Cyberrisiken aktiv managen

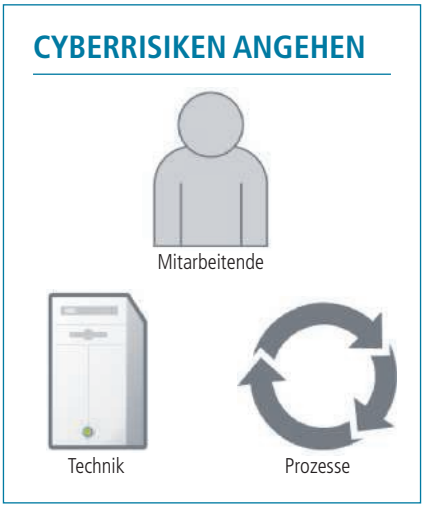
Know-how Die Gefahr, Opfer einer Cyberattacke zu werden, steigt unaufhörlich. Ebenso der Bedarf, sich als Unternehmen davor zu schützen. Einem umfassenden und weitsichtigen Risikomanagement kommt eine Schlüsselrolle zu, um den Gefahren zu begegnen.

Von Carlos Casián, Carlo Pugnetti, Albena Björck

So verlockend das Versprechen der digitalen Welt auf Vereinfachung, Effizienzsteigerung oder auf bessere Gesundheit auch ist, so real sind die Gefahren, die sich daraus ergeben. Jedes Gerät, jede Schnittstelle, jeder Benutzende von Informationstechnologie stellt in unserem vernetzten Alltag eine mögliche Schwachstelle dar. Bis Ende 2022 sollen rund 75 Milliarden Geräte mit dem Internet of Things (IoT) verbunden sein – mit entsprechendem Risikopotential. Wird beispielsweise durch eine Cyberattacke die Stromzufuhr unterbrochen, können die eigenen vier Wände im Smart Home oder das Büro zum Gefängnis werden. Wird ein (teil-)autonomes Fahrzeug gehackt und von Kriminellen ferngesteuert, kann es zu einer unkontrollierbaren Waffe werden. Und auch ein moderner, technisch aufgerüsteter Herzschrittmacher kann manipuliert werden und unter Umständen Leben kosten. Diese Beispiele zeigen: Wir haben durch den digitalen Wandel eine gesellschaftliche Herausforderung erschaffen, die uns alle betrifft – und über deren Auswirkungen sich nur die Wenigsten im vollen Ausmass bewusst sind und aktiv angehen: Cyberrisiken.

Lukratives Geschäft für Cyberkriminelle

Für die einen ein unbekanntes Terrain, für die anderen ein lukratives Geschäft: Schätzungen zufolge verursachten Cyberkriminelle 2021 weltweit Schäden im Wert von 6 Billionen Dollar – bis 2025 sollen es jährlich mehr als 10 Billionen Dollar sein. Eine schier unfassbare Zahl. Zwei Hauptmotive stehen bei den Angriffen im Fokus. Zum einen geheime und wertvolle Informationen sammeln. Hier sprechen wir in der Regel von staatlich gesponserten Angriffen und Spionage. Sind die Angreifer motiviert genug und verfügen über ausreichende Ressourcen und Zeit, ist kein Ziel vor ihnen sicher. Das andere Hauptmotiv ist, möglichst effizient Geld zu beschaffen. Letzteres ist das Hauptrisiko für die meisten Unternehmen und manifestiert sich vorwiegend als Ransomware-Angriff. Der Mechanismus ist einfach: Das IT-System und sämtliche Daten eines Unternehmens werden verschlüsselt, um im Anschluss Lösegeld für die Freigabe zu fordern. Allein das ist für Unternehmen schon zeit- und kostenintensiv. Cyberkriminelle geben sich mit der Lösegeldforderung für die verschlüsselten Daten jedoch nicht mehr zufrieden, denn sie haben festgestellt, dass in den Firmen vermehrt gute Backuplösungen vorhanden sind. Deshalb wird zunehmend ein zweiter und dritter Erpressungsgrund beobachtet: zunächst drohen sie mit der Veröffentlichung von sensiblen (Kunden-)Daten und danach mit einem Cyberangriff auf die Kunden des betroffenen Unternehmens. Das ist dann für viele der Super-GAU. Aber es zeigt: Es kann uns alle treffen – immer und überall.



