EXPERTENMEETING ZUM THEMA CYBERSICHERHEIT UND CYBERVERSICHERUNG

Eine Standortbestimmung

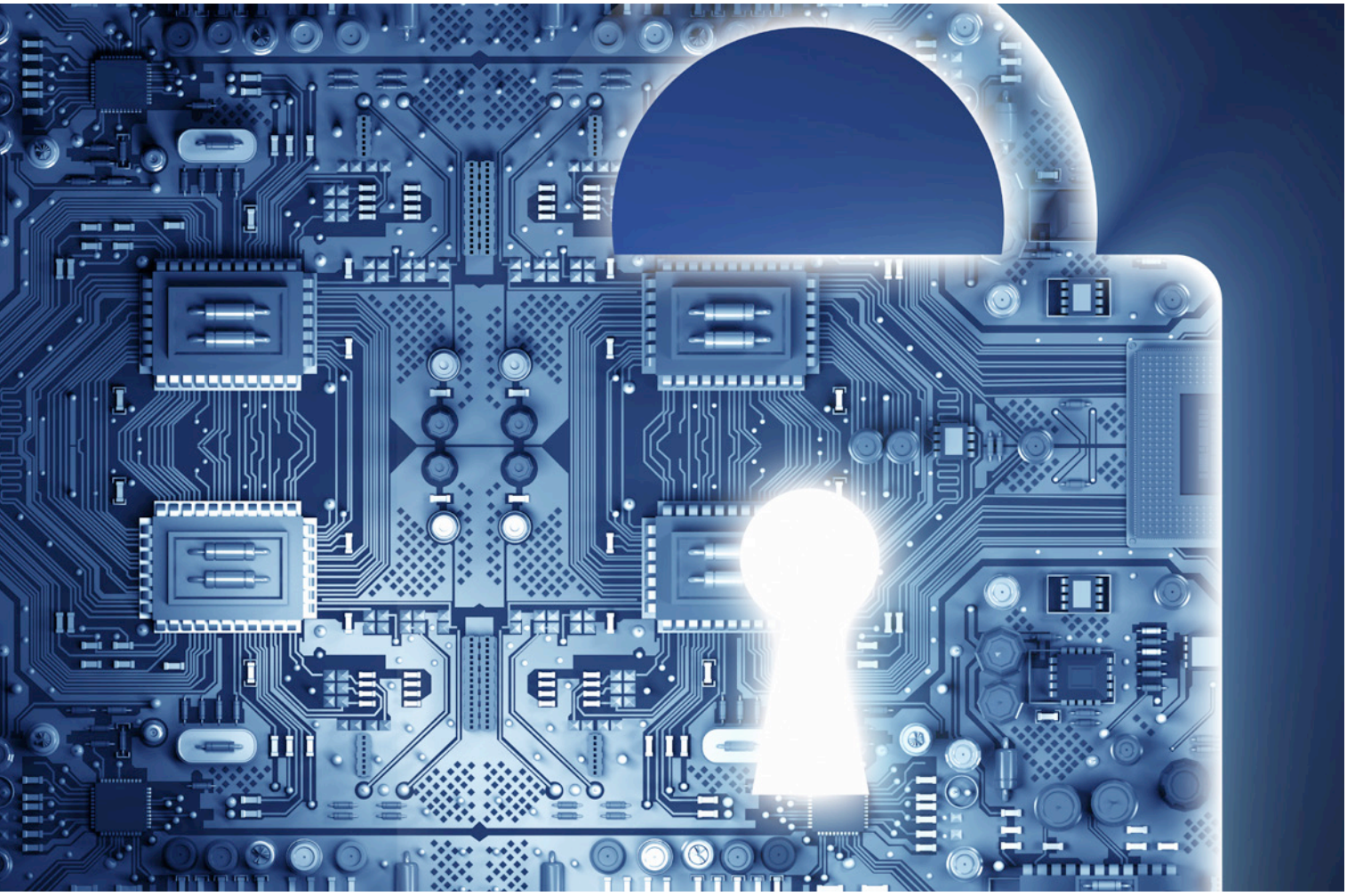

Foto: Henrik5000/iStock

Am 11. März 2015 trafen sich im Hause der Risk Consultants der Corporate Trust Business Risk & Crisis GmbH Experten zum Thema Cyberversicherung. Vor dem Hintergrund der aktuellen Cyber-Bedrohungslage ging es vor allem um die Frage, welche Versicherungsangebote die Assekuranz derzeit macht, sowie um die betriebswirtschaftliche Frage nach den Kosten infolge eines Cyberangriffs und nach den Investitionen in die Prävention. Peter Janson, Leiter des Competence Centers IT, sowie Michael Dutz, Leiter des Fachbereichs Non Marine der SCHUNCK GROUP, nahmen an der Expertenrunde teil.

„Rein technisch ist das Problem der Cybersicherheit nicht mehr zu lösen." So eröffnete Florian Oelmaier, Leiter IT-Sicherheit & Computerkriminalität bei Corporate Trust, die Gesprächsrunde. Allerdings sei auch im Hinblick auf die technischen Möglichkeiten der Prävention gerade im Mittelstand noch viel Raum, um Risiken zu reduzieren. So stünden „technische, organisatorische und personelle Maßnahmen" im Vordergrund eines funktionierenden IT-Sicherheitsmanagements.

