



Cyberangriffe: „Die Antwort auf hybride Kriegsführung muss hybride Sicherheit sein“

Michael Fiedler

Das Bundeskabinett will die Geschäftsordnung für den neuen Nationalen Sicherheitsrat beschließen. Er soll den bisherigen Bundessicherheitsrat ablösen und künftig eine integrierte Sicherheitspolitik koordinieren, Strategien entwickeln und gemeinsame Lagebewertungen vornehmen. Besonders Cyberangriffe und digitale Sabotage rücken dabei ins Zentrum – mit erheblichen