«Cyberrisiken sind heute Chefsache»

Funk bietet mit Funk CyberSecure einen innovativen und individuell anpassbaren Versicherungsschutz gegen Cyberrisiken und arbeitet mit hochkarätigen Sicherheitsspezialisten zusammen, die Unternehmen beim Schliessen von Sicherheitslücken unterstützen.

Thomas Meier, CEO InfoGuard

Dr. Martin Eckert, Partner MME

Die Funk Gruppe beschäftigt sich seit Jahren mit Cyberrisiken. Über 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, GL-Mitglied von Funk Insurance Brokers. «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 Versicherungslösungen in der Schweiz erhältlich, womit die Kunden heute unterschiedliche Bedürfnisse abdecken können. Doch das sei nur ein Teil der Lösung, sagt Jufer. Weil Cyberrisiken Unternehmen in ihrer Gesamtheit durchdringen, brauche es zusätzlich 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 im Cyber Risikomanagement mit InfoGuard und MME zusammen. InfoGuard ist ein Spezialist für Cyber-Security aus Baar/ZG und Bern. Die Anwaltskanzlei MME mit Standorten in Zürich und Zug ist u.a. auf Datenschutz und IT-Recht spezialisiert und vergibt das Zertifikat «ePrivacy» (siehe Kasten). Gemeinsam stehen die drei Partner für einen umfassenden und wirkungsvollen Ansatz im Umgang mit Cyberrisiken. Der Erfolg hängt massgeblich davon ab, dass sich die Unternehmensleitung der Problematik bewusst ist und sich dafür zuständig fühlt.

Gemäss einer Umfrage im deutschsprachigen Raum von Ende März 2017 ist das bei grossen Börsenkotierten durchaus der Fall. Kleine und mittlere Unternehmen hinken jedoch hinterher. Bemerkenswert ist, dass nur ein Drittel der mittelständischen Entscheider der Meinung ist, Ziel von Hackerangriffen werden zu können. Die meisten finden ihr Unternehmen entweder zu klein oder zu uninteressant für Cyberkriminelle. Diese Haltung kommt Rolf Th. Jufer bekannt vor. Bereits im Jahr 2013 organisierte Funk Kundenevents mit Live-Hackingsimulationen. «Diese Demonstrationen kamen zwar gut an», erinnert sich Jufer. Am Ende bezweifelten viele KMU-ler jedoch, dass Hacker sich ihr Unternehmen aussuchen würden. «Wären wir ein lohnenswertes Ziel, hätte man uns doch schon längst angegriffen», so der Tenor.

Thomas Meier, CEO InfoGuard, als Security-Spezialist müssen Ihnen bei solchen Aussagen die Haare zu Berge stehen. Wie steht es um das Bewusstsein für Cyberrisiken?

«Solche Aussagen haben wir früher auch 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 wirkt nachhaltig. Damit ist 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, fragen uns heute Geschäftsleitungen, wie wir die Cybersicherheit in ihrem Unternehmen beurteilen.»

InfoGuard SWISS CYBER SECURITY

MME

funk

Geht es um Verantwortung und rechtliche Fragen, interessiert das offenbar die Chefs. Dr. Martin Eckert, Partner MME, wie beurteilen Sie die Entwicklung aus Rechts- und Governance-Optik?

«Das ist heute ganz klar ein Verwaltungsratsthema und wird dort auch aufgenommen, nicht zuletzt wegen der Reputation. Die Frage ist letztlich, auf welcher Ebene bzw. in welcher Division des Unternehmens das Thema abgehandelt wird. Oft hört man «Das ist ein IT-Problem» oder «Wenn was passiert, fragen wir einen Juristen». Die Zuordnung ist tatsächlich nicht ganz einfach – Stichwort Governance. Während die Informatik früher etwas für Techniker im Backoffice war, ist sie heute der Kern der Geschäftstätigkeit. Ohne IT läuft nichts mehr.»

