Keiner zu klein

Immer noch halten sich viele KMU für zu klein oder uninteressant, um Ziel eines ernsthaften Hackerangriffs zu werden. Das ist ein grosser Irrtum.

VON ROB HARTMANS

Rolf Jufer GL-Mitglied von Funk Insurance Brokers

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 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 umfassende Versicherungslösungen in der Schweiz erhältlich, mit welchen Kunden unterschiedliche Bedürfnisse abdecken können. «Doch das ist 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 lasse 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». Gemeinsam stehen die drei Partner für einen umfassenden und selbstbewussten Ansatz im Umgang mit Cyberrisiken. Hier gilt, was sich allgemein im Risikomanagement bewährt: Der Erfolg hängt davon ab, dass sich die Unternehmensleitung der Problematik bewusst ist und sich dafür zuständig fühlt.

Fehlendes Risikobewusstsein

Gemäss einer Umfrage im deutschsprachigen Raum von Ende März 2017 ist das bei grossen börsenkotierten Unternehmen durchaus der Fall. Kleine und mittelgrosse Unternehmen hinken jedoch hinterher. Bemerkenswert ist, dass nur ein Drittel der Entscheider in mittelständischen Unternehmen der Meinung ist, Ziel von Hackerangriffen zu werden. Die meisten finden ihr Unternehmen entweder zu klein oder zu uninteressant für Kriminelle. Diese Haltung kommt Rolf Jufer bekannt vor. Bereits im Jahr 2013 organisierte Funk Kundenevents mit Live-Hackersimulationen. «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. Die Frage ist aber für Unternehmen schon lange nicht mehr, ob sie angegriffen werden. Die Frage ist, wie intensiv und mit welchen Mitteln.

Bild: zvg

NACHGEFRAGT

«SENSIBILISIERUNG IST WICHTIG»

Thomas Meier, CEO InfoGuard

Wie steht es um das Bewusstsein für Cyberrisiken?
Thomas Meier: In den vergangenen zwei Jahren hat ein Umdenken stattgefunden. Dazu beigetragen haben sicher die Publizität rund um Hackerangriffe sowie die Enthüllungen von Edward Snowden. Das Thema ist definitiv in den Chef-Etagen angekommen.

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?
Generell ist es so, dass der Mensch das schwächste Glied in der Kette ist und bleibt. Darum sind Sensibilisierung und Ausbildung von entscheidender Bedeutung für Cybersicherheit.