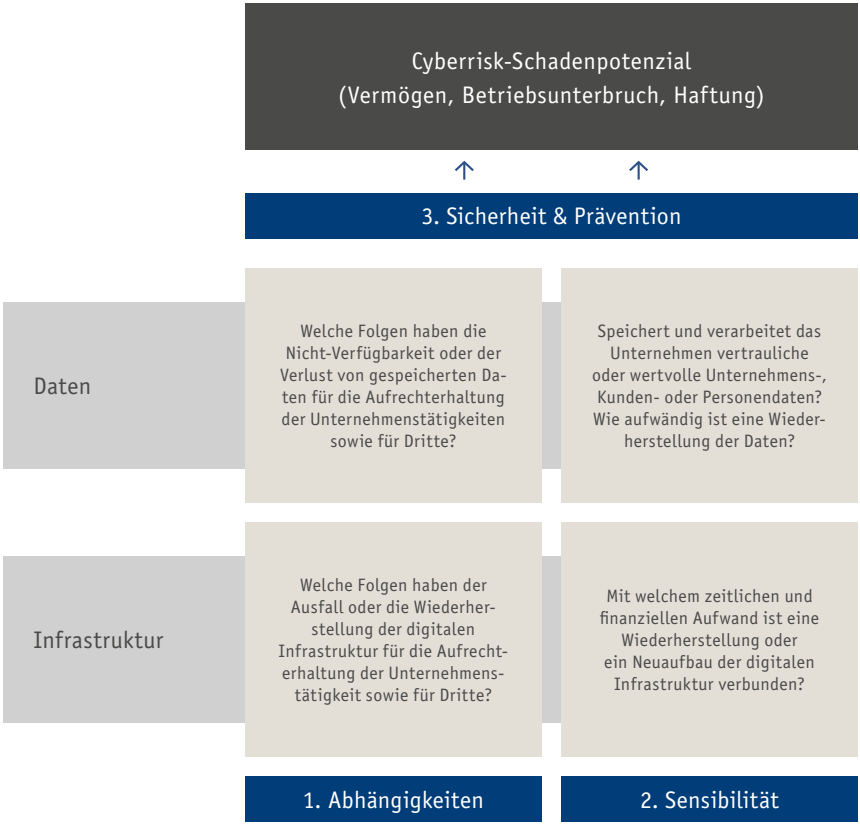
Inwiefern sich ein Unternehmen gegen Cybergefahren versichern sollte, ist abhängig von der Risikofähigkeit und -einstellung sowie insbesondere vom potenziellen Schadenausmass, dem «Cyberrisk-Schadenpotenzial».

Das Intermakler-Evaluationsmodell erlaubt eine Beurteilung des Cyberrisk-Schadenpotenzials aufgrund der drei Faktoren «Abhängigkeiten», «Sensibilität» sowie «Sicherheit & Prävention».

1. Zur Ermittlung des Cyberrisk-Schadenpotenzials gilt es in einem ersten Schritt zu eruieren, wie stark der Betrieb von der Blockierung oder dem Verlust der Infrastruktur (IT-System) oder der gespeicherten Daten betroffen wäre. Eine grosse Abhängigkeit erhöht die Gefahr eines Betriebsunterbruchs und der damit einhergehenden Ertragsausfälle.

2. Weiter gilt es zu prüfen, mit welcher Komplexität die Infrastruktur und die gespeicherten Daten verbunden sind. Hier sind insbesondere die Aufwände zur Wiederherstellung relevant sowie die Sensibilität der gespeicherten Daten (z.B. vertrauliche Personendaten) hinsichtlich allfälliger Haftungsansprüche.

3. Die Präventions- und Sicherheitsmassnahmen zum Schutz der IT-Systeme und Daten sind auf die ermittelten Abhängigkeiten und die Sensibilität aus- und einzurichten. Je nach erzieltem Sicherheitsgrad sowie verbleibenden Anfälligkeiten verringert sich das Cyberrisk-Schadenpotenzial. Die IT-Sicherheit kann in diesem Sinn als ein Filter verstanden werden, der möglichst viele Risiken reduziert.



Das Cyberrisk-Schadenpotenzial kann aufgrund der drei Elemente «Abhängigkeiten», «Sensibilität» sowie «Sicherheit & Prävention» beurteilt und mit der Risikofähigkeit und -einstellung des Unternehmens abgeglichen werden, um den Bedarf einer Cyberversicherung zu eruieren.

Kommentar: Schritt halten mit der Digitalisierung

Im Umgang mit Cyberrisiken sind drei Dinge gefragt: Kompetenz, Verantwortung und Differenzierung.

Für Unternehmen ist das Risiko, Opfer eines Cyberangriffs zu werden oder finanziell weitreichende Schäden durch Cyberrisiken zu erleiden, stark gestiegen. Nicht nur für Grosskonzerne, sondern auch für KMU. Unternehmer und Führungspersonen müssen daher den richtigen Umgang mit dem Risiko «Cyber» erlernen.

Kompetenz

Es scheint selbstverständlich, sich über aktuelle Entwicklungen in der Politik oder auf den Finanzmärkten auf dem Laufenden zu halten und daraus die richtigen Schlüsse für das eigene Unternehmen zu ziehen. Aufgrund der immensen Bedeutung der Digitalisierung in Gesellschaft und Wirtschaft zählen digitale Kompetenzen heute zu den unbestrittenen Anforderungen an eine Firmenleitung. Dazu zählt auch, sich grundlegendes Wissen und Basisfähigkeiten zu Cyberrisiken anzueignen.

Verantwortung

Die Herausforderungen hinsichtlich der Digitalisierung, respektive ihrer Risiken, delegiert man, zum Beispiel als Geschäftsführer oder CFO, an die internen oder externen IT-Zuständigen. Durchaus zu Recht, denn die Komplexität und rasend schnelle Entwicklung der Systeme erfordert sehr viel Fachwissen. Dies entlässt die Unternehmensführung aber nicht aus der Verantwortung. Denn aufgrund ihrer Bedeutung und ihres Schadenpotenzials gehören Cyberrisiken auf die Management-Agenda, unter fachkundiger Beratung und Mitarbeit von Experten. Die Ermittlung des Cyberrisk-Schadenpotenzials und daraus abgeleitet die Eruierung von Investitionen in Sicherheit und Prävention sowie Versicherungen sind aufgrund der Risikoentwicklung unerlässlich.

Differenzierung

Zu guter Letzt gilt es bei einem so weitreichenden Themengebiet zu lernen, welche Gefahren für das eigene Unternehmen relevant sind, respektive wie gross das Cyberrisk-Schadenpotenzial tatsächlich ist. Denn nur weil Schlagzeilen über Hackerangriffe für Aufmerksamkeit sorgen oder die Schadenfälle aufgrund von Cyberrisiken ansteigen, heisst dies nicht, dass man sämtliche Ressourcen in die Abwehr von Cyberangriffen investieren muss, respektive andere Risiken an Bedeutung verloren haben. Im Risk Management ist die Einschätzung der unterschiedlichen Risiken bezogen auf das spezifische Umfeld und Tätigkeitsgebiet des Unternehmens entscheidend. Auch bei Cyberrisiken ist daher eine differenzierte und analytische Betrachtungsweise notwendig.

Lesen Sie Fachartikel und Neuigkeiten der Versicherungs- und Vorsorgebranche auf unserer Webseite www.intermakler.ch

Intermakler AG, Giacomettistrasse 1, CH-3006 Bern
T +41 31 350 55 05, info@intermakler.ch, www.intermakler.ch