# CYBER RISKS – NO THANKS!

Das World Wide Web hat in vielerlei Hinsicht dazu beigetragen, dass unser Leben einfacher geworden ist. Doch mit der zunehmenden Digitalisierung ist Internetkriminalität an der Tagesordnung. Mit der richtigen Strategie können Sie sich effektiv schützen.

**VON FRANCO AURELIO BARONE**

**FRANCO AURELIO BARONE**
ist Finanzplaner mit eidg. FA, Geschäftsführer von BFG BARONE Finance GmbH und Vorstandsmitglied des FPVS.

Es ist noch nicht lange her, seit das Internet nur mit einer sehr mühsamen DFÜ-Verbindung und lediglich am Computer erreichbar war. Heute ist das Internet allgegenwärtig. Mit einer «Streicheleinheit» oder per Sprachbefehl sind wir im Nu online und haben Zugang zu allen nützlichen Informationen, kaufen ein passendes Kleidungsstück oder buchen gerade die nächsten Ferien.

Das Internet ist gleichzeitig ein Schlaraffenland für Betrüger und Kriminelle. Die Täter können sehr viele Opfer überall auf der Welt in sehr kurzer Zeit attackieren, ohne dass jene es bemerken. Gestohlen wird fast alles – vom geistigen Eigentum der Unternehmen bis zu sensiblen Regierungsdaten. Auch Spionage, Sabotage und Erpressung gehören bei Cyberattacken längst zum Geschäftsmodell. Treffen kann es jeden: Privatpersonen wie auch Grosskonzerne oder KMUs. Diverse Studien zeigen, dass Cyber-Angriffe zu den grössten globalen Risiken für Unternehmen zählen. Zudem können die Kosten nach einem Angriff schnell in Millionenhöhe gehen. Jährlich gehen beim Fedpol (Bundesamt für Polizei) über 15 000 Meldungen ein – Tendenz stark steigend! Cyber-Sicherheit ist entsprechend zu einer grossen Herausforderung unseres Jahrhunderts geworden.

**Kein vollständiger Schutz möglich**

In einem engeren Sinn unterscheidet man heute zwischen digitalisierter Kriminalität und Cybercrime. Zur ersten Kategorie zählt man klassische Delikte, die unter Zuhilfenahme des Internets und sozialer Netzwerke verübt werden: also beispielsweise Drohungen via Facebook oder WhatsApp. Mit Cybercrime hingegen sind Straftaten gegen das Internet und seine Instrumente gemeint. Darunter fällt zum Beispiel die Infizierung eines Computers mit Hilfe einer Software. Sicher haben Sie auf Ihren Rechnern ein Anti-Viren-Programm installiert. Aber auch eine Sonnencreme bietet keinen vollständigen Schutz vor UV-Strahlen …

Hinter jedem Risiko steckt allerdings auch eine Chance: Längst haben Versicherungsgesellschaften und Consultingfirmen das Bedürfnis entdeckt. In der Zwischenzeit hat diese Industrie verschiedene Lösungspakete geschnürt, das Dienstleistungsangebot wurde mit Experten-Teams erweitert. Auch für die nationale Sicherheit wird gesorgt, denn, wenn es einen Staat trifft, indem beispielsweise kritische Infrastrukturen wie die Strom- und Wasserversorgung oder das Telekommunikationsnetz lahmgelegt werden, können die Folgen katastrophal sein. Mittlerweile bieten namhafte Versicherungsgesellschaften wie die Allianz, die Mobiliar oder die Zurich eine Cyber-Risk-Versicherung für Privatpersonen und Unternehmungen an. Der Leistungskatalog kann je nach Bedürfnis gestaltet werden. Versicherbar sind z.B. folgende Risiken:

- **Eigenschaden:** Daten wurden aufgrund eines Hacker-Angriffs gestohlen, der Kriminelle erpresst mittels Ransomware z.B. eine Bitcoin-Lösegeldzahlung. Die Datenwiederherstellung nach einem solchen Vorfall kann sehr teuer werden.

- **Haftpflichtansprüche:** Deckt Ansprüche von Dritten bei Datenschutzverletzungen, Datenverlust oder Weitergabe von Schadsoftware.

- **Betriebsunterbruch:** Je nach Grösse des Unternehmens kann ein Umsatzausfall durch einen Cyber-Angriff oder durch Datenschutzverletzungen existenzielle Folgen haben.

- **Krisenmanagement:** Vielleicht benötigt man forensische Dienstleistungen, IT-Spezialisten oder einen PR-Berater, um einen Schaden zu beheben und das angekratzte Image wieder auf Vordermann zu bringen. Durch eine Kooperation mit spezialisierten Unternehmen kann die Versicherung hierbei vermitteln.

- **Cyber Crime Social Engineering:** Schäden infolge Täuschung durch eine Drittperson, insbesondere bei Betrug durch Vorspiegelung einer falschen Identität sowie durch Umleitung von Zahlungsströmen.

- **Rechtsschutz:** Streitigkeiten im Zusammenhang mit Vertragsrecht, Identitätsmissbrauch oder Persönlichkeitsverletzung, wobei diese Leistungen meist schon in einer bestehenden Rechtsschutzdeckung beinhaltet sein können.

**Unverzichtbarer Schutz**

Cyber-Versicherungen stecken noch in den Kinderschuhen und lassen sich daher noch schlecht vergleichen. Ihr Nutzen sollte indes unbestritten sein. Die Prämien für einen solchen Versicherungsschutz halten sich in Grenzen und sind gut mit einer Privat- oder Betriebshaftpflichtversicherung vergleichbar. Somit gehört diese Versicherung im Versicherungsportefeuille zukünftig einfach dazu.

Wir selbst können natürlich auch etwas gegen einen Angriff tun, indem wir uns präventiv dagegen schützen, privat wie auch im Geschäft. Richtige IT-Architektur-Massnahmen, Cloud-Computing und Internet of Things, die passenden Protokolle und Vorsichtsmassnahmen sorgen für den nötigen Datenschutz. Wachsam bleiben und Risiken antizipieren dämmt das Risiko ein. Bevor wir Angst haben müssen, dass am Himmel Drohnenkämpfe stattfinden oder dass gar schlimmere Szenarien à la Terminator Realität werden, schützen wir uns davor, denn es ist Zeit dafür!

**Association des Conseillers Financiers — Associazione dei Consulenti Finanziari — Association of Financial Planners**
**Redaktion:** FPVS, Münzgraben 6, 3000 Bern 7, Tel. 056 500 51 50, www.fpvs.ch