Cyberrisiken sind kein reines IT-Thema. Durch eine interdisziplinäre Zusammenarbeit vermindern Unternehmen die eigenen Risiken und bereiten sich auf einen Cyberangriff vor. Quelle: Allianz Suisse

Risiken im Unternehmen managen

Diese besorgniserregende Entwicklung zusammen mit der zunehmenden Abhängigkeit von der IT-Infrastruktur stellt Unternehmen vor grosse Herausforderungen. Verschiedene Studien wie der Allianz Risk Barometer (siehe auch Seite 32ff) zeigen, dass Cyberrisiken zu den wichtigsten Geschäftsrisiken gehören und deshalb mit hoher Priorität im Rahmen des Risikomanagements angegangen werden müssen.

Unternehmen haben grundsätzlich vier Möglichkeiten, mit Risiken umzugehen. Sie können die Risiken:

1. meiden, das heisst nicht eingehen,
2. vermindern, das heisst die Wahrscheinlichkeit oder das Ausmass der möglichen Schäden reduzieren,
3. übertragen, das heisst an Dritte weitergeben oder
4. selbst tragen, das heisst das Risiko und die möglichen Konsequenzen akzeptieren.

Diese Optionen können auch kombiniert werden, indem ein Unternehmen das Risiko vermindert, einen Teil davon an einen Geschäftspartner überträgt und das Restrisiko bewusst eingeht.

Cyberrisiken können in unserer vernetzten Welt nur mit wenigen Ausnah-

men vollständig vermieden werden. Andererseits ist es problematisch, als Unternehmen die gesamten Risiken selbst zu tragen, denn die Auswirkungen können verheerend sein und im schlimmsten Fall die Existenz vernichten. Cyberrisiken zu vermindern ist für die meisten Unternehmen allerdings eine Herausforderung, weil die Technologie und die Risiken sich dynamisch entwickeln und in der Regel nicht zum Kern-Know-how eines Unternehmens gehören. Die Versuchung ist daher gross, das IT-Management auszulagern und die Risiken einer Versicherung zu übertragen. Ohne ein durchdachtes Risikomanagement kann dieser Ansatz jedoch nicht gelingen.

Aus zwei Gründen: Externe Dienstleister können die Risikoverminderung nicht optimieren und Versicherungen unverminderte Cyberrisiken nicht langfristig decken. Nur wer die Gesamtverantwortung für ein Unternehmen trägt, kann optimale Entscheidungen über die notwendigen Investitionen zur Risikoverminderung treffen. Dieser Entscheidungsprozess kann nicht vollständig ausgelagert werden, da externe Dienstleister die Folgen der Entscheidung nicht tragen müssen. Effizientes Risikomanagement ist zu grossen Teilen also Chefsache. Beim Outsourcing besteht zusätzlich die Gefahr von Risikokompensation, wobei die Verminderung eines Risikos das Verhalten in Bezug auf ein anderes Risiko beeinflussen kann. So hat zum Beispiel die Einführung des Antiblockiersystems (ABS) nicht zu einem Rückgang tödlicher Autounfälle geführt. Auf die IT übertragen: Beim IT-Outsourcing wird die technische Infrastruktur professionell(er) geschützt, dadurch erhöht sich jedoch das Risiko, dass sich Mitarbeitende in falscher Sicherheit wiegen und beispielsweise unvorsichtiger mit Phishing-Mails umgehen.

