SPECIAL RISK MANAGEMENT

IMAGO

«Top Gun: Maverick», 2022: Tom Cruise handelt, wie der Filmtitel dieses «Top Gun»-Sequels andeutet, nach 35 Jahren wieder auf eigene Faust und geht hohe Risiken ein. Auch Unternehmen sollten bestimmte Risiken eingehen.

Krisen gut antizipieren

Um sich in der Technologiegesellschaft zurechtzufinden, ist **Risikokompetenz** Vorbedingung.

SANDRA ESCHER CLAUSS

Je ungewisser die Welt, so scheint es, desto mehr sehnt sich die Gesellschaft und mit ihr die Unternehmen als integraler Bestandteil davon nach Gewissheit. Heerscharen an Beraterinnen und Beratern und eine scheinbar perfekte Technik sollen es richten und die Illusion einer Null-Risiko-Welt kreieren. Dabei geht gerne vergessen, dass «no risk» nicht primär «no fun» bedeutet.

Wer alle Risiken einschränkt, beschränkt nicht nur die Freiheit, sondern verunmöglicht Neues, verhindert Innovation und letztlich auch das Leben. Vor lauter Risk-Management-Prozessen, teuren Tools, Audits und Reportings geht gerne vergessen, dass Risiken nicht nur gefährlich sind, sondern auch Upsides haben: Unternehmertum, Kreativität und Forschung sind nur einige davon.

Selbstverständlich spricht nichts dagegen, sich als Unternehmen im Rahmen eines vernünftigen Business-Continuity-Managements auf mögliche Ernstfälle vorzubereiten, und auch Kontrollmechanismen und Regulierungen machen bis zu einem gewissen Grad Sinn. Daneben braucht es aber auch den Mut, sich einzugestehen, dass nicht alles kontrollier- und vorhersehbar ist, und vor allem braucht es Vertrauen in die eigene Intuition, Vertrauen in die Mitarbeitenden und eine transparente Risikokommunikation.

Für Gerd Gigerenzer, Direktor des Harding-Zentrums für Risikokompetenz an der Universität Potsdam, ist Risikointelligenz eine Grundvoraussetzung dafür, um sich in einer modernen technologischen Gesellschaft zurechtzufinden. Risikointelligenz setzt sich aus Gefahren- und Verantwortungsbewusstsein zusammen und aus der Fähigkeit, die relevanten Informationen zu erkennen und daraus intuitiv die richtigen Schlüsse zu ziehen.

Keine Krise kommt aus dem Nichts. Allerdings muss man die Anzeichen, Trends und andere Frühwarnsignale sehen wollen, die Situation realistisch einschätzen und danach etwas unternehmen. Denn Risk-Management ist zwar eine Führungsaufgabe, aber es ist vor allem auch eine Frage der Führungs- und Unternehmenskultur.

Wenn Risk-Management-Verantwortliche, die Geschäftsleitung und das Controlling auf Warnhinweise von Mitarbeiterinnen und Mitarbeitern reagieren würden, wären Unternehmen meist schon viel besser auf Krisen vorbereitet, als sie es mit den rigidesten Kontrollmechanismen sind.

Foto-Portfolio
In dieser Bildstrecke müssen Filmheldinnen und Filmhelden hohe Risiken eingehen, um ihr Ziel zu erreichen und um zu überleben. Gerade in dieser Zeit geht es Unternehmen ähnlich. Risikomanagement ist ein hochaktuelles Thema. (Fotos: Imago)

Verantwortlich für diesen Special: Sandra Escher und Eckhard Baschek

Impressum
Der Special «Risk Management» ist eine redaktionelle Eigenbeilage der «Handelszeitung» und Bestandteil der aktuellen Ausgabe.
Herausgeber: Redaktion und Verlag «Handelszeitung», Ringier Axel Springer Schweiz, 8021 Zürich.

Die Risiken verdrängen bringt nichts

Ein gutes **Business-Continuity-Management** (BCM) hilft, im schlimmsten Fall die Geschäftstätigkeit aufrechtzuerhalten.

IMAGO

«Apollo 13», 1995: Kevin Bacon, Tom Hanks und Bill Paxton (von links) müssen sich mit minimalem Energieaufwand aus der Bredouille befreien. Angesichts der derzeitigen Energieknappheit ein aktuelles Thema auch für Unternehmen.

PATRICK GUNTI

Kaum ein Tag vergeht ohne Nachrichten über Cyberangriffe auf Unternehmen, über Brände, die ganze Unternehmen lahmlegen, oder über Firmen, die aufgrund gestörter Lieferketten und fehlender Teile die Produktion stilllegen müssen. Von drohenden Strommangellagen ist zu hören, und der Ausfall von Arbeitskräften ist seit Covid-19 ebenso keine Theorie mehr. Auch wenn der Staat wie während der Pandemie viele Risiken abfedert, liegt es doch in der Eigenverantwortung jedes KMU, sich auf den Tag X vorzubereiten.

BCM als Plan B

Diese Krisenvorbereitung kann man im Rahmen des klassischen Risk Managements vornehmen, nämlich die Risiken identifizieren sowie Schadenausmass und Eintrittswahrscheinlichkeit bewerten. Also Plan A. Plan B wiederum ist ein Vorsorgesystem in Form des Business-Continuity-Managements (BCM). Es beinhaltet alle Massnahmen, die es ermöglichen, im Fall des doch eintretenden Schadens den Betrieb aufrechtzuerhalten oder eine schnelle Wiederaufnahme zu ermöglichen.

«Letztlich geht es beim betrieblichen Kontinuitätsmanagement im Sinne einer Überlebensgarantie um die Ereignisbewältigung inklusive Bewältigung des Restrisikos», sagt Uwe Müller-Gauss, Inhaber von Müller-Gauss Consulting, Verfasser von zahlreichen Publikationen zum Thema Sicherheit und Risikomanagement sowie Dozent für Risikomanagement und BCM. «Die Bewältigung dieses Restrisikos, aber auch die Bewertung der Risiken bezüglich der Entdeckungszeit und des Umgangs im Ereignisfall führen direkt zum zwingend nötigen BCM», so Müller-Gauss.

