FLORIAN

«Man vertraut

Flächendeckende IT-Sicherheit und Konnektivität haben das Potenzi

INTERVIEW: SANDRA WILLMEROTH

Das Thema Cybersecurity scheint in vielen Firmen noch immer nicht wirklich ernst genommen zu werden. Sind sich die Unternehmen der Risiken nicht bewusst?
Im Jahr 2023 sollte man schon wissen, dass Cyberangriffe ein Problem werden könnten. Oft weiss man aber vielleicht nicht, wie man mit dem Thema umgehen soll. Hier sehe ich unter anderem eine Rolle des Staates und konkret des Nationalen Zentrums für Cybersicherheit, diesbezüglich für Sensibilisierung und Aufklärung zu sorgen und gleichzeitig mit der Politik gemeinsam nach Lösungen zu suchen. Unternehmen sind selber für ihre IT-Sicherheit verantwortlich, aber der Staat hat die Aufgabe, die Rahmenbedingungen zu schaffen, damit Unternehmen diese Verantwortung wahrnehmen können.

Haben Sie einen konkreten Vorschlag?
Heute wird noch sehr häufig ein Geheimnis um Cyberangriffe gemacht und das Thema wird weitestgehend tabuisiert. Das ist aus meiner Sicht aber falsch. Man müsste über jeden Angriff offen sprechen, alle Angriffe dokumentieren und feststellen, wie die Angreifer vorgegangen sind. So kann man vergleichen und andere warnen, sodass alle besser vorbereitet sind. Denn die kriminellen Gruppen haben kein Interesse daran, dass ihre Vorgehensweisen ans Licht kommen. Hier könnte mehr Transparenz abschreckend wirken.

Wie könnte diese Transparenz hergestellt werden und von wem?
Es braucht natürlich Ressourcen, um das zu dokumentieren. Man könnte beispielsweise aufseiten des Bundes bei grösseren Vorfällen die Zusammenhänge untersuchen und publizieren.

Unternehmen fürchten häufig einen Reputationsverlust, wenn sie einer Cyberattacke ausgesetzt waren, und machen einen Vorfall lieber nicht publik.
Eine solche Dokumentation kann ja auch anonymisiert geschehen. Zudem hat sich das Verhalten zum Glück schon ein bisschen geändert. Wir hatten in der Schweiz ein paar Unternehmen, auch grössere Konzerne, die vorbildlich über ihre Cybervorfälle berichtet haben. Das enttabuisiert das Thema, und das ist auch gut so.

Die Versicherer schätzen, dass lediglich 10 Prozent der KMU in der Schweiz eine Cyberversicherung abgeschlossen haben. Beunruhigt Sie diese tiefe Zahl?
Jede Unternehmung muss gut abwägen, wo sie ihr Geld investiert, um sich vor Cyberangriffen zu schützen. Eine Versicherung hilft dem Unternehmen, den Wiederaufbau zu finanzieren. Zu diesem Zeitpunkt ist aber bereits ein Schaden entstanden.

> «Eine Versicherung verhindert keine Cyberattacke.»

Höre ich bei Ihnen eine gewisse Skepsis heraus in Bezug auf Cyberversicherungen?
Eine Versicherung ist ein valides Mittel, wie in allen üblichen Lebensbereichen auch, aber sie verhindert keine Cyberattacke. Gerade ein KMU kann viel auslagern und für die Cybersicherheit beispielsweise einen externen Anbieter an Bord holen, der die notwendigen Sicherheitspakete liefert und in den Service Level Agreements Zusicherungen für den Fall eines Angriffs macht. Sollte dieser Anbieter jedoch für einen Cybervorfall nicht geradestehen, muss die Unternehmerin oder der Unternehmer diese Deckungslücke irgendwie kompensieren. Die Verträge sollten das klar und eindeutig definieren. Und wenn das dafür notwendige Wissen über IT-Serviceleistungen nicht vorhanden ist, sollten die Personen, die im Unternehmen die Verträge verhandeln, eine entsprechende Weiterbildung in Betracht ziehen.