Zunehmende Schadenbelastung bei Versicherungen

Eine Versicherung ist wiederum ein hervorragender Mechanismus, um Schwankungen abzudecken und die Auswirkungen von unerwarteten Ereignissen für die Kunden abzufedern. Sie bündelt ähnliche Risiken und berechnet als Prämie den Durchschnitt der erwarteten Schadenskosten. Eine Versicherung ist übrigens ein guter Frühindikator für aufkommende oder sich rasch verändernde Risiken, weil überregionale Schadensmuster erkannt werden. Sie kann jedoch die notwendigen Investitionen in die Risikoverminderung nicht ersetzen, denn mit der zunehmenden Schadensbelastung durch unverminderte Risiken steigen die Versicherungsprämien. Diese Dynamik macht auch intuitiv Sinn: Bei einer Diebstahlversicherung haben wir als Kunden Sorgfaltspflichten. Wenn wir das Auto nicht abschliessen oder regelmässig wertvolle Gegenstände liegen lassen, wird die Schadensbelastung steigen. Die Prämie erhöht sich in der Folge, Schäden werden abgelehnt oder die Police gekündigt, wenn das Risiko nicht mehr tragbar ist. Cyberversicherungen sind in dieser Hinsicht keine Ausnahme. Die Anzahl an Cyberangriffen hat sich von 2020 auf 2021 verdoppelt. Die zunehmende Schadensbelastung in den letzten Jahren reflektiert diese Entwicklung: Bei Grossunternehmen beispielsweise haben sich die Prämien im Durchschnitt schätzungsweise um 30 bis 40 Prozent pro Jahr erhöht, und bis zu 80 Prozent der Unternehmen werden aktuell abgelehnt, weil sie die Mindestanforderungen an Cybersicherheitsvorkehrungen nicht erfüllen. Hier sind im Sinne der Risikominderung also auch die Unternehmen gefragt.

Investition in Cybersicherheit

Versicherungslösungen erlauben es Unternehmen, die Schwankungen zu glätten und ihre Risiken kontrollierbar zu machen. Sie sind aber kein Ersatz für umfassende und professionelle Massnahmen zur Sicherung der IT-Systeme. Damit Cyberversicherungen langfristig funktionieren und Unternehmen ein finanzielles Auffangnetz für den Super-GAU anbieten können, müssen Unternehmen ihre Cyberrisiken vermindern.

Der erste Schritt ist ausschlaggebend für den Erfolg oder Misserfolg der Cybersicherheit in einem Unternehmen: Verstehen, dass Cyberrisiken kein reines IT-Thema sind, sondern ein Geschäftsrisiko, das zuerst im Management als solches wahrgenommen werden muss. Der Ver-

RISIKOKOMMUNIKATION: RICHTIG UND ZIELGERICHTET KOMMUNIZIEREN

Den Mitarbeitenden kommt eine Schlüsselrolle bei der Cybersicherheit und im Falle eines Cyberangriffs zu. In der Studie «Cyberrisiken und Schweizer KMU» der ZHAW und der Allianz Suisse wurden die Einstellungen der Mitarbeitenden und ihre Anfälligkeiten hinsichtlich Cyberrisiken unter die Lupe genommen. Die Ergebnisse zeigten verschiedene Gründe, weshalb die Mitarbeitenden Teil des Problems sind, jedoch noch wichtiger, dass sie Teil der Lösung sein können und sein wollen. Um die Mitarbeitenden einzubinden und eine Risikokultur im Unternehmen zu schaffen, ist eine effektive Risikokommunikation zentral. Zu den zentralen Aufgaben gehört die Förderung des internen Risikodialogs, um das Vertrauen und Engagement der Mitarbeitenden zu stärken. Sie hilft bei der Vorbereitung auf den Umgang mit Risiken und später mit Krisen indem sie einen Lernprozess auf individueller Ebene auslöst.

Statistiken zeigen, dass menschliches Versagen den Weg für einen erfolgreichen Cyberangriff ebnen. Trotz der Schlüsselrolle der Mitarbeitenden bei der Entdeckung, der Vermeidung und dem Management von Cybergefahren bleibt die interne Risikokommunikation in Bezug auf Cyberrisiken ein schwieriges Thema:

1. Dynamische Technologieentwicklung und Gefahrenlage führen dazu, dass Informationen ständig aktualisiert werden müssen.
2. Cyberkriminalität ist abstrakt und anonym und kann deshalb nur schwer untersucht und erklärt werden.
3. Technische Begriffe erschweren das Verständnis und damit die Diskussion über Cyberrisiken in der Öffentlichkeit und im Unternehmen.