KMU haben BCM in ihrer DNA verankert

Trotz der Wichtigkeit des Themas zögern viele KMU. Müller-Gauss glaubt, viele KMU scheuten angesichts umfassender Standards den Aufwand für etwas, das sie von jeher jeden Tag leben. «Banken und Versicherungen sind seitens des Regulators angehalten, ein wirkungsvolles BCM-System aufzubauen. Unternehmergeführte KMU hingegen haben meines Erachtens das BCM-Gedankengut bereits vom Start weg in ihrer DNA verankert», sagt der Experte.

Nicht normgetreu, aber effektiv

Eine sorgfältige und umsichtige Unternehmerin kenne jederzeit ihre Risiken und insbesondere das Risiko, das für sie das Aus bedeuten könnte. Entsprechend bereite sie sich mit Notfallplänen darauf vor, meint Müller-Gauss und ergänzt: «Vielleicht ist das BCM-System in einem KMU weniger strukturiert oder dokumentiert. Es erfüllt daher kaum die einschlägigen Normen, aber es ist sicherlich effizient und effektiv.»

Für die Einführung eines BCM empfiehlt Müller-Gauss KMU denn auch, sich auf das Wichtigste zu konzentrieren: «Es genügt, wenn der Unternehmer mit den Prozessverantwortlichen die kritischen Prozesse und die zugrunde liegenden Ressourcen inklusive der kritischen externen Dienstleister identifiziert. Damit wird auch ein gemeinsames BCM-Verständnis geschaffen.» Danach gelte es, die Überlebensstrategie mit der grundsätzlichen Vorgehensweise zur Aufrechterhaltung einer kontinuierlichen Geschäftstätigkeit festzulegen und für die Prozesse Notfallpläne, sogenannte Business Continuity Plans, zu erstellen: «In ihnen wird das Vorgehen bei einem Ausfall von externen Dienstleistern und Lieferanten, aber auch der Ausfall der IT oder einzelner Applikationen beschrieben.»

Nützlich auch ohne den Ernstfall

Auch wenn Risiken Risiken bleiben und – wie erhofft – nicht eintreten, lohne sich das BCM für KMU. Zwar sei der Aufbau mit zeitlichem Aufwand und mit Investitionen verbunden, die nach Ansicht von Müller-Gauss jedoch überschätzt werden. Dafür aber würden die Strukturen des Unternehmens stabilisiert. Die Sensibilisierung der Stakeholder für eine verantwortliche Unternehmensführung wachse, und das Vertrauen von Kunden, Partnern und Mitarbeitenden in das Unternehmen werde gestärkt. «Und Kontinuität der Geschäftstätigkeit bedeutet nachhaltige Erfolgssicherung für alle», sagt Müller-Gauss.

«Wir bereiten uns auf negative Ereignisse vor»

Was könnte zu einem teilweisen oder vollständigen Unterbruch in Ihrem Betrieb führen?
Wie in jedem Unternehmen ist die IT ein zentraler Punkt. Würde ein Hackerangriff unsere Systeme lahmlegen, kämen wir in grosse Bedrängnis. Auch ein Brandfall ist trotz allen Sicherheitsvorkehrungen nie ganz auszuschliessen. Und wie wir aktuell sehen, treffen unterbrochene Lieferketten die Automobilbranche sehr stark.

Fred Zwahlen, GL-Mitglied, Autobahn-Garage Zwahlen & Wieser AG, Lyss.

Welchen Stellenwert hat die Absicherung der Aufrechterhaltung des Betriebs?
Wir bereiten uns auf negative Ereignisse vor. Die gesamte IT ist gut geschützt. Auch im schlimmsten Fall könnten wir innert vier Stunden den Betrieb wieder aufnehmen. Aber es gibt auch Grenzen: Wird die Garage durch einen Brand oder ein Naturereignis zu schwer in Mitleidenschaft gezogen, haben wir keinen Plan B. Ich kann mir auch nicht vorstellen, dass das eine Garage unserer Grösse – wir haben etwa 50 Mitarbeitende – planen kann.

Sie haben die unterbrochenen Lieferketten angesprochen. Waren Sie auf sie vorbereitet?
Nicht in dem Sinne, dass dieser Faktor im Risikomanagement ein prioritärer Faktor gewesen wäre. Aber die Situation hat sich schon länger abgezeichnet. Mit unserer Mehrmarkenstrategie sind die Risiken gut verteilt. Und das breite Dienstleistungsangebot bringt uns zusätzliche Flexibilität.

INTERVIEW: PATRICK GUNTI

Das beschäftigt Risk Manager

Dem Topmanagement ist bewusst geworden, dass **Business-Continuity-Management** priorisiert werden muss.

Die Quotes auf dieser Seite und auf Seite 31 stammen von Risikoexpertinnen und -experten aus Mitgliedsfirmen der Schweizerischen Vereinigung der Insurance und Risk Manager (Sirm). Sie wurde 1973 gegründet und ist die älteste und grösste Vereinigung für Versicherungs- und Risikomanager in der Schweiz. Sie zählt aktuell rund achtzig führende Firmen aus der Industrie, dem Handel und dem Dienstleistungssektor zu ihren Mitgliedern.

www.sirm.ch

Julian Ledergerber

Insurance & Risk Manager, Bühler AG

«Die Wahrnehmung gegenüber dem Risikomanagement im Topmanagement hat sich verändert. Man ist sich bewusst geworden, dass dem Business-Continuity-Management höhere Priorität beigemessen werden sollte. Zudem möchte es künftigen Grossereignissen noch besser und mit möglichst sinnvollen Vorkehrungen und Massnahmen entgegentreten können. Leider hat die Digitalisierung noch zu wenig Einfluss auf das Risk Management. Daten bilden zwar eine Grundlage zur Bemessung von Risiken und den Massnahmen. Es mangelt jedoch an Verständnis dafür, warum es sich lohnt, in die Digitalisierung des Risk Management zu investieren. In meinem Alltag beschäftige ich mich stark mit Möglichkeiten für den Risikotransfer; er wird durch den verhärteten Versicherungsmarkt merklich geschmälert. Und auch Lieferkettenprobleme beschäftigen uns stark.»