Cyberrisiken sind relativ neu, sehr komplex und unterscheiden sich je nach Firma oder Branche zum Teil fundamental. Standardmässig ist das versicherungstechnisch nicht so einfach abzubilden. Was gilt bei Erpressung, wenn noch gar kein Schaden eingetreten ist? Oder was ist, wenn Mitarbeiter irrtümlich oder vorsätzlich Cyberschäden verursachen? Oder bei Cyber-Datendiebstahl? Die Versicherungslösung, die Funk mit international tätigen Versicherern entwickelt hat und die weltweit gilt, lässt sich an unterschiedliche Bedürfnisse anpassen. Sie kann auch in bestehende Deckungen integriert werden. «Am Ende», so Rolf Th. Jufer, «ist unsere Deckung aber nur ein wichtiges Puzzleteil. Entscheidend ist es, die Kunden direkt einzubeziehen. Hier kommen unsere Partner ins Spiel. Sie sind die Spezialisten für Cyberrisiken. Sie untersuchen, wie gut ein Unternehmen aufgestellt ist bzw. was alles schief laufen kann. Nur so kann das zu versichernde Restrisiko angemessen abgebildet werden.»

Thomas Meier, bei einem Assessment schauen Sie sich die IT-Infrastruktur sowie die Prozesse und die Expertise der Mitarbeitenden an. Was untersuchen Sie konkret?

«Zentral sind die Fähigkeiten und Erfahrungen der Mitarbeitenden im bewussten Umgang mit der Technologie. Wie und wo surft jemand im Web. Was kann man problemlos machen und wovon lässt man besser die Finger – auch im Einsatz mit mobilen Geräten, wenn man unterwegs ist. Dann schauen wir uns die Organisation und Prozesse an. Wie wird Cyber Security im Unternehmen gelebt? Was passiert bei einem Ereignis? Wer ist wofür zuständig und unternimmt wann was? Der dritte Teil unseres Assessments schliesslich ist sehr technisch. Wir starten einen simulierten Hackerangriff, um die Schwachstellen im System zu finden. Nach einem solchen «Penetration-Test» empfehlen wir dem Kunden angemessene Gegenmassnahmen.»

Und wo hapert es am meisten?

«Das kommt ganz darauf an. Bei einem Pen-Test machen wir ganz gezielte Angriffe auf das System und die Software. Bei umfassenden Angriffen auf ein Unternehmen suchen wir aber nach dem schwächsten Glied im ganzen Abwehrdispositiv – so wie das ein richtiger Hacker macht. Komme ich via Webshop am einfachsten ins System oder mit Social Engineering, also indem ich versuche, auf arglistige Weise Mitarbeitende einzuspannen, um Trojaner oder mich selber ins System einzuschleusen. Die Kombination Mensch und Technik verspricht am meisten Erfolg. Klar ist aber: Der Mensch ist und bleibt das schwächste Glied in der Kette. Darum sind Sensibilisierung und Ausbildung von entscheidender Bedeutung für Cybersicherheit.»

Kontakt: Rolf Th. Jufer
E-Mail: rolf.jufer@funk-gruppe.ch
Telefon: +41 58 311 05 74

Rolf Th. Jufer, GL-Mitglied Funk

ePrivacy

Funk rät nicht nur seinen Kunden, sich gegen Cyberrisiken zu wappnen, sondern handelt auch selber danach. Funk lässt sein Kundenportal auf der Website nach «ePrivacy» zertifizieren. Aktuell durchläuft Funk das Assessment von InfoGuard und MME.

«Das Label hat seinen Ursprung in Deutschland und orientiert sich an EU-Richtlinien», erklärt Martin Eckert von MME, der das Qualitäts-Label in die Schweiz gebracht hat. «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 gegenwärtig verschärf werden, erwartet Martin Eckert, dass auch die regulatorischen Anforderungen in der Schweiz zunehmen und die Bedeutung von «ePrivacy» zunimmt.