Sie wollen den Patron einer Schreinerei oder den Geschäftsführer eines Skiherstellers zurück auf die Schulbank schicken?
In der Geschäftsleitung eines jeden Unternehmens sollte generell ein Fundament an Cyberwissen vorhanden sein. Ob sich das der CEO oder der Patron aneignet, kommt auf die Organisation der Firma an. Man muss nicht verstehen, wie

Neues Qualitätssiegel

Cyberversicherungen sind für die Anbieter oft nicht rentabel. Das lässt sich ändern. Und der **Markt** wächst sehr schnell.

RENÉ FERNANDEZ

Zwei Qualifikationskriterien entscheiden massgeblich über die Versicherbarkeit von Risiken: Eintrittswahrscheinlichkeit und das Schadenausmass. Wird eines der beiden Kriterien mit «tief» bewertet, stehen die Versicherer potenziell vor einem Geschäftsfeld, das langfristig profitabel betrieben werden kann.

Bei der Bewertung von Cyberrisiken mussten die Anbieter feststellen, dass sie zu optimistisch waren. Cybereregnisse kommen sehr häufig vor und bringen verheerende Konsequenzen für die betroffenen Unternehmen. Deshalb arbeiteten die Cyberversicherer in den Jahren 2019 bis 2021 fast flächendeckend unrentabel. Lässt sich längerfristig in einem Geschäftsfeld kein Geld verdienen, steht der Ausstieg des Versicherers aus dieser Sparte kurz bevor.

Der globale Markt verdoppelt sich

Im Gegensatz zu dieser sehr düsteren Ausgangslage zeichnen die globalen Wachstumsprognosen des Cyberversicherungsmarktes ein ganz anderes Bild. Das weltweite Prämienvolumen wird von Imarc aktuell auf etwa 10 bis 12 Milliarden Dollar geschätzt. Eine Verdoppelung des Prämienvolumens wird bereits 2025 erwartet. Wie ist das möglich?

Die Cyberbedrohungslage bleibt unverändert hoch. Neben direkten Angriffen auf Unternehmen stehen auch ganze Lieferketten im Fokus. Gemäss einer repräsentativen Studie der ETH Zürich war jedes fünfte Unternehmen seit 2020 von einem Cyberangriff betroffen. Ransomware-Attacken werden immer komplexer und nehmen kontinuierlich zu. Sie bleiben die grösste Sorge aller Cyberversicherer. Oft greifen die Back-up-Konzepte der Betroffenen nicht und sie sind zu Lösegeldzahlungen gezwungen, um wieder an ihre Daten zu gelangen.

Die spannende Frage ist nicht, ob Lösegelder gezahlt werden, sondern vielmehr, in welcher Qualität die Daten zurückfliessen. Der IT-Dienstleister Sophos (The State of Ransomware 2021) und Veeam (Data Protection Report 2021) publizierten unabhängig voneinander, dass etwa zwei Drittel der verschlüsselten Daten wiederhergestellt werden können. Der Rest geht selbst nach Lösegeldzahlungen verloren. Diese Form von Attacken wird in absehbarer Zeit nicht abnehmen – im Gegenteil: Mit «Ransomware as a Service»-Dienstleistern ist der Zugang zu solcher Schadsoftware so einfach wie nie zuvor.

Deshalb bleibt die Nachfrage nach Cyberversicherungen weiterhin hoch. Die meisten Versicherer haben sich daher gegen einen Ausstieg aus dem Cyberversicherungsmarkt entschieden und nach Wegen gesucht, diese Sparte nachhaltig profitabel zu gestalten.

Weil das Schadenpotenzial (Frequenz multipliziert mit dem Ausmass) derart hoch bewertet wird, genügten die Sanierungsmassnahmen der Versicherer wie die Erhöhung von Prämien und Selbstbehalten sowie eine Reduktion des Deckungsumfangs und der zur Verfügung gestellten Kapazitäten nicht. Wichtiger wurde die Frage: Welche Kundinnen soll man überhaupt versichern?