Bettina Spagnolo

Leiterin Risk-Management & Compliance, Flughafen Zürich

«Risk-Management war für uns schon immer ein zentrales Thema, daher hat es sich auch in den vergangenen Jahren nicht gross verändert. Natürlich stellen wir aktuell eine grössere Awareness für die Themen Pandemie und Cyber fest. Der Flugbetrieb ist heute ohne IT nicht mehr möglich, und auch mit unseren Partnern sind wir stark vernetzt. Cyberangriffe auf Airlines oder einen anderen Flughafen können auch Auswirkungen auf uns haben. Im Auge haben wir aktuell auch den Krieg in der Ukraine und die daraus resultierenden Reisebewegungen, die höheren Energiepreise sowie die Sanktionen. Die Digitalisierung nutzen wir zurzeit vor allem im operativen Bereich – und dort vor allem dazu, Reportingprozesse zu vereinfachen.»

Arthur Treichler

Leiter Risk Management, Cellere Bau

«Risk Engineering im Bereich AHS sowie das Thema Nachhaltigkeit sind in der Baubranche stark im Fokus. Heute sehen wir uns zudem mit vielen veränderten gesetzlichen Rahmenbedingungen konfrontiert und auch mit höheren Anforderungen von Auftraggeberseite sowie seitens der Öffentlichkeit. Dank der Digitalisierung ist der Zugang zu Risikofaktoren einfacher geworden, weil die Datenverfügbarkeit deutlich besser und schneller ist.»

Keine Frage der Technik

Die Achillesferse im Risk Management grösserer Schweizer Unternehmen ist das **Cloud-Computing,** zeigt eine aktuelle Studie der Hochschule Luzern.

IMAGO

«Cliffhanger», 1993: Sylvester Stallone muss die Schwerkraft und üble Schurken überwinden. Die kommen heute in der Wirtschaft oft statt mit dem Helikopter über Datenleitungen.

WERNER RÜEDI

Cyberrisiken zählen zu den globalen Toprisiken. Auch die Treiber der Entwicklung sind bekannt: Die zunehmende Entwicklungen Richtung Cloud Computing, die Virtualisierung des Arbeits- und Privatlebens und die stärkere Vernetzung mit dem Internet auch im industriellen Umfeld führen dazu, dass die Risiken zunehmen.

Vor allem die Industrie, die vermehrt auf Cloud-Services setzt, ist mit nicht zu unterschätzenden Risiken konfrontiert: Datenschutz, rechtliche Unsicherheiten, Vertraulichkeit der Daten, Abhängigkeit von einem einzelnen Anbieter, Know-how- und Kontrollverlust, Zunahme der Komplexität, weil Cloud-Anbieter in diverse Massnahmen und Prozesse eingebunden werden müssen wie etwa ins Business-Continuity-Management (BCM).

Unübertragbare Aufgaben

Leitungsgremien tun daher gut daran, Cyberrisiken nicht ausschliesslich als technisches IT-Problem zu verstehen. «Damit sind Aufsichtsorgane zunehmend gefordert, ihre rechtlichen Kontroll- und Aufsichtspflichten auch im Bereich Cyberrisk-Management wahrzunehmen», sagt Stefan Hunziker, Professor und Leiter Kompetenzzentrum Risk and Compliance Management der Hochschule Luzern (HSLU). Denn «der angemessene Umgang mit Cyberrisiken gehört zu den unübertragbaren und unentziehbaren Aufgaben jedes Aufsichtsorgans». Dies, weil Cyberangriffe einen erheblichen Schaden in Organisationen verursachen können, die im schlimmsten Fall hohe Bussen, starke Reputationseinbussen, einen Entzug der Betriebsbewilligung oder sogar den Konkurs bedeuten können.

Hunziker hat mit seinem Team und unterstützt von Economiesuisse sowie von der Schweizerischen Mobiliar das Cyberrisk-Management in 18 grösseren Schweizer Unternehmen aus unterschiedlichen Branchen mit Fokus auf Cloud-Computing untersucht. Dazu liess er 33 Interviews mit Chief Information Security Officers (CISO) und Risk-Management-Verantwortlichen durchführen. Die Ergebnisse zeigen deutlich auf, dass die Relevanz von Cyberrisiken in allen Organisationen in den letzten Jahren erheblich gestiegen ist.

Die oberste Verantwortung für Risiken trägt immer der Verwaltungsrat.

Gefährliche Lücke

Ebenso ist in den Leitungsgremien eine hohe bis sehr hohe Awareness feststellbar. Beispielsweise bei der Fenaco Genossenschaft: «Cyberrisiken sind ein Teil unseres Enterprise-Risk-Managements (ERM)», betont Maria Nutz, Bereichsleiterin Sachversicherungen und Risk Management bei Fenaco, «sie werden speziell im Informationssicherheits-Risikomanagement erfasst, konsolidiert und der Risiko-Controlling-Stelle gemeldet. Letztere sammelt und aggregiert alle Risiken. So fliessen auch Cyberrisiken in den Risikobericht ein.» Das ist für die Agrargenossenschaft mit gut 43 000 Mitgliedern und unterschiedlichen Geschäftsbereichen zentral.

