Cyberrisiko – Schweizer KMU nach dem Prinzip Hoffnung. Eine repräsentative Stude des gfs zeigte Ende letzten Jahres Überraschendes: Auf der einen Seite zeigen sich KMU von Cyberrisiken betroffen, scheinen aber auf der anderen Seite recht non-chalant damit umzugehen. Ein grösseres Risikobewusstsein tut not.

VON ROLF THOMAS JUFER*

Das Resultat der repräsentativen gfs-Studie «Cyberrisiken in Schweizer KMU» vom Dezember 2017 überrascht und verunsichert zugleich. Nach drei massiven globalen Cybercrime-Wellen im vergangenen Jahr (WannaCry – NotPetja – Bad Rabbit), wird das Risiko, Opfer eines Angriffs zu werden, von der grossen Mehrheit der Geschäftsführer noch immer als klein bewertet. Die gleiche Studie schätzt jedoch die Betroffenheit der KMU als sehr hoch ein. 23 000 Schweizer Unternehmen sollen von Cybererpressung betroffen und gar rund 210 000 Unternehmen dürften durch Malware wie Viren oder Trojaner behindert worden sein.

Diese Diskrepanz von individueller optimistischer Wahrnehmung und der ernsten Realität gibt zu denken. Werden doch die Schweizer KMU vielfach als Rückgrat der Schweizer Wirtschaft bezeichnet. Verständlich ist die Haltung der Unternehmen zwar, da das Kerngeschäft mit den eigenen Kunden und die Fokussierung auf neue Aufträge näherliegen als die komplexen Prozesse zur Bewältigung der IT-Sicherheit.

Cyberbedrohungen: Wir stehen erst am Anfang. Unter der überwiegenden Mehrheit der Experten besteht Konsens, dass die Entwicklung der letzten Jahre im Bereich der Cyberrisiken und der Cyberkriminalität erst den Beginn einer grossen Bedrohung darstellt. Ebenso ist klar, dass auch mit hohen Investitionen in die IT-Sicherheit und die Sensibilisierung der Mitarbeitenden nie ein hundertprozentiger Schutz erreicht werden kann. Die kriminelle Energie und Dynamik der Angreifenden sowie die massiv zunehmende Vernetzung und Komplexität von Systemen sind nur zwei Gründe dafür.

Die letztes Jahr entdeckten und am 3. Januar 2018 veröffentlichten Hard- bzw. Softwarelücken «Meltdown» und «Spectre» lassen nun auch den letzten IT-Sicherheitsoptimisten aufhorchen und hoffentlich handeln. Denn über ein halbes Jahr nach Feststellung der gravierenden Sicherheitslücken ist noch immer keine nachhaltige Lösung verfügbar.

Für Unternehmen stellt sich bei dieser Ausgangslage konkret die Frage nach den unternehmensspezifischen **Cyberrestrisiken**. Diese lassen sich heute schätzen und auch passgenau nach Branche und Grösse in den Versicherungsmarkt transferieren.

Verschärfung der Datenschutzgesetze. Die eingangs zitierte gfs-Studie zeigt auf, dass knapp die Hälfte der befragten Firmen Geschäftsgeheimnisse und drei von fünf Firmen personenbezogene Kundendaten verwalten. Schützenswerte Daten, die im Rahmen der neuen Gesetzgebung besonderer Behandlung bedürfen.

Die Erfahrung zeigt, dass der Datenschutz bei grösseren Unternehmen heute ganz klar ein Verwaltungsratsthema ist. Dabei geht es nicht nur um die Reputation des Unternehmens – verstärkt steht auch die Reputation der einzelnen Verwaltungsräte respektive der Geschäftsleitungsmitglieder selbst im Fokus.

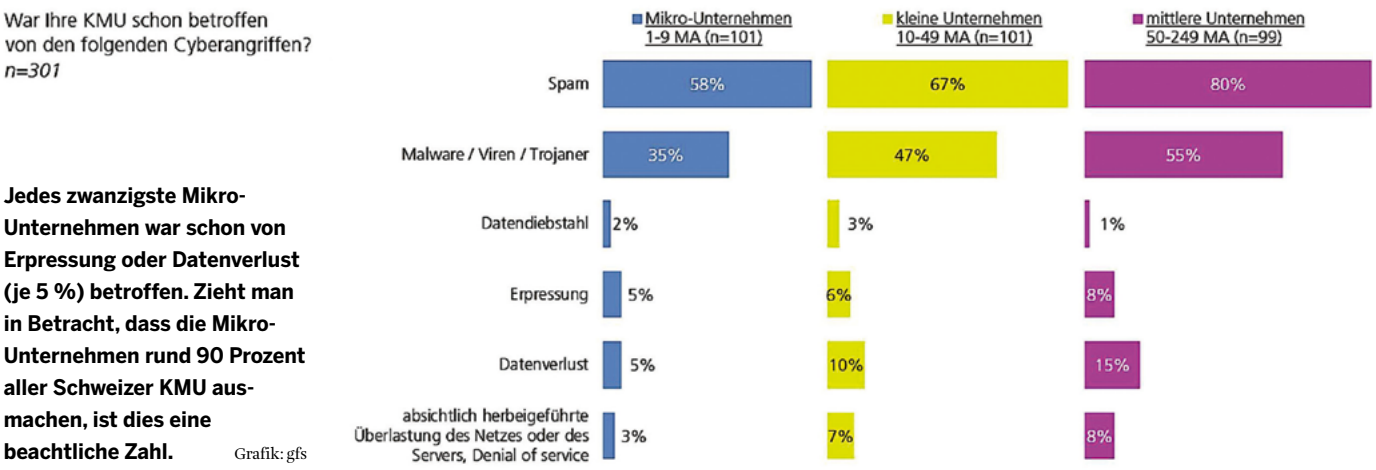
Die aktuellen Verschärfungen der Datenschutzgesetzgebung auf europäischer Ebene und der Vorentwurf zum Datenschutzgesetz in der Schweiz haben auch zur Sensibilisierung beigetragen. Die vorgesehenen Strafen bei fahrlässigem oder gar vorsätzlich destruktivem Umgang mit Daten können für Unternehmen schmerzhafte finanzielle Folgen haben. Die EU-Datenschutz-Grundverordnung tritt bereits am 18. Mai 2018 in Kraft.

JEDES DRITTE KMU BETROFFEN

Im vergangenen September befragte das Markt- und Sozialforschungsinstitut gfs-zürich in einer repräsentativen Umfrage 300 CEO von Schweizer KMU zum Thema Cyberrisiken. Die nach wissenschaftlichen Methoden erfolgte Auswahl der KMU erlaubt es, die Resultate auf die Gesamtheit der Schweizer KMU (2015: 580 000) zu übertragen. Die Befragung wurde im Auftrag des Schweizerischen Versicherungsverbands (SVV), der Schweizerische Vereinigung für Qualitäts- und Management-Systeme (SQS), dem Dachverband ICTswitzerland und der Information Security Society Switzerland (ISSS) in Zusammenarbeit mit dem Informatiksteuerungsorgan des Bundes (ISB) und der Expertenkommission des Bundesrates zur Datenbearbeitung und Datensicherheit durchgeführt.

Die wichtigsten Ergebnisse

- Die IT muss kontinuierlich funktionieren: Rund 62 % der Befragten bewerten das kontinuierliche Funktionieren der IT als sehr wichtig für ihren Betrieb.
- Mehr als ein Drittel der KMU sind von Cyberattacken betroffen: Auf Basis der 300 befragten KMU kann die Anzahl der von Erpressung betroffenen Firmen schweizweit auf 23 000 (4 %) geschätzt werden. Ungefähr 209 000 Unternehmen (36 %) dürften von Malware wie Viren oder Trojanern betroffen gewesen sein.
- Das Risiko von Cyberangriffen wird stark unterschätzt: Das Risiko, Opfer eines Cyberangriffs zu werden, wird als tief eingeschätzt. Einen Tag lang ausser Gefecht gesetzt oder gar in der Existenz gefährdet zu werden, empfinden nur 10 % bzw. 4 % als grosse oder sehr grosse Gefahr. Über die Hälfte der befragten Geschäftsführer/-innen (56 %) fühlt sich gut bis sehr gut vor Cyberangriffen geschützt.
- Der Schutz vor Cyberangriffen ist ungenügend: Nur 60 % der Befragten geben an, Grundschutzmassnahmen wie Malware-Schutz, Firewall, Patch-Management und Back-up voll und ganz umgesetzt zu haben. Systeme zur Erkennung von Cybervorfällen wurden nur von jedem fünften Unternehmen vollständig eingeführt. Prozesse zur Behandlung von Cybervorfällen nur noch von 18 % der befragten Unternehmen, Mitarbeiterschulungen über den sicheren Gebrauch von IT lediglich von 15 %.



Jedes zwanzigste Mikro-Unternehmen war schon von Erpressung oder Datenverlust (je 5 %) betroffen. Zieht man in Betracht, dass die Mikro-Unternehmen rund 90 Prozent aller Schweizer KMU ausmachen, ist dies eine beachtliche Zahl. Grafik: gfs

Cybersicherheit – die letzte Meile konsequent gehen. Im letzten Schritt der ganzheitlichen Behandlung von Cyberrisiken sollten sich Unternehmen wie bereits erwähnt der Cyberrestrisiken bewusst werden. In der Praxis hat sich gezeigt, dass der im Funk RiskLab entwickelte Cyber Risk Calculator (Funk CRC) die Unternehmensleitung wirksam in diesem Prozess unterstützt. Auf Basis konkreter unternehmensspezifischer Informationen werden Schadenswerte ermittelt (Betriebsunterbruch, Kosten für Wiederherstellung, Rechtsberatung und Forensik sowie realistische Diebstahl- und Erpressungssummen usw.). In einem Cyberrisikodialog werden die Resultate zusammen mit der Unternehmensleitung detailliert überprüft und gegebenenfalls noch angepasst.

Die Unternehmensleitung erhält so eine Entscheidungsgrundlage, ob und, wenn ja, zu welchen Konditionen die Cyberrestrisiken in den Versicherungsmarkt transferiert werden sollen. Diese letzte Meile ist für die Verantwortlichen elementar. Nur so kann im Schadenfall dargelegt werden, ob das Management die Prozesse im Rahmen des Risikomanagements vollständig abgearbeitet hat und der Entscheid «Versicherung – ja oder nein» gut dokumentiert wurde.

Die Erfahrung der letzten beiden Jahre zeigt, dass der Zeitaufwand für Unternehmen für diese letzte Meile in der Regel in engen Grenzen gehalten werden kann. Auf Basis von zwei Fragebogen werden die benötigten Daten erhoben und in zwei Sitzungen à ca. zwei Stunden können die relevanten Entscheidungsgrundlagen erarbeitet werden.

Beschränktes Angebot an intelligenten Cyberversicherungen für Unternehmen. Bei Cyberversicherungen sind Standardprodukte ebenso wenig zielführend wie pauschale, undifferenzierte Versicherungssummen. Erst seit kurzer Zeit sind umfassende und kundenfreundliche Versicherungslösungen für Unternehmen erhältlich.

Prüfenswerte Versicherungslösungen haben aufgrund unserer Erfahrung sowohl Versicherungs- als auch Service-Elemente. Bei den Versicherungselementen ist darauf zu achten, dass nicht nur klassische Schäden durch Cyberkriminalität (Diebstahl, Erpressung etc.) gedeckt sind, sondern auch Schäden, die durch unsachgemässe Bedienung von Steuerungssystemen durch eigene Mitarbeitende entstanden sind. Ebenso ist es zunehmend von Bedeutung, dass auch Cloud-Lösungen in der Versicherungsdeckung eingeschlossen sind, da immer mehr Unternehmen Elemente der IT in externe Clouds auslagern.

Zentrale Service-Elemente beinhalten primär ein gut verständliches Wording (AVB), welche die Bedürfnisse des Unternehmens in den Mittelpunkt stellen. In diesem Zusammenhang ist die «Beweislastumkehr» von zentraler Bedeutung. Cyberangriffe können komplexe technische Vorgänge darstellen, die selbst umgehend angeforderte Forensiker nur teilweise nachvollziehen können. Mit der erwähnten «Beweislastumkehr» liegt die Beweislast (Cyberangriff ja oder nein) beim Versicherer und nicht beim Kunden. Auch eine bewährte Cyber-Notfallorganisation muss der Versicherer glaubhaft darstellen können. Es geht dabei um organisatorische Elemente (Notfallnummer, Reaktionszeit etc.) sowie die richtigen Partner. Wir legen als beratende Broker Wert darauf, dass auch die bestehenden IT-Security-Partner des Unternehmens im Cyberkrisenteam eine wichtige Rolle erhalten. So ist sichergestellt, dass lokales Know-how schnell verfügbar ist und nicht unbekannte «Consultants» wichtige Zeit verlieren.

Höchste Diskretion gefordert. Sollte sich das Unternehmen letztlich für eine Cyberversicherung entscheiden, so ist mit dieser Information höchst vertraulich umzugehen. Da Cyberversicherungen in der Regel Leistungen bei Erpressung beinhalten, ist die Information bezüglich dem Vorhandensein einer solchen Versicherung nur dem kleinstmöglichen Kreis innerhalb des Unternehmens zugänglich zu machen.

*

ROLF THOMAS JUFER
ist Partner und Mitglied der Geschäftsleitung der Funk Insurance Brokers AG. Er ist seit 2013 als Leiter von Marketing und Vertrieb für die Bereiche Marktentwicklung, Markenpositionierung, Neukundengewinnung und das Funk RiskLab verantwortlich. **www.funk-gruppe.ch**