Der Markt verlangt nach Mindestkriterien, die eine adäquate Risikoqualität der Unternehmen sicherstellen. So werden umfassende Multi-Faktor-Authentifizierung, zeitgemässes Patch-Management und getestete Back-up-Strategien konsequent eingefordert. Aber auch beim Faktor Mensch werden regelmässige Mitarbeiterschulungen sowie eine präventive Vorbereitung auf Cybervorfälle erwartet. Dieses Sicherheitslevel erreichen bei weitem nicht alle Unternehmen, sodass einige ihre Cyberversicherung nicht mehr erneuern konnten.

Auch bei Neuanfragen bleibt die Ablehnungsquote unserer Erfahrung nach mit 30 Prozent hoch. Die Versicherer legten Kriterien fest, um zwischen guten und schlechten Cyberrisiken zu unterscheiden. Kunden mit einer Cyberversicherung sind deshalb sehr gut aufgestellt. Trotz der gegenwärtigen Cyberbedrohungslage war nämlich ein Versicherer bereit, einen Teil des Cyberrisikos zu übernehmen. Damit wird die Cyberversicherung zum Qualitätssiegel für den Umgang mit Cyberrisiken.

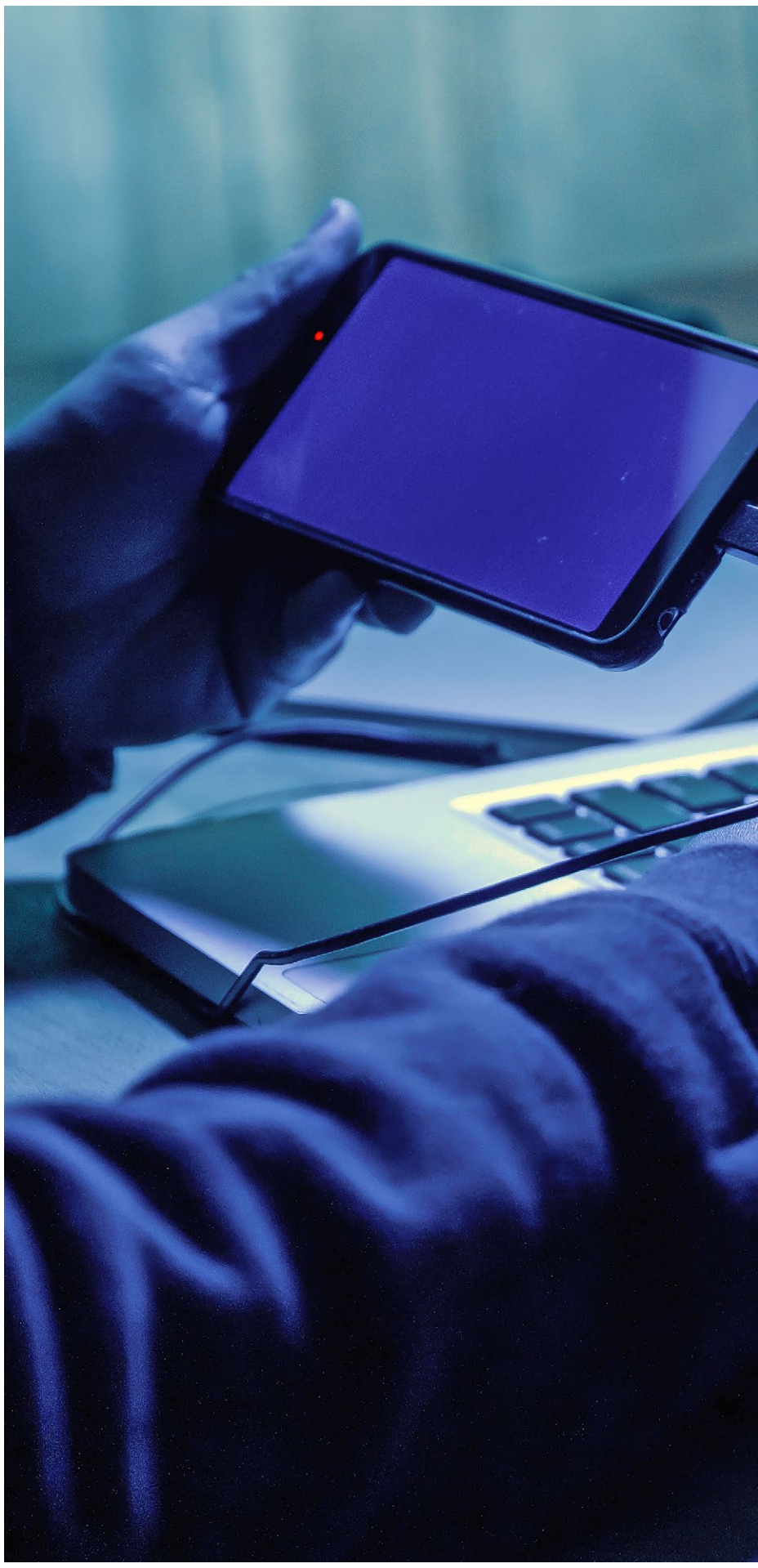
Erste Massnahmen tragen Früchte

Erfreulicherweise haben die ergriffenen Massnahmen 2022 Wirkung gezeigt. Viele Versicherer verzeichnen inzwischen wieder schwarze Zahlen in dieser Versicherungssparte.

Inwiefern diese langersehnte Balance am Cyberversicherungsmarkt von Dauer ist, wird sich zeigen. Fest steht, dass die Unternehmen auch in Zukunft nicht darum herumkommen werden, in ihre Sicherheitsstandards zu investieren. Das Forschungs- und Beratungsunternehmen Gartner Inc. geht davon aus, dass 2025 bereits 80 Prozent der Unternehmen eine Strategie zur Vereinheitlichung von Web-Services, Cloud-Services und privaten Applikationszugriffen über die «Security Service Edge»-Plattformen (SSE) verfolgen und 60 Prozent auf «Zero Trust»-Konzepte umsteigen werden – also weg von einem impliziten vertrauensbasierten Ansatz bei der Erteilung von Zugriffsrechten hin zu einem kontextbasierten und risikoadäquaten Ansatz.