Und doch: Bei vielen Unternehmen scheint ein zentrales Fundament zum Managen von Cyberrisiken zu fehlen. So hat keine der befragten Organisationen explizit definiert, in welchem Ausmass Cyberrisiken bewusst eingegangen werden sollen, um die Geschäftsziele zu erreichen. «Aus der Sicht des Risikomanagements ist das vergleichbar mit einem Schiff, das keinen Kapitän hat», bringt es Studienautor Stefan Hunziker auf den Punkt. Offenbar bereitet das Entwickeln von sogenannten Risikoappetitaussagen in der Praxis grosse Mühe.

Die HSLU-Studie zeigt: Im Umgang mit Cyberrisiken herrscht eine Lücke zwischen der technischen IT-Infrastrukturebene und der organisatorischen Ebene. «Cyberrisiken werden noch zu stark als reines IT-Thema verstanden. Entsprechend werden sie dezentral und operativ gesteuert und zu wenig in das unternehmensweite Risk Management integriert», erläutert Hunziker. Hier ist eine Diskrepanz zwischen der Relevanz des Risikos (Awareness) und der Risk Governance feststellbar. «Dieser Umstand verhindert einen konsistenten Vergleich – und damit auch eine sinnvolle Priorisierung – von Cyberrisiken und anderen Risikokategorien auf oberster Führungsebene», sagt der Experte.

Cyberversicherungen

Cyberrisiken können nicht gänzlich verhindert werden. Gerade im Zuge der Pandemie mit dem vermehrten Homeoffice oder der steigenden Anzahl Cyberattacken rückt die Möglichkeit eines Risikotransfers an Versicherer in den Fokus. Aufgrund dieser Entwicklung könnten sich Cyberrisken in den nächsten Jahren zu einer Risikokategorie vergleichbar mit anderen bekannten Risiken entwickeln, gegen die sich zunehmend mehr Firmen und Organisationen versichern.

Doch was können Versicherer beitragen, um Risiken zu minimieren? «Wir als Versicherer sind in der Tat gefordert», so Andreas Hölzli, Leiter Kompetenzzentrum Cyber Risk der Mobiliar. «Mit der Cyberversicherung ermöglichen wir beispielsweise Unternehmen einen bedürfnisgerechten Risikotransfer.»

Die aufgezeigten Schwachpunkte in der Studie in Bezug auf deren Anwendbarkeit müsse jedes Unternehmen für sich beurteilen, sagt Hölzli. Aber: «Ungeachtet der technischen Massnahmen kann ein Unternehmen mit dem gezielten Aufbau einer Risikokultur gegenüber Cybergefahren bereits viel erreichen; für diese Stärkung der Widerstandsfähigkeit ist ein Mix von personenbezogenen, technischen, organisatorischen und physischen Massnahmen wichtig.» Andreas Hölzli zeigt sich erstaunt darüber, dass die steigende Gefahr von Cyberrisiken kaum Thema in den Gesprächen mit den Versicherungsgesellschaften ist: «Auch Handlungsempfehlungen und Bedarfsabklärungen werden bei einem etwaigen Restrisiko wenig angesprochen. Dieser Cyberrisikodialog würde nicht nur im Risikoverständnis und Bewusstsein helfen, sondern unter anderem auch in der Risikoeinschätzung, in der Festlegung der Risikoakzeptanz sowie in der Überwachung.»

In der Industrie geht es aber auch um Grundsätzliches: «Man muss die Balance finden: Ist es klüger, das Geld in die Versicherungslösung zu investieren, oder ist es besser, in Cyber-Security zu investieren?», fragt Peter Jussel vom Corporate Risk and Insurance Management der Hilti Corporation, dem weltweit tätigen liechtensteinischen Werkzeughersteller. Die Balance dürfe man nicht so verstehen, dass die Ausgaben für die Versicherungsdeckung einerseits und die Cyber-Security anderseits in etwa gleich gross seien. Es ist eine Balance, die – so die HSLU-Studie – vermehrt von der obersten Führungsebene gehalten werden muss.

www.hslu.ch, Über uns, Medienstelle, Aktuelle Medienmitteilungen, «Cyber Risk Management: Bewusstsein allein reicht nicht».

Wertvolle Erkenntnisse der Studie

Cloud-Agnostizismus Basierend auf der Studie «Cyber Risk Management in grösseren Schweizer Unternehmen» und in Abstimmung mit der aktuellen Literatur werden folgende acht konkrete Empfehlungen im Umgang mit Cyberrisiken an die Praxis formuliert:

1. Integration von Cyberrisiken ins ERM fördern.

2. Fehlende Risk Governance – fehlendes Fundament: Cyberrisiken müssen in der Corporate Governance jeder Organisation formell verankert werden.

3. Mehrwert bringende Dienstleistungen des Versicherers: Im Risikodialog zwischen Kundschaft/Risk Manager und IT-(Security-)Dienstleister oder Chief Information Security Officer (CISO) kann ein Versicherer auch als Sparringspartner auftreten.

4. Faktor Mensch – ein lohnendes Investment: Menschliche Verhaltensweisen werden im Bereich der Cybersicherheit tendenziell noch zu wenig adressiert.

5. Cloud-Kosten früh und langfristig planen.

6. Cloud-Agnostizismus ermöglicht Flexibilität: Wer Dienstleistungen auslagert, begibt sich in ein Abhängigkeitsverhältnis. Durch die Gestaltung einer Cloud-agnostischen IT-Infrastruktur lässt sich der Grad der Abhängigkeit gezielt reduzieren und steuern.

7. Kontrolle behalten – klassifizieren und verschlüsseln.

8. Vorbereitet sein für Notfälle durch Planung und Übung.

PHILIPP GRABHER

«Richtiges Verhalten fördern»

Der Chief Information Security Officer des Kantons Zürich will eine Sicherheitskultur entwickeln.