Ein Beispiel der Risikokommunikation ist die regelmässige Information über aktuelle Ereignisse, das Durchführen von Phishing-Simulationen zusammen mit der gemeinsamen Besprechung und Aufarbeitung der Erkenntnisse sowie die Weitergabe von Tipps an die Mitarbeitenden, wie Phishing-Mails erkannt werden können.

Die Cyber-Risikokommunikation steckt noch in den Kinderschuhen und ist Gegenstand der aktuellen Forschung. Die Autoren befassen sich mit den verschiedenen Elementen der Risikokommunikation, um den zielgerichteten und effizienten Risikodialog in Unternehmen voranzutreiben. Das Ziel ist es, ein Tool zu entwickeln, das es Unternehmen erlaubt, ihre Ausgangslage hinsichtlich Ressourcen, Kompetenzen und Prozessen zu evaluieren. Im Anschluss wird die Wahrnehmung der Mitarbeitenden erfasst und daraus Massnahmen abgeleitet, um eine Risikokultur zu etablieren, die das Unternehmen resilienter gegenüber Cyberangriffe macht.

CYBERVERSICHERUNGEN

Cyberversicherungen machen Cyberrisiken für Unternehmen kontrollierbar. Sie decken einerseits Eigenschäden des Unternehmens, zum Beispiel Kosten für die forensische Abklärungen, Wiederherstellungskosten und den Betriebsunterbruch nach einem Ransomware-Angriff. Andererseits Haftpflichtforderungen, wenn beispielsweise Kundendaten bei einem Angriff gelöscht werden oder gestohlen und veröffentlicht werden. Im Schadensfall unterstützen sie die Kunden mit ihrem Partnernetzwerk. Zudem können finanzielle Schäden infolge Täuschung durch einen Dritten wie der CEO-Betrug und Rechtsstreitigkeiten im Zusammenhang mit Cyberrisiken versichert werden.

such, die Verantwortung vollständig der IT-Abteilung oder sogar einem externen IT-Dienstleister zu übertragen, ist keine gute Idee. Denn die Frage steht im Raum, wer die Verantwortung trägt und sich nach aussen hin rechtfertigen muss, wenn Kundendaten gestohlen und veröffentlicht werden oder wenn der Betrieb unterbrochen wird und sich das Unternehmen im schlimmsten Fall nicht mehr erholen kann: die Geschäftsleitung.

Cybersicherheit ist ein essenzielles Werkzeug, das eine erfolgreiche und nachhaltige Geschäftsfortführung unterstützt. Werden die Risiken und die Verantwortung erkannt, ist der Grundstein gelegt, um die Cybersicherheit von einem reinen Kostenpunkt in eine Disziplin zu verwandeln, die strategisch angegangen, in die investiert und die aktiv weiterentwickelt werden kann.

Im zweiten Schritt geht es um die strategischen und operativen Massnahmen. Jedes Unternehmen ist einzigartig und damit auch ihre Risiken und Anfälligkeiten. Wo kommt überall IT zum Einsatz? Welche Daten verwalte ich und wie? Wie kann mein Betrieb durch einen Cyberangriff unterbrochen werden? Aus dem individuellen Schutzbedarf lassen sich die konkreten Massnahmen ableiten. Spätestens an diesem Punkt ist es wichtig, zu erkennen, dass Cyberrisiken keine isolierte IT-Herausforderung sind und dass rein technische Vorkehrungen allein nicht der Schlüssel zum Erfolg sind. Mitarbeitende, welche die IT bedienen, müssen involviert werden (vgl. Box zu Risikokommunikation) und prozessbezogene Vorkehrungen getroffen werden, wie beispielsweise der korrekte Umgang mit der IT und vordefinierte Notfallprozesse.

Nehmen wir ein Geschäftsauto als sinnbildliches Beispiel: Es ist wichtig, dass das Auto ein Schloss und eine Alarmanlage hat (technische Massnahmen). Der Mitarbeitende muss wissen, dass er das Fahrzeug abschliessen muss und nicht einem Fremden übergeben darf (mitarbeiterbezogene Massnahmen). Und schliesslich muss der Mitarbeitende die Erwartungen des Unternehmens zum Umgang mit dem Fahrzeug kennen und wissen, was zu tun ist, wenn das Fahrzeug aufgebrochen oder gestohlen wird (prozessbezogene Massnahmen).