Mit der laufenden Implementierung neuer Regulierungen, wie dem Schweizer Datenschutzgesetz (DSG) und der NIS2-Direktive der EU, in der Cybersecurity-Mindeststandards für die Betreiber kritischer Infrastrukturen festgelegt werden, nehmen auch die rechtlichen Anforderungen an die Unternehmen stetig zu. Es besteht kein Zweifel, dass die Risikoqualität der Unternehmen steigen wird – und das sind durchaus positive Aussichten für die Cyberversicherung.

René Fernandez, Team Leiter Special Risks und Practice Leader Cyber, Kessler & Co, Zürich.



Hacking: Per Definition nicht zwingend strafbar, aber in den Medien häufig im kriminellen Konte

SCHÜTZ

t der Schweiz»

ial, zu einem weiteren Standortfaktor für das ganze Land zu werden.

der Virenschutz funktioniert, aber man muss verstehen, welche Prozesse in welchem Masse von digitalen Leistungen abhängig sind. Wenn aufgrund eines Cyberangriffs beispielsweise nicht mehr auf digital gesteuerte Maschinen zugegriffen werden kann, muss der Geschäftsleitung klar sein, welche Auswirkungen das auf die Prozesse, die Lieferfähigkeit und die Verpflichtungen gegenüber den Stakeholdern hat.

Da höre ich die Unternehmerinnen und Unternehmer im Hintergrund schon argumentieren, dass sie dafür weder Zeit und noch Geld haben …
Drei Viertel der Schweizer Unternehmen machen unter einer halben Million Franken Umsatz pro Jahr. Wenn man das je nach Branche herunterbricht, ergibt es einen Richtwert von 2500 bis 7500 Franken, die man in die Sicherheit investieren sollte. Das ist nicht viel Geld, also muss man gut damit wirtschaften. Und immer, wenn es knapp zu wirtschaften gilt, muss man auch etwas von der Materie verstehen. Insofern wäre das gut investierte Zeit.