INTERVIEW: JOLANDA BRÜHWILER

Wo setzen Sie mit der Security-Awareness-Strategie an?
Top-down. Mitunter das Wichtigste ist es, mit der Geschäftsleitung und Business-Stakeholdern aus dem HR, dem Rechtsdienst, dem Marketing und anderen Abteilungen aktiv in den Dialog zu treten und Aufmerksamkeit für das Thema zu erwirken. Wir wollen mehr an wichtigen Sitzungen und in Gremien vertreten sein und aufzeigen, was der aktuelle Stand des Security-Programms ist, wo neue Risiken lauern, und aktiv Möglichkeiten aufzeigen, wie wir diesen Risiken am besten begegnen.

Also essenzielle Stakeholder ausserhalb der IT abholen?
Ja, es werden mit gezielten Schulungen und Hilfsmitteln die unterschiedlichen Stakeholder von uns unterstützt. Das ermöglicht es ihnen, in ihrem Fachbereich bezüglich Security möglichst selbst Entscheidungen treffen zu können. Zudem ist wichtig, dass sie die Security-Kultur vorleben und hinter den Vorgaben stehen, die definiert wurden.

Heisst das, mehr Verantwortung in die Hände der Business-Units zu legen?
Genau, denn hier muss ein Umdenken stattfinden. Wenn Abteilungen neue Software evaluieren und Prozesse definieren, ist es Aufgabe der entsprechenden Verantwortlichen, Security-Vorgaben und Richtlinien einzuhalten. Damit sie Risiken richtig einschätzen können, definieren wir eine übersichtliche Anzahl von Massnahmen, die sie einhalten müssen. Daran können sie sich gut orientieren und erhalten eine Art Risk Score, der eindeutig aussagt, wo sie sich auf der sicheren Seite befinden und wo Korrekturen notwendig sind.

Sind sie damit nicht überfordert?
Nicht, wenn wir sie aktiv ins Boot holen, ihre Bedürfnisse mit einbeziehen und sie richtig ausbilden. Das ist ein kontinuierlicher Prozess und erfordert drei elementare Punkte: Transparenz, Risikobewusstsein und gegenseitiges Vertrauen. IT- und Cybersecurity betrifft das ganze Unternehmen. Deshalb ist es wichtig, dass alle Mitarbeitenden Verantwortung übernehmen und zur Sicherheit beitragen. Des Weiteren sollten technologische Lösungen und Prozesse immer so gestaltet sein, dass sie sicheres Verhalten fördern oder durchsetzen.

Der Stratege

Name: Philipp Grabher
Funktion: Chief Information Security Officer (CISO), Kanton Zürich
Geboren: 5. März 1981
Zivilstand: ledig
Ausbildung: MSc in Information and Computer Engineering, PhD in Information Security

Wie meinen Sie das?
In meinen Augen ist es wichtiger, eine Art Sicherheitskultur zu etablieren. Es mag ein etwas abgegriffenes Wort sein, aber ich mag es. Das Aufzeigen von Gefahren und das damit verbundene richtige Verhalten kann nicht nachhaltig mit umfangreichen Dokumenten, Pflichtschulungen oder Phishing-Mails vermittelt werden. Man muss das vielmehr geschickt in den Alltag einbauen – sogenannte Security Nudges – und versuchen, den Mitarbeitenden zu helfen, ihre Gewohnheiten anzupassen und sich automatisch sicherheitsbewusst zu verhalten. Es sollte so verinnerlicht werden, wie sie ihr Zuhause abschliessen, wenn sie es verlassen. Unser Ziel ist, dass Security zum Alltag gehört und unsere Mitarbeitenden das Erlernte auch im privaten Umfeld anwenden können.

Haben Sie dazu schon Pläne?
Wir haben eigens für die Security Culture eine Stelle geschaffen und sind überzeugt, die Leute positiv zu inspirieren. Was die Cybersecurity allgemein betrifft, arbeiten wir an einem neuen, umfassenderen Programm, das wir demnächst der Öffentlichkeit vorstellen.

Sie erwähnten die Idee, Cybersecurity als Kriterium bei der Mitarbeitendenbeurteilung einzuführen. Wie könnte das in der Praxis aussehen?
Bei Entscheidungsträgerinnen und Entscheidungsträgern könnten beispielsweise ihr Engagement und die Security-Maturität in ihrem Verantwortungsbereich bewertet werden – unter anderem, welche Security-Risiken sie eingehen, wie oft sie sich mit dem Thema auseinandersetzen. Bei den IT- und Prozessverantwortlichen kann mit einfliessen, inwieweit die Cybersicherheit im Lösungsdesign berücksichtigt wurde, unter anderem auch anhand von erkannten kritischen Schwachstellen, von Sicherheitsvorfällen oder auch von Audit-Befunden. So wie ein Score, ähnlich einem Security-Health-Status, kann bei jeder Mitarbeiterin und jedem Mitarbeiter aufgezeigt werden, wo sie oder er sich im grünen Bereich bewegt und wo nicht.

IMAGO

«Fast & Furious 5» («Fast Five»), 2011: Vin Diesel und Paul Walker mit viel Ballast im Schlepptau und Dwayne Douglas «The Rock» Johnson im Nacken im Showdown am Ende der Brücke. Auch von alten IT-Systemen, «Legacy Systems», gehen Risiken für kleine und grosse Unternehmen aus.

Die Wertschöpfung steht im Zentrum

Bei den SBB arbeitet man mit dem **«Combined Assurance»-**Risikomanagementansatz, um die Risiken zu handhaben.