Unternehmen werden bei diesem Unterfangen nicht alleine gelassen. Die IT-Abteilung oder der IT-Dienstleister haben eine Schlüsselfunktion und leisten einen wichtigen Beitrag bei der operativen Umsetzung der Cybersicherheit. Checklisten und Tools zur Standortbestimmung stehen online zur Verfügung (beispielsweise der KMU-Schnellcheck von Digitalswitzerland). Die Anforderungen der Versicherung können als Abgleich dienen und Optimierungspotentiale aufzeigen. Und Dienste wie Cyber Security Health Checks oder Penetrationstests gewähren weitergehende und individuelle Einblicke in das Unternehmen.

Cyberrisiken vermindern und absichern

Cyberrisiken gehören zu den grössten Geschäftsrisiken. Die Cybersicherheit auf die lange Bank zu schieben, kann fatale Folgen haben. Mit der zunehmenden Abhängigkeit von der IT und den zunehmenden Angriffen aus dem Netz erhöht sich der Schutzbedarf für Unternehmen. Ein umfassendes und gut implementiertes Cybersicherheitskonzept reduziert die Wahrscheinlichkeit, Opfer eines Cyberangriffs zu werden. Die Herausforderung, alle möglichen Schwachstellen zu schliessen, kann aussichtslos erscheinen, ist sie aber nicht. Die allermeisten Cyberkriminellen benutzen keine allmächtigen High-tech-Tools. Stattdessen halten sie Ausschau nach Lücken im Grundschutz der Unternehmen. Eine Auswertung des Industrieversicherers Allianz Global Corporate & Specialty (AGCS) hat gezeigt, dass 80 Prozent der Schadenfälle vermeidbar gewesen wären. Wichtig ist deshalb, dass der Grundschutz ernst genommen und von allen Beteiligten getragen wird. Es ist eine interdisziplinäre Aufgabe, die strategisch beim Management beginnt und operativ von jedem Mitarbeitenden umzusetzen ist. Das Ergebnis ist ein vermindertes Risiko, das sich auch langfristig auf eine Versicherung übertragen lässt, welche die Folgen für ein Unternehmen abfedern kann.

Wenn wir diese Herausforderung in der Breite anpacken, erhöhen wir damit die dringend benötigte Cyberresilienz als Wirtschaft und Gesellschaft und stellen damit die Weichen für einen sicheren und nachhaltigen Umgang mit der IT. Die Zukunft beginnt jetzt. ■

DIE AUTOREN

Carlos Casián ist Unternehmensberater und Sprecher der Allianz Suisse in Sachen Cyberrisiken. Er hat das Assekuranzgeschäft von der Pike auf gelernt und beschäftigt sich in den letzten Jahren vertieft mit Cyberrisiken und ihren Auswirkungen auf die Risikoprofile von Unternehmen.

Carlo Pugnetti ist Dozent am Institut für Risk & Insurance an der Zürcher Hochschule für Angewandte Wissenschaften ZHAW. Schwerpunkt seiner Forschung ist das Verhalten von Assekuranz-Kunden, insbesondere Veränderungen, die durch Technologie oder Generationswechsel entstehen. Vor seiner Tätigkeit an der ZHAW war Carlo Pugnetti CEO der Allianz Global Assistance in der Schweiz.

Albena Björck ist Dozentin für International Business, Strategie und Marketing an der Zürcher Hochschule für Angewandte Wissenschaften ZHAW. Ihre Forschungstätigkeit ist an der Schnittstelle zwischen Unternehmensstrategie und Kommunikation, und untersucht insbesondere das Verhalten von Organisationen in Sondersituationen wie Change, Krisen, und Erneuerung. Vor ihrer Tätigkeit an der ZHAW war Albena Björck in leitenden Funktionen in der Schweizer Finanzbranche tätig und begleitete kommunikativ eine der grössten Krisen am Finanzplatz Schweiz.