Intangible Risks – Cybergefahren: Nicht greifbar, aber so angreifbar!

Man kann sie nicht anfassen. Doch wenn Viren die IT-Systeme erst einmal verseucht haben, können die Schäden bei den betroffenen Unternehmen immens und im schlimmsten Falle vergleichbar mit einem Großfeuer in der Produktion sein. Ein Großfeuer verursacht Sachschaden, Verrußung und den Stillstand des Betriebes. Je besser man gegen das Feuer gewappnet ist, zum Beispiel durch Sprinkleranlagen, Alarmmelder oder sogar Betriebsfeuerwehren, desto schneller kann man den Brand löschen und Folgeschäden beseitigen.

Nicht viel anders ist es bei einem ernst zu nehmenden Hackerangriff. Wurde der Angriff erkannt, heißt es, unmittelbar zu reagieren und nicht betroffene Systeme zu retten. Schnelle und kompetente Forensik ist zur Überprüfung der betroffenen Systeme erforderlich und um den „Patienten Null", die Einflugschneise für die Attacke, zügig zu ermitteln. Danach beginnt der Austausch beziehungsweise die Dekontamination der verseuchten Soft- und Hardware zur Wiederherstellung des Geschäftsbetriebes. Auf diese Weise soll die Zeit der Betriebsunterbrechung so kurz wie möglich gehalten werden.

Durch die heutzutage umfassende, weltweite Vernetzung der Betriebe in der Kommunikations- und Produktionssoftware kann sich ein Schaden – zum Beispiel ausgelöst durch eine Ransomware-Attacke – im schlimmsten Fall auf alle anderen Gesellschaften der Unternehmensgruppe auswirken. Ähnlich wie die Folgen eines Großbrandes in einem kritischen Bereich Wechsel- und Rückwirkungsschäden in der eigenen Unternehmensgruppe, bei Zulieferern sowie bei Kunden verursachen.

Bestmögliche Cybersicherheit und ein Risikomanagement auf höchstem Niveau sind die Grundvoraussetzungen, um sich gegen derartige Gefahren zu wehren, etwaige Attacken frühzeitig zu erkennen und zu verhindern beziehungsweise – wenn doch die Systeme infiltriert wurden – weitere Ausbreitungen zu vermeiden.

Die Cyberversicherung bildet das i-Tüpfelchen für den Bilanzschutz, um diese nicht greifbaren Risiken abzusichern. Allerdings hat sich der Versicherungsmarkt in den vergangenen zwölf Monaten stark gewandelt. Aufgrund der bereits sehr hohen Schadenbelastung und immer neuer Softwarelücken und Ransomware-Attacken haben die Risikoträger ihr Zeichnungsverhalten deutlich verändert.

Die Limite bei den Versicherungssummen wurden massiv reduziert – von vormals bis zu 25 Millionen Euro je Versicherer auf nunmehr 10 Millionen Euro oder sogar nur fünf Millionen. Gleichzeitig wurden die Selbstbehalte und Eigentragungen der Versicherungsnehmer im Schadenfall deutlich erhöht und die Prämie erheblich angehoben, teilweise um bis zu 400%.

Kunden müssen ihre CyberSecurity offenlegen, aber auch optimieren

Versicherer fokussieren sich verstärkt auf das technische Underwriting bei der Überprüfung der Unternehmen. Dezidierte Fragebögen von mehr als 15 Seiten oder Zusatzfragen zur Absicherung bei Ransomware-Schäden haben Einzug gehalten. Es gibt zwar noch einen erheblichen Unterschied bei Fragebögen und Mindestanforderungen zwischen kleineren und mittelständischen Industriekunden und den sogenannten Großrisiken, doch eins ist bereits jetzt erkennbar: Werden

Sandra Dammalacks, Spartenleiterin Financial Lines & Cyberversicherungen, deas Deutsche Assekuranzmakler GmbH