

# CH-D

## WIRTSCHAFT

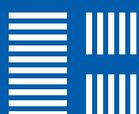
108. Mitgliederversammlung der Handelskammer Deutschland-Schweiz

Aktuelle Rechts- und Steuerthemen Deutschland-Schweiz

Corona-Pandemie: Ausgewählte Themenschwerpunkte

**Unternehmen wollen Transparenz  
zu finanziellen Cyber-Restrisiken**

S. 18



Handelskammer  
Deutschland Schweiz

Wir wissen,  
was Sie wissen müssen

# UNTERNEHMEN WOLLEN TRANSPARENZ ZU FINANZIELLEN CYBER-RESTRISIKEN

Viele Unternehmen kennen aktuell die finanziellen Konsequenzen eines Cyberzwischenfalls nicht. Funk hat einen konsistenten Prozess entwickelt, um die potenziellen und versicherbaren finanziellen Risiken zu bewerten. So entsteht Transparenz für die Unternehmensleitung zu einem bisher eher diffusen Risiko. Die Funk Gruppe ist seit Januar ein neuer Premiumpartner der Handelskammer Deutschland-Schweiz.

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 trotz der hohen Investitionen in die IT-Sicherheit und der regelmässigen Sensibilisierung der Mitarbeitenden ein hundertprozentiger Schutz nie erreicht werden kann. Die kriminelle Energie und Dynamik der Angreifenden sowie die massiv zunehmende Vernetzung und Komplexität von Systemen sind nur zwei Gründe dafür. Für Unternehmen stellt sich bei dieser Ausgangslage konkret die Frage nach den unternehmensspezifischen Cyber-Restrisiken. Diese lassen sich heute berechnen und passgenau nach Branche und Grösse in den Versicherungsmarkt transferieren.

## Kontinuierlicher Prozess mit spezialisierten Partnern

Best Practice aus heutiger Sicht kann man vereinfacht wie folgt zusammenfassen:

- die technische IT-Sicherheit kontinuierlich optimieren
- Datenschutzkonformität herstellen und erhalten
- sich in der IT und in dem Geschäftsbetrieb auf den Ernstfall vorbereiten (BCM und Krisenmanagement)
- die Mitarbeitenden kontinuierlich sensibilisieren, sowie
- im Rahmen des Cyber-Risikomanagements das finanzielle Cyber-Restrisiko regelmässig quantifizieren und bei Bedarf transferieren.

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.

Um diesen umfassenden Service Unternehmen zugänglich zu machen, arbeitet Funk in der Schweiz, Deutschland, Österreich und Liechtenstein mit spezialisierten Partnern zusammen.

## IT-Sicherheit – die letzte Meile konsequent gehen

Im letzten Schritt der ganzheitlichen Behandlung von Cyberrisiken sollten sich Unternehmen 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 usw.). In einem Cyber-Risikodialog 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 Cyber-Restrisiken in den Versicherungsmarkt transferiert werden können. 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 Jahre zeigt, dass der Zeitaufwand für Unternehmen für diese letzte Meile in der Regel in engen Grenzen gehalten werden kann. Auf Basis von zwei Fragebögen werden die benötigten Daten erhoben und die relevanten Entscheidungsgrundlagen in maximal zwei Sitzungen erarbeitet.

## Verschärfung der Datenschutzgesetze

Eine aktuelle Studie der gfs zeigt auf, dass knapp die Hälfte der befragten Firmen Geschäftsgeheimnisse und drei von fünf Firmen personenbezogene Kundendaten verwalten. Dies sind schützenswerte Daten, die im Rahmen der neuen Gesetzgebung besonderer Behandlung und besonderen Schutz bedürfen. Datenschutz ist damit zu einem Verwaltungsratsthema geworden. 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 aktuelle Verschärfung der Datenschutzgesetzgebung hat aber auch zur Sensibilisierung beigetragen. Die vorgesehenen Strafen bei fahrlässigem oder gar vorsätzlich destruktivem Umgang mit Daten, können für Unternehmen schmerzhaft finanzielle Folgen haben.

## Beschränktes Angebot an zweckmässigen Cyberversicherungen für Unternehmen

Bei Cyber-Versicherungen sind Standardprodukte ebenso wenig zielführend wie pauschale, undifferenzierte Versicherungssummen. Umfassende und kundenfreundliche Versicherungslösungen für Unternehmen sind zwar erhältlich, grundsätzlich jedoch nur für Unternehmen mit guter Cyberfitness.

Prüfungswerte Versicherungslösungen haben aufgrund der Erfahrung von Funk sowohl Versicherungs- als auch Serviceelemente. 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 Cloudlösungen in der Versicherungsdeckung eingeschlossen sind, da immer mehr Unternehmen Elemente der IT in externe Clouds auslagern.

Zentrale Serviceelemente beinhalten primär ein gutes 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 Risikoberater und Versicherungsspezialisten Wert darauf, dass auch die bestehenden IT-Security-Partner des Unternehmens im Cyber-Krisenteam eine wichtige Rolle erhalten. So ist sichergestellt, dass lokales Know-how schnell verfügbar ist und nicht unbekannt «Consultants» wichtige Zeit verlieren.

Sollte sich das Unternehmen letztlich für eine Cyber-Versicherung entscheiden, so ist mit dieser Information höchst vertraulich umzugehen. Da Cyber-Versicherungen in der Regel Leistungen bei Erpressung beinhalten, ist die Information bezüglich dem Vorhandensein einer solchen Versicherung nur dem kleinst möglichen Kreis innerhalb des Unternehmens zugänglich zu machen.

## Über Funk

### Tradition, Werte und Verantwortung

Rund 140 Jahre erfolgreiche Unternehmensgeschichte, Eigenständigkeit, eine gewachsene Unternehmenskultur und die Fähigkeit zu langfristigem Denken und Handeln prägen das Familienunternehmen Funk in der fünften Unternehmensgeneration. In dem Bestreben, Funk als Familienunternehmen zu erhalten und weiterzuentwickeln, setzt Funk auf



Die Geschäftsleitung der Funk Schweiz am Sitz in Zürich: Rolf Th. Jufer, Martin Vögeli, Urs A. Bleisch, VRP und CEO (v.l.n.r.)

die Beständigkeit ihrer Werte und auf eine starke Unternehmenskultur. Die Entscheidungen werden mit Blick auf Kontinuität und die daraus resultierenden langfristigen Strategien gefällt.

### Internationalität liegt in der Funk DNA

Die 1879 in Berlin gegründete Funk Gruppe mit Sitz in Hamburg ist mit über 1'300 Mitarbeitenden in Europa der grösste eigenständige Risikoberater und Versicherungsbroker im deutschsprachigen Raum. Mit dem eigenen Brokernetzwerk «The 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.

Derzeit betreut Funk mit 35 eigenen Büros und der Unterstützung durch die Funk Alliance eine Vielzahl internationaler Kunden in über 100 Ländern. Die internationalen Aktivitäten haben seit jeher grosse Bedeutung für Funk. Mittlerweile machen sie mehr als ein Drittel der Geschäftsaktivitäten aus. Um dem kontinuierlichen Wachstum des internationalen Geschäfts gerecht zu werden, stellt Funk den nachhaltigen Ausbau der Netzwerk-

struktur und die fortlaufende Entwicklung integrierter, kundenspezifischer IT- und Reporting-Tools klar in den Fokus der Investitionsstrategie. Mehr Informationen zum internationalen Netzwerk von Funk: [www.funk-gruppe.ch/de/international/funk-alliance/](http://www.funk-gruppe.ch/de/international/funk-alliance/)

### Funk in der Schweiz und Liechtenstein

Seit über 30 Jahren ist die Funk Gruppe durch die Funk Insurance Brokers AG mit einer Ländergesellschaft in der Schweiz vertreten. Fünf Niederlassungen (Basel, Bern, Luzern, St. Gallen und Zürich) mit 90 Mitarbeitenden bilden das Schweizer Unternehmen. Das Management ist am Unternehmen beteiligt und entwickelt die Gesellschaft zum führenden Dienstleister in der Schweiz. Dies mit Kundennähe, Qualität und Begeisterung für innovative Lösungen. Die Ländergesellschaft in Vaduz, Liechtenstein, wurde 2018 gegründet und ist eine Tochtergesellschaft der Schweizer Holding.

Die Parallelen von Funk und der Handelskammer sind offensichtlich. Die starke Präsenz in Deutschland und der Schweiz sowie die weit über 100-jährige Geschichte beider Organisationen sprechen für eine erfolgreiche Partnerschaft.