MATTHIAS NIKLOWITZ

Witterungseinflüsse hatten 2021 bei den SBB zu etwa 200 000 Verspätungsminuten geführt – obwohl man von den heftigen Unwettern in Europa im Sommer 2021 kaum betroffen war. Gemäss dem Geschäftsbericht 2021 werden die Extremereignisse ohne Begrenzung der Erderwärmung in den kommenden Jahren noch häufiger und intensiver auftreten. Die SBB beteiligen sich deshalb am Forschungsprojekt «From Hazard to Risk» oder auf Deutsch «Prospektives Naturgefahrenmanagement SBB», mit dem man Auswirkungen des Klimawandels auf das Anlagenmanagement ableiten wird.

Das konzernweite Risk Management, das sich an ISO 31000 orientiert, basiert auf der konzernweiten Risk Policy, die die Ziele, Grundlagen und Aufgaben festlegt. Jährlich werden Risiken identifiziert, beurteilt und Massnahmen ergriffen. «Wir definieren Risiken wie folgt: Auswirkungen von Unsicherheiten auf Ziele. Dies inkludiert unter anderem finanzielle, qualitative und betriebliche Ziele wie auch Tätigkeiten und Anforderungen», sagt Angela Hunziker, Leiterin Corporate Risk Management bei den SBB.

Hier setzt die «Assurance» ein: Darunter versteht Hunziker die Gesamtheit der SBB-Überwachungs- und Kontrollfunktionen, die der Führung eine Sicherheit bezüglich der Überwachung von Unternehmensrisiken und der Einhaltung von gesetzlichen und internen Vorgaben bieten. «Assurance ist heute noch nicht offiziell in den SBB-Regelwerken definiert, was ja bereits die erste Schwierigkeit darstellt», so Hunziker. Gemäss Institute of Internal Auditors (IIA) wird «Assurance» definiert als «unabhängige Bestätigung und Vertrauen»; Assurance kann nur als «angemessen» beziehungsweise «reasonable» konzipiert werden, denn Vertrauen ist selten absolut.

Qualität der Governance steigern

Die «Combined Assurance» entspricht laut Hunziker unter Rückgriff auf Ansätze von Marc Eulerich und des Deutschen Instituts für Interne Revision einer «koordinierten und integrierten Zusammenarbeit aller Funktionen, die direkten und indirekten Risikobezug haben und zur Verbesserung der Governance-Struktur beitragen können». Zielsetzung sei es, entweder den Ressourcenaufwand der Governance-Funktionen zu minimieren oder die Leistung ceteris paribus zu optimieren. Ergänzend kann diese Zusammenarbeit mit Governance-relevanten Funktionen weitere risikorelevante Bereiche einbinden. «Durch die Erfüllung der Zielsetzung steigert Combined Assurance die Qualität der Corporate Governance», sagt Hunziker.

Was statisch klingt, muss in einem Unternehmen mit sich verändernden Risiken funktionieren. «Wir zeigen die sehr dynamischen Risiken wie etwa die Fahrplanrisiken nicht im jährlichen Risk Reporting», so Hunziker. «Es geht bei der Berichterstattung an Leitungsgremien wie die Divisions- und Konzernleitungen oder an den Verwaltungsrat um mittel- und langfristige Risiken.» Der mittelfristige Horizont liegt hier bei sechs Jahren.

Es geht zum dynamischen Risikomanagement via Change-Management.

«Unter dynamischen Risikomanagement im Sinne von ISO 31000 verstehe ich die ständige Beurteilung und Behandlung von Risiken», erklärt Angela Hunziker weiter. «Das heisst konkret: Mittelfristige Risiken werden aktualisiert, wenn etwas passiert, was die Beurteilung tangiert; das geschieht meilensteinbasiert, laufend und dynamisch. Gleichzeitig sind wir jetzt daran, Risiken stärker mit der unterjährigen Finanzplanung zu verknüpfen. Beispiel: Rohstoffpreise, Energiepreise. Diese Betrachtung ist unterjährig, also kurzfristig und sehr dynamisch.»

Meilensteinbasierte Umsetzung

Für Angela Hunziker geht der Weg zum dynamischen Risikomanagement via Changemanagement. «Wir sind es gewohnt, ein- bis zweimal jährlich die Risiken hervorzuholen, zu überlegen, wie sie sich verändert haben und sie gegebenenfalls anzupassen.» Eventuell würden dann neue Massnahmen definiert und eingeleitet. «Das soll meilensteinbasiert geschehen, also losgelöst vom Jahresprozess.» Das bedeute nicht automatisch mehr Aufwand, ganz im Gegenteil: Die Welle würde geglättet, indem nicht alles auf einen spezifischen Abgabetermin erarbeitet werden muss, sondern auf dann, wenn es sinnvoll ist.

Ein gutes Tool sei dafür auch eine Riesenstütze. Klassische Assurance leistet die interne Revision der SBB. Als «Third-Line-Assurance-Funktion» (zur ersten Linie gehört das Management, zur zweiten Linie zählen die Hüter der Managementsysteme) prüft diese unter anderem die Funktionsfähigkeit der Second-Line-Assurance-Funktionen, die die Managementsysteme zur Operationalisierung von Vorgaben und zur Überwachung betreiben und die First Line bei der Umsetzung unterstützen.

«Diese aufgeführten Funktionen arbeiten sehr gut und gerne miteinander, das hat mit den Köpfen der Leitenden dieser Funktionen zu tun. Diese wollen zusammenarbeiten. Einzig dass eine koordinierende Stelle fehlt, empfinde ich als verbesserungswürdig.»

Auch die interne Berichterstattung soll aufgebaut werden. Dazu gehört ein integriertes Konzernlage-Monitoring mit aktuellen Bedrohungslagen und einem Zusammenspiel mit der «Second Line». Die Jahresberichte sind ebenfalls davon betroffen, denn die werden zwar zeitlich synchron fertiggestellt, aber sie sind inhaltlich noch nicht genügend aufeinander abgestimmt.