Angesichts der rasanten technischen Entwicklung – Stichwort „Industrie 4.0" – stecken die Bemühungen um einen effektiven Schutz gegen

Cyberangriffe in vielen Bereichen der Gesellschaft noch in den Kinderschuhen. Vor diesem Hintergrund sieht Klaus Keus, Referatsleiter Analyse und Prognose im Bereich der Cybersicherheit beim Bundesamt für Sicherheit in der Informationstechnik (BSI), die Assekuranz in einer Rolle der „gesamtgesellschaftlichen Mitgestaltung der Verbesserung der Cybersicherheit".

Doch eine adäquate Versicherungslösung bedarf einer ausreichenden Datenbasis, gerade wenn man sich die möglichen Schadensszenarien und die daraus ergebenden Kosten vor Augen führt. Die bisher noch wenigen Anbieter für Cyberversicherungen behelfen sich derzeit mit Daten aus den USA, wo zu diesem Thema bereits gewisse Erfahrungswerte vorliegen. Jedoch taugen diese aus haftungsrechtlicher Sicht nur bedingt für Europa, wie Norbert Schrödel, Underwriter Cyber Insurance der Zürich Gruppe Deutschland, verdeutlichte. Lassen sich Auswirkungen zu Eigenschäden noch weitgehend vergleichbar übertragen, so sind Kosten beziehungsweise Haftungsfragen in Verbindung mit Fremdschäden – etwa bei Datenschutzverletzungen von Kunden oder Mitarbeitern – nur sehr eingeschränkt aus dem angelsächsischen Recht auf deutsches Recht übertragbar.

Trotz fehlender objektiver Bewertungskriterien gehen mittlerweile 12 Versicherungsgesellschaften mit eigenen – zum Teil höchst unterschiedlichen – Versicherungsangeboten gegen Cyberrisiken auf den Markt. Gerade für mittelständische Unternehmen sind bereits heute umfassende Lösungen darstellbar, die allerdings in hohem Maße individuell auf die jeweiligen Bedürfnisse zugeschnitten werden müssen.

Um die Sicherheit beim Datenschutz nachhaltig zu verbessern, gibt es zahlreiche Ansätze. In Deutschland ist laut Klaus Keus deshalb eine „Informationsaustauschkultur" dringend notwendig, um die konkreten Risiken besser greifen zu können. Keus wies darauf hin, dass es in diesem Bereich „keine Denkverbote" geben dürfe. Ein möglicher Denkansatz wäre eine anonyme Meldepflicht für Cybervorfälle beim BSI. Unter dem Stichwort „Security by Design" wurde darüber diskutiert, Sicherheitsüberprüfungen oder Zertifizierungen für sicherheitskritische IT-Produkte zu erlassen.

Um das Risiko für die Assekuranz besser kalkulierbar und damit attraktiver zu gestalten, wird der Trend in Richtung eines präventiven vorvertraglichen Risikochecks gehen. Neben einem Risikofragebogen wird auch der Einsatz externer Dienstleister wie Corporate Trust zunehmend eine Rolle spielen. In diesem Sinne präsentiert der Verband der Schadenversicherer (VdS) auf der CeBIT ein eigenes Zertifizierungsprogramm in verschiedenen Stufen: vom VdS-Quick-Check über ein VdS-3473-Zertifikat bis hin zum VdS-ISO-27001-Zertifikat.

Das Fazit des Expertenmeetings formulierte Florian Oelmaier: „Eine hundertprozentige Sicherheit gibt es nicht, und die Einschläge kommen immer näher." Schon heute gebe es praktisch keinen Geschäftsbereich mehr, der ohne IT auskomme. Daher sei – ähnlich dem Brandschutz in Unternehmen – auch für den Bereich der Cybersicherheit ein umfassendes betriebliches IT-Sicherheitsmanagement gefragt. Und dies sollte neben technischen, organisatorischen und personellen Maßnahmen auch den Risikotransfer über eine Cyberversicherung beinhalten.

„Unser größtes Anliegen ist es, unseren Kunden der bestmögliche Berater und Dienstleister zu sein. Deshalb stehen wir zu Fragen rund um die Absicherung von IT-Risiken jederzeit gerne Rede und Antwort", betonte Peter Janson. ■

Vorn: Michael Michael Dutz, Risikomanager, SCHUNCK GROUP (l.); Florian Oelmaier, Leiter IT-Sicherheit & Computerkriminalität, Corporate Trust; hinten (v. l. n. r.): Peter Janson, Leiter Competence Center IT, SCHUNCK GROUP; Klaus Keus, Referatsleiter Analyse und Prognose, Bundesamt für Sicherheit in der Informationstechnologie (BSI); Friedrich Wimmer, Lead Consultant IT-Sicherheit, Corporate Trust; Norbert Schroedel, Underwriter Cyber Insurance, Zürich Gruppe Deutschland