Zeit ist auch bei einem Cyberangriff ein kritischer Faktor. Sie haben die Internet-Service-Provider schon kritisiert, weil sie Cyberattacken nicht im erforderlichen Umfang und Tempo an die Kunden melden. Wo sehen Sie da die Gefahr?
Wir kennen Fälle, bei denen eine schnellere Alarmierung seitens des Internet-Service-Providers grössere Schäden beim Kunden hätte reduzieren können. Die Provider sollten ihre Pflichten ernst nehmen und ihre Kunden bestmöglich schützen – und ihnen nicht nur ein Sicherheitspaket als zusätzliche Option zum Kauf anbieten. Ich verstehe, dass das ein Geschäftsmodell für die Provider ist, aber wir müssen uns offensichtlich ernsthaft darüber unterhalten, welche Services zur Grundausstattung dazugehören sollten, damit der Service in der nötigen Sicherheit und Qualität erbracht werden kann.

> «Provider sollten ihre Kunden bestmöglich schützen.»

Alle Anbieter sollten also den gleichen, maximalen Sicherheitsstandard in ihren Grundpaketen offerieren?
Das wäre auch aus strategischer Sicht klug. Wenn die Schweizer Internet-Service-Provider hier einen sehr hohen Standard setzen würden, kann das motivierend und fördernd dafür sein, dass sich mehr Firmen in der Schweiz ansiedeln. Das könnte vermutlich eine positive Spirale in Gang setzen.

Flächendeckende und grundlegende IT-Sicherheit könnte also für das ganze Land zu einem Standortvorteil werden, ähnlich wie es die stabilen politischen Rahmenbedingungen sind, mit denen die Schweiz seit jeher trumpfen kann?
Durchaus, denn wir haben in der Schweiz eine sehr gute Infrastruktur und eine sehr gute Konnektivität, und das macht es auch sehr einfach. Das wird schnell zu einem Standortfaktor, zumal Firmen in Zukunft immer digitaler werden dürften. Und da hat die Schweiz eine gute Chance, zu einem bevorzugten Standort im Bereich Sicherheit zu werden, zumal es ja auch so ein bisschen ein Schweizer Thema ist, denn man vertraut der Schweiz und dem hiesigen Datenschutz.

Der Cyberexperte

Name: Florian Schütz
Funktion: Delegierter des Bundes für Cybersicherheit und Leiter des Nationalen Zentrums für Cybersicherheit (NCSC)
Ausbildung: Master in Computerwissenschaft sowie Master of Advanced Studies in Sicherheitspolitik und Krisenmanagement der ETH Zürich

GETTY IMAGES

ext verwendet, ist das (illegale) Eindringen in Rechnersysteme und in Social Media Accounts.

Cyberrisiken clever absichern

Wer sein Unternehmen schützen will, sollte auf ein **Risikomanagement** setzen, das die Versicherbarkeit von Cyberrisiken im Auge behält.

LEOTRIM JASIQI

Cyberrisiken haben in den vergangenen Jahren eine stärkere strategische und operationelle Bedeutung erlangt. Einerseits ist die Gefahr eines Betriebsunterbruchs durch die zunehmende Digitalisierung bedeutend gestiegen. Hierauf müssen Unternehmen sich vorbereiten. Im Ernstfall können Stunden oder wenige Tage entscheidend dafür sein, ob sich ein Unternehmen von einem Angriff erholen kann oder nicht.

Anderseits nehmen die Anforderungen auf regulatorischer Seite zu. Ein Beispiel hierfür ist das revidierte Datenschutzgesetz, welches per 1. September 2023 in Kraft treten wird. Es verbessert den Schutz persönlicher Daten, gewährt neue Rechte und bringt damit zusätzliche Verpflichtungen für Unternehmen mit sich.

Jeder ist betroffen

Von den operativen und rechtlichen Risiken von Cyberattacken sind zum Beispiel Pensionskassen stark betroffen, denn sie verwalten besonders schützenswerte Daten. Dass sie zu den grössten Investoren am Aktien- und Immobilienmarkt gehören, macht sie zusätzlich zu attraktiven Angriffszielen. Blickt man jedoch auf die Schadenstatistiken, zeigt sich schnell, dass auch andere Geschäftszweige für Attacken attraktiv sind.

Egal, ob Finanz-, Gesundheitswesen oder Industrie – ein Betrieb, der schützenswerte Daten nicht ausreichend absichert, läuft über kurz oder lang Gefahr, einem erfolgreichen Cyberangriff zum Opfer zu fallen. Zusätzlich zur Prävention durch eine widerstandsfähige IT-Infrastruktur wäre daher ein umfassendes Risikomanagement die ideale Ergänzung, um das Reputationsrisiko zu minimieren und eine Ausgangslage zu schaffen, in der eine Cyberversicherung eine finanzielle Absicherung ermöglicht.

Für ein optimales Risikomanagement sollte man sich frühzeitig mit potenziellen Risiken auseinandersetzen. Vereinfacht gesagt, geht es um die Schritte Identifizierung, Quantifizierung, Prävention und Abwälzung, sprich Versicherung. Bei dieser Analyse kann die Unterstützung durch einen externen Berater sinnvoll sein. Gestützt auf Daten und Fakten werden die individuellen Risikomerkmale erhoben und mit Branchen-Benchmarks verglichen. Unter Einbezug der vorgängig umgesetzten Sicherheitsmassnahmen unterstützt die Analyse Versicherer bei der Risikoprüfung und der Prämienkalkulation.

> **Der Faktor Mensch bleibt bei der Cybersicherheit entscheidend.**

Geht es um die Risikoermittlung und Prognose im Bereich Cyber sowie massgeschneiderte Versicherungslösungen, helfen quantitative Methoden. Das individuelle Cyberverlustpotenzial und finanzielle Optimierungen werden dabei anhand einer breiten Schadenstatistik und unter Berücksichtigung der individuellen Risikomerkmale berechnet. So wird es Unternehmen ermöglicht, das Risiko eines Netzwerkausfalls zusätzlich zur Haftung für Datenverletzungen interaktiv zu modellieren und verschiedenen Risikostrategien gegenüberzustellen.

Ganz auf Technologie und Daten dürfen sich Unternehmen aber nicht verlassen. Der Faktor Mensch bleibt bei der Cybersicherheit entscheidend. Entsprechend gehören regelmässige interne Sicherheitstest mit scheinbaren Phishing-Mails zu den Präventionsmassnahmen. So können Schwachstellen identifiziert und entsprechende Sensibilisierungs- und Weiterbildungsmassnahmen geplant werden. Ebenso gehören Pläne für den Erhalt der Geschäftskontinuität sowie Krisenpläne für Zwischenfälle zum Risikomanagement. Diese theoretischen Szenarien sollten für den Ernstfall getestet werden, um die Reaktionszeiten so kurz wie möglich zu halten.

Bleiben Cyberrisiken versicherbar?

Wer eine Cyberversicherung abschliessen will, sollte sich bewusst sein, dass die Versicherer einen gewissen Reifegrad bei der IT-Sicherheit voraussetzen. Zudem sind je nach Unternehmensgrösse bestimmte Mindestselbstbehalte eingeführt worden und das Prämienniveau ist in der letzten Zeit weiter gestiegen. Verständliche Schritte, blickt man auf das stark angestiegene Risiko für einen Versicherungsfall aufgrund einer erfolgreichen Cyberattacke.

Ob Versicherungen auch in Zukunft bereit sein werden, entsprechende Risiken abzusichern, ist offen. Zwar wird aktuell ein Rückgang der durchschnittlichen Ransomware-Zahlungen verzeichnet und die Unternehmen investieren kontinuierlich in die Verbesserung der technologischen Massnahmen. Gleichzeitig ermöglichen künstliche Intelligenz oder Quantencomputing ganz neue Angriffsmethoden. Wie schnell diese Technologien für die Verteidigung nutzbar sein werden, muss sich dann jeweils zeigen.

Mit Blick auf die Dynamik im Bereich Cyber bedeutet ein ganzheitliches Risikomanagement, alle Bausteine permanent im Auge zu behalten, um beim Versagen eines Bausteins auf die Verfügbarkeit eines anderes setzen zu können.

Leotrim Jasiqi, Head of Financial Experience bei WTW Schweiz.