Risk Management ist kein Selbstzweck

«Das Risikomanagement ist nie Selbstzweck, sondern soll immer die Wertschöpfung ins Zentrum stellen», so Hunziker. Das gelte auch für integrierte Assurance. «Wenn wir effizienter und besser zusammenarbeiten, sparen wir Ressourcen, die dann wiederum in anderen Bereichen Gutes tun können. Vielleicht können wir diese zukünftig für beratende Tätigkeiten einsetzen, beispielsweise um den Zielkonflikt zwischen Verfügbarkeit, Sicherheit und Wirtschaftlichkeit aufzulösen.»

IMAGO

«Kill Bill – Volume 1», 2003: Uma Karuna Thurman muss alle ihre Fähigkeiten einsetzen, um multiple Gefahren abzuwehren. Und schnell entscheiden. Wie es auch Unternehmen tun müssen.

Dunkle, leider lukrative Geschäfte über das Netz

Viele **Cyberattacken** bauen auf aktuelle Ereignisse und Trends – und auf menschliches Versagen, die «Schnittstelle Mensch» und Schwächen der Cloud. Auch Fachleute kann es dabei treffen.

JOLANDA BRÜHWILER

Warum gehen viele Menschen Hackern trotz Warnungen, Medienberichten und unternehmensinternen Awareness-Trainings noch immer auf den Leim und klicken unheilvolle Links an? Ist es die menschliche Neugierde, Unachtsamkeit oder Unwissen über neueste Tricks via Social-Media-Posts, Whatsapp und Videokonferenz-Tools? Nicht nur. Auch ein perfektes Timing kann zum Erfolg führen, wie das Beispiel eines Experten zeigt, der selbst in die Falle tappte.

Der unwiderstehliche Link

Alvaro Amato, Country Manager Schweiz von Check Point Software Technologies, erzählt, wie es dazu kam. «Sogar ich, als Security-Spezialist, habe auf meinem Mobiltelefon auf einen Phishing-Link geklickt. Ich erwartete eine Sendung, war im Stress, abgelenkt und bekam ein sehr gutes Phishing-E-Mail der Schweizerischen Post. Alles stimmte. Das Logo des Anbieters, der fehlerfreie Text und sogar ein Impressum war vorhanden. Dank unserer Technologie wurde mein menschliches Versagen zum Glück abgefangen.»

Wie Amato geht es leider noch zu vielen. Nicht nur Klicks auf Links, das Öffnen bösartiger Anhänge oder das Offenlegen von Passwörtern sind Schwachstellen. Ilona Simpson, CIO EMEA von Netskope, kennt aus Erfahrung einige Beispiele erfolgreicher Angriffe, bei denen Cyberkriminelle auf ungesicherte Daten in der Cloud zugreifen konnten. «Fast alle Datenlecks sind darauf zurückzuführen, dass Benutzerinnen und Benutzer ihre Daten in Cloud-Umgebungen speichern, ohne sich viele Gedanken über den Schutz dieser Informationen zu machen», erklärt sie.

Alarmstufe rot

Angreifer und Angreiferinnen machen sich aktuelle Themen und Ereignisse zunutze. Sie wissen um die Anziehungskraft relevanter Inhalte und nutzen das schamlos aus, wie die Verdoppelung der Angriffe seit der Pandemie zeigen. Das ruft neue Vorgehensweisen im Bereich des Sicherheitsbewusstseins bei den Mitarbeitenden auf den Plan. Doch dies ist leichter gesagt als getan, denn seit das Homeoffice Einzug in den Alltag gehalten hat, sind auch die Risiken proportional gestiegen – sowohl technisch als auch menschlich. Hinzu kommt, dass in vielen Firmen innert kürzester Zeit die gesamte Belegschaft fürs Remote-Arbeiten eingerichtet werden musste. Verständlich, dass dann die Prioritäten und Budgets nicht auf Security-Awareness-Trainings gelegt wurden.

Gemäss Christian Meier, Head Business Security Consulting bei Ispin, mangelte es leider schon vor der Pandemie an Security-Schulungen. «In der Vergangenheit wurden Awareness-Trainings selten durchgeführt. Es gab noch wenige unterstützende Tools, und eine gute Awareness-Kampagne benötigt einiges an Ressourcen und Zeit, und nur ein risikobasierter Ansatz führt zu korrekter Allokation der Mittel.»

Das deckt sich mit den Erfahrungen von Harald Drexler, Senior-Projektleiter Informationssicherheit bei der IABG. «Die meisten Unternehmen, die ich kenne, führen Trainings nur rudimentär durch.» Laut dem «2021 Verizon Data Breach Investigations Report» sind 85 Prozent der Datenschutzverletzungen auf menschliche Interaktion zurückzuführen, erläutert Rob Rashotte, Vice President, Global Training & Technical Field Enablement bei Fortinet: «Sie können über alle Sicherheitslösungen der Welt verfügen, aber wenn Sie es versäumt haben, Ihre Mitarbeitenden im Umgang mit dem Internet und den Risiken zu schulen, werden Sie nie wirklich sicher sein.»

Mitarbeitende sind nicht nur die wichtigste Ressource. Sie sind auch zentral bei der Cybersicherheit.

Dem Bewusstsein mehr Leben einhauchen

Mitarbeitende sind nicht nur die wichtigste Ressource von Unternehmen. Sie spielen auch eine zentrale Rolle bei der Cybersicherheit. Ihre Handlungen sind oft die Ursache von Vorfällen. Und das waren allein im ersten Halbjahr 2022 nicht wenige. Das häufigste Einfallstor für Angriffe sind laut allen Expertinnen und Experten nach wie vor E-Mails. Doch Social Engineering holt rasant auf. Da gilt es, die Nutzenden mehr als ein- bis zweimal jährlich zu sensibilisieren. Sie sollten mit inhaltlich interessanten Aktionen zu mehr Bewusstsein und Vorsicht aufgerufen werden. Vor allem, weil im Homeoffice mehr Ablenkung vorhanden ist und die Geräte meist nicht nur geschäftlich genutzt werden.

«Eine grosse Herausforderung sind eigene, mobile Devices. Wir hören oft, dass sich Angestellten gegen Security Agents wehren, wenn ihre Arbeitgeber solche installieren wollen. Dabei könnte damit eine riesige Security-Lücke geschlossen werden – und die Agents sorgen nur für Sicherheit und sind kein Überwachungstool», so Amato. Candid Wüest, Vice President Cyber Protection Research bei Acronis, sieht die Herausforderung darin, die Mitarbeitenden zur Mithilfe zu motivieren. «Wenn die Angst vor Bestrafung besteht, wenn man meldet, dass man ein Phishing-E-Mail angeklickt hat, wird das keiner tun.» Er empfiehlt, die menschliche Firewall zu nutzen und positiv zu fördern.

Ein Belohnungsprogramm wäre eine Möglichkeit, das Bewusstsein zusätzlich zu fördern und sich die Unterstützung der Mitarbeitenden zu sichern. Eine gute Gelegenheit, die Wichtigkeit der Cybersicherheit zu zeigen und den Grundstein für eine starke Sicherheitskultur zu legen. Auch freundliche Reminder und Hinweise auf aktuelle Bedrohungen sind adäquate Massnahmen. Erst recht, wenn die Informationen in bildhafter Sprache und mit emotionalen Komponenten umgesetzt werden, die auch Hackerinnen und Hacker nutzen. Rashotte weist auf einige hin, die beispielsweise Social-Engineering-Angriffe ausmachen: ein emotionaler Appell, der Angst, Neugier, Aufregung, Wut, Traurigkeit oder Schuldgefühle hervorruft. Oder Inhalte, die das Gefühl von Dringlichkeit im Zusammenhang mit der Anfrage aufkommen lassen.

Klare Regeln und Notfallplan

Klare Regeln und ein Notfallplan, den alle Mitarbeitenden kennen, sollte in jedem Unternehmen zum Standard gehören. Simpson erachtet ein digitales Hotline-System, das es Nutzerinnen und Nutzern ermöglicht, schnell auf fragwürdiges Material oder einen laufenden Angriff zu reagieren, als hilfreich. «Dieses System sollte intuitiv zu finden und zu nutzen sein. Zudem sollte der Ton in der Kommunikation des Sicherheitsteams niemals anklagend, sondern verständnisvoll und unterstützend sein», so Simpson.

Vertragliche Regelung

Um das Bewusstsein der Mitarbeitenden zu schärfen, wäre eine separate Klausel im Arbeitsvertrag eine zusätzliche Möglichkeit, um die Klaviatur auf allen Ebenen zu spielen und Risiken auf ein Minimum zu beschränken. Manche Unternehmen haben dies bereits umgesetzt, andere, wie Meier, sehen darin keine Notwendigkeit oder erachten dies als nicht zielführend «Ich finde, es sollte, ähnlich wie Compliance-Trainings, für alle Mitarbeitenden verpflichtend sein, aber nicht als bestrafende Klausel im Arbeitsvertrag integriert werden», so Wüest.

Auch Drexler erachtet dies als nicht notwendig, kennt aber Unternehmen, die diesen Aspekt in die Policy integrieren. Beim Amt für Informatik des Kantons Zürich ist die Einhaltung von Sicherheitsvorgaben ein integrierter Bestandteil der Arbeitsverträge. «Man könnte für die Zukunft in Betracht ziehen, für bestimmte Rollen die Cybersicherheit als Kriterium bei der Mitarbeitendenbeurteilung heranzuziehen», erklärt Philipp Grabher, CISO beim Kanton Zürich.

Ob vertraglich geregelt oder nicht: Security Awareness ist mehr ein Marathon denn ein Sprint und eine Kombination von Wissen, Verständnis und richtigem Verhalten. Das will gelernt sein.

«Den Fokus auf strategische statt operative Risiken legen»

Evelyn Lämmli

Head Corporate Risk & Insurance, Rieter Management

«Die Compliance-Thematiken haben sich in allen Bereichen massiv verstärkt und auch die Anfälligkeit, Preisgestaltung und Abhängigkeiten der Lieferketten haben zugenommen. Ausserdem zeigt sich, dass sich das Aufgabengebiet im Risk Management verstärkt in andere Bereiche ausdehnt, da viele Themen vernetzter und komplexer werden und die Anforderungen an ein effizientes Risikomanagement steigen. Die Digitalisierung schafft teilweise eine Vereinfachung beim Generieren von Auswertungen und auch beim Erhalt von Informationen. Im Gegenzug wächst jedoch die Anfälligkeit bezüglich Datensicherheit und Datenverletzlichkeit. Verstärkt sehen wir zudem, dass die Forderungen zunehmen, eine soziale, ökologische und ökonomische Nachhaltigkeit innerhalb des Betriebes sicherzustellen.»

Sabrina Hartusch

Global Head of Insurance, Triumph Holding

«Risikomanagement ist mittlerweile nicht mehr nur Sache der Risk-Management-Abteilungen, sondern ist auch in anderen Abteilungen angekommen. Allerdings liegt der Fokus meiner Ansicht nach immer noch zu stark auf operativen Risiken statt auf strategischen. Tendenziell ist das Risikomanagement noch nicht dynamisch genug und hinkt den Trends etwas hinterher. Ich bin überzeugt, dass die Digitalisierung das Risk Management stärken und prägen wird, gerade im Bereich Data Analytics. Allerdings muss das Bewusstsein für digitale Risiken noch verschärft werden und digitale Risiken müssen ganzheitlich erfasst werden, denn sie sind von einer anderen Natur als rein physische Risiken. Das treibt mich im Alltag genauso um wie die Nachhaltigkeit der Supply Chain und die hohe Volatilität der Welt.»