Bundeskriminalamt

BKA

Cybercrime –

Die Perspektive des Versicherers

DR. THOMAS SEPP

CYBERCRIME – DIE PERSPEKTIVE DES VERSICHERERS

Cybervorfälle – interne Systempannen ebenso wie externe Angriffe – zählen seit einigen Jahren zu den größten Geschäftsrisiken weltweit für Unternehmen, wie das jährliche erhobene Allianz Risk Barometer zeigt. Cyberrisiken entwickeln sich mit hoher Dynamik fortlaufend weiter – die Kommerzialisierung von Malware und Hacking-Tools, die Zunahme von Ransomware-Angriffen, die weitreichenden Folgen von Mega-Datenlecks und von staatlichen Akteuren gesponsorte Kampagnen zielen auf einzelne Unternehmen und immer häufiger auch auf die Destabilisierung ganzer Volkswirtschaften. Durch den Digitalisierungsschub und den vielerorts ungeplanten Übergang zu Remote Working in der Breite hat die Covid-19-Pandemie im vergangenen Jahr weitere Einfallstore für Cyberkriminalität geschaffen.

Als ein führender Anbieter von Cyberversicherungen sehen wir eine kontinuierlich steigende Zahl von Schadensfällen, die teils auf das Wachstum des globalen Cyberversicherungsmarktes zurückzuführen ist, aber auch auf die wachsende Bedrohungslage. Nicht immer hält die Weiterentwicklung der IT-Sicherheit und der Cyberabwehr in den deutschen Unternehmen Schritt mit der hohen Veränderungsdynamik der Cyberrisiken – gerade im Mittelstand und bei kleineren Unternehmen besteht Aufholbedarf. Denn jedes Unternehmen gleich welcher Größe und Branche ist ein potenzielles Angriffsziel.

Aus Sicht der Allianz Global Corporate & Specialty besteht in der Wirtschaft Handlungsbedarf in drei Bereichen, um sich besser gegen Cybergefahren zu wappnen: Wie lässt sich das Verständnis von Cyberrisiken bei Geschäftsführung und Mitarbeitern weiter erhöhen? Wie können umfassende und nutzerfreundliche Cybersicherheitslösungen aussehen – gerade für kleinere Unternehmen mit beschränkten Ressourcen? Wie lässt sich den zunehmenden Ransomware-Angriffen und Lösegeldforderungen besser entgegentreten?

Umfassender Cyberschutz für Unternehmen erfordert ein hohes Maß an IT-Sicherheit und Präventionsarbeit im Vorfeld, Minderung und Transfer der finanziellen Risiken und professionelles Krisenmanagement im Ernstfall. Dazu sind vielfältige Maßnahmen notwendig, die eine enge Kooperation innerhalb eines Unternehmens, aber auch mit einer Vielzahl von externen Partnern und Spezialisten in einem Cyber-Ökosystem voraussetzen.