Rolf Thomas Jufer
Partner und Mitglied der Geschäftsleitung
der Funk Insurance Brokers AG

Cyberrisiken ganzheitlich angehen

Immer mehr Unternehmen nehmen Cyberrisiken ernst und wappnen sich gegen Hackerangriffe. Verwaltungsrat und Geschäftsleitung sind besonders gefordert. Wollen sie doch einerseits die Chancen der Digitalisierung optimal nutzen und andererseits Angriffe wirksam abwehren.

Digitalisierung, Industrie 4.0, IoT - Begriffe, die eine neue Epoche für die Gesellschaft und Wirtschaft eingeläutet haben und so auch den Unternehmensalltag massgeblich prägen. Es geht für Unternehmen einerseits darum, die Chancen dieser Entwicklung optimal zu nutzen und sich andererseits auch den Risiken der dynamisch voranschreitenden Vernetzung von Menschen, Maschinen und Prozessen zu stellen.

Eine komplexe Aufgabenstellung, die zwar einen Projektanfang aber kein Projektende kennt. Die kontinuierliche Auseinandersetzung mit den neusten technischen Mitteln der Cyber-Abwehr/Cyber-Security als auch das Antizipieren von künftigen Angriffsformen (Threat Intelligence) gehören im Rahmen des IT-Risikomanagements ebenso dazu, wie das konsequente Umsetzen von operativen Massnahmen und das Durchführen von Kontrollen.

Kontinuierlicher Prozess mit spezialisierten Partnern

Etwas konkreter heisst das, regelmässig die Robustheit der eigenen Unternehmung zu prüfen, Mitarbeitende kontinuierlich zu sensibilisieren, die IT-Sicherheit permanent zu optimieren sowie sich im Rahmen und Zyklus des Cyber-Risikomanagements kontinuierlich ein Bild über das finanzielle Cyber-Restrisiko zu machen. Dieses Cyber-Restrisiko ist dann zu bewerten und gegebenenfalls in den Versicherungsmarkt zu transferieren.

Die Funk Gruppe beschäftigt sich seit Jahren mit Cyberrisiken. Via ihr internationales Netzwerk «The Funk Alliance» war sie am Puls der ersten grossen Fälle von Cyber-Kriminalität in den USA. «In unserer Branche herrschte damals grosse Unsicherheit», erinnert sich Rolf Th. Jufer, Geschäftsleitungsmitglied von Funk Insurance Brokers in der Schweiz. «Weder wir noch die Versicherer hatten Erfahrungen, wie mit diesem Thema umzugehen ist. Aber uns war sofort klar, da kommt ein neues und sehr komplexes Risiko auf unsere Kunden zu». Erst seit kurzer Zeit sind nun umfassende und kundenfreundliche Versicherungslösungen im europäischen Raum erhältlich, mit der die Kunden heute unterschiedliche Bedürfnisse abdecken können. Doch Versicherung ist nur ein kleiner aber wichtiger Teil der Lösung. Weil Cyberrisiken Unternehmen in ihrer Gesamtheit durchdringen, braucht es zusätzliche Spezialisten aus den Bereichen Informatik und Recht.

Nur so lässt sich beurteilen, ob das IT-System sowie die Aufbau- und Ablauforganisation gängigen Sicherheitsanforderungen genügen und ob der Umgang mit dem Datenschutz im Einklang mit der Rechtsordnung steht. Aus diesem Grund arbeitet Funk in der Schweiz im Cyber-Risikomanagement mit **InfoGuard** und **MME** zusammen. InfoGuard ist ein Spezialist für Cyber-Security. Die Anwaltskanzlei MME ist u.a. auf Datenschutz und IT-Recht spezialisiert und vergibt das Zertifikat **«ePrivacy»** in der Schweiz. Gemeinsam stehen die drei Partner für einen umfassenden und stringenten Beratungsansatz im Umgang mit Cyberrisiken. Ebenso wichtig wie erfahrene Partner ist, was sich allgemein im Risikomanagement bewährt. Der Erfolg hängt davon ab, dass sich die Unternehmensleitung der Problematik bewusst ist und sich dafür zuständig fühlt.

Mehrheit der Unternehmen mit Handlungsbedarf

Gemäss einer Unternehmensumfrage im deutschsprachigen Raum vom Frühjahr 2017 sind grosse börsenkotierte Unternehmen durchaus Cyberfit. Kleine und mittlere Unternehmen hinken jedoch hinterher. Bemerkenswert ist, dass nur ein Drittel der Entscheider von mittleren Unternehmen der Meinung ist, im Fokus von gezielten Hackerangriffen zu sein. Die meisten finden ihr Unternehmen entweder zu klein oder zu uninteressant für Kriminelle. Diese Haltung kommt Rolf Th. Jufer bekannt vor. Bereits im Jahr 2013 organisierte Funk Kundenevents mit Live-Hacking. «Diese Demonstrationen kamen zwar gut an», erinnert sich Jufer. Am Ende bezweifelten viele Unternehmer jedoch, dass Hacker sich ihr Unternehmen aussuchen würden. «Wären wir ein lohnenswertes Ziel, hätte man uns doch schon längst angegriffen», so der Tenor.

Auch die IT-Spezialisten der InfoGuard haben diese Aussagen früher oft gehört. In den letzten zwei Jahren hat aber ein Umdenken stattgefunden. Dazu hat die Publizität rund um Hackerangriffe sicher das ihre dazu beigetragen. Das Outing von Edward Snowden wirkte nachhaltig. Mit den Enthüllungen zu den Cyberaktivitäten der amerikanischen Geheimdienste war das Thema definitiv in den Chef-Etagen angekommen. Interessierten sich früher fast nur IT-Leute für das Thema und liefen damit intern oft ins Leere, wird InfoGuard heute aktiv von Verwaltungsräten oder Unternehmensinhabern angefragt, um die Cybersicherheit im Unternehmen zu beurteilen.

Verschärfung der Datenschutzgesetze

Die Erfahrung von MME zeigt, dass der Datenschutz 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 selbstverständlich auch zur Sensibilisierung auf höchster Stufe beigetragen. Die vorgesehenen Strafen bei fahrlässigem oder gar vorsätzlich destruktivem Umgang mit Daten, können für Unternehmen schmerzhafte finanzielle Folgen haben.

Cyber-Krisenmanagement

Unternehmen müssen sich bewusst sein, dass es trotz allen präventiven Massnahmen und hohen Investitionen keine 100%-ige IT-Sicherheit gibt. Zu dynamisch organisieren sich die Angreifer und zu kreativ agieren sie. So hat der globale Umsatz der Cyberkriminellen bereits den Umsatz des globalen Drogenhandels übertroffen.

Trotz aller Sensibilisierungen und Warnungen wird es immer Mitarbeitende geben, die verdächtige Mails samt Anhängen öffnen («einer klickt immer»). Ferner ist insbesondere bei gezielten Cyberangriffen (z.B. Social Engineering) eine Abwehr sehr anspruchsvoll. Deshalb sollte auch der Notfall im Rahmen des Business Continuity Managements (z.B. IT-Systemausfall verursacht durch eine Ransomware) und des Krisenmanagements (z.B. Diebstahl von sensiblen Kundendaten) vorbereitet und geübt werden.

Cybersicherheit – die letzte Meile konsequent gehen

Im letzten Schritt der ganzheitlichen Behandlung von Cyberrisiken im Rahmen des Risikomanagements sollten Unternehmen sich den Cyber-Restrisiken 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). In einem Cyber-Risikodialog wird das Resultat zusammen mit der Unternehmensleitung detailliert überprüft und gegebenenfalls noch angepasst.

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

Rolf Thomas Jufer

Rolf Thomas Jufer ist Partner und Mitglied der Geschäftsleitung der Funk Insurance Brokers AG in der Schweiz. Er ist seit 2013 für Marketing, Vertrieb und das Funk RiskLab verantwortlich. Zuvor leitete Rolf Jufer die Tochtergesellschaften von zwei US-Beratungs- und Brokergesellschaften in der Schweiz nachdem er für einen Schweizer Lebensversicherungskonzern die Märkte Nordamerika, UK und Irland verantwortete.

Funk in der Schweiz rät nicht nur seinen Kunden, sich gegen Cyberrisiken zu wappnen, sondern handelt auch selber danach. Der Risikomanagement-Berater und Versicherungsbroker hat sein Kundenportal nach «ePrivacy» zertifizieren lassen. Das Assessment erfolgte durch InfoGuard und MME. Das Label hat seinen Ursprung in Deutschland und orientiert sich an den EU-Richtlinien. Auch in der Wirtschaft wächst das Bedürfnis nach Klarheit darüber, welche Anbieter im Umgang mit Cyberrisiken und dem Thema Datenschutz zeitgemässen Anforderungen genügen. Während InfoGuard das technische Gutachten macht, fokussiert MME auf rechtliche Faktoren (Datenschutz). Weil die EU-Richtlinien und auch die Datenschutzgesetzgebung in der Schweiz verschärft werden, ist zu erwarten, dass auch die Bedeutung von «ePrivacy» zunimmt.

Der inhabergeführte und unabhängige Versicherungsbroker Funk ist in der Schweiz seit 30 Jahren aktiv. Funk Insurance Brokers AG ist die Schweizer Organisation der 1879 gegründeten Funk Gruppe, Hamburg. Das in der 5. Generation geführte Familienunternehmen ist der grösste eigenständige Risikoberater und Versicherungsbroker im deutschsprachigen Raum. In den Niederlassungen Basel, Bern, Luzern, St. Gallen sowie Zürich beschäftigt Funk über 80 Spezialisten verschiedenster Fachrichtungen. Funk in der Schweiz zeichnet sich durch Nähe zum Kunden, Kompetenz und Begeisterung bei Bewertung und Management von Risiken für Unternehmen aus. Über ihr Brokernetzwerk Funk Alliance stellt Funk die weltweite Betreuung ihrer Kunden im gesamten betrieblichen Risiko-, Vorsorge- und Versicherungsmanagement sicher und bietet nationalen und internationalen Unternehmen einen individuellen Service aus einer Hand. Funk ist zertifiziert nach ISO 9001 und betreibt das erste Kundenportal der Schweiz mit dem ePrivacyseal (IT-Security und Datenschutz nach EU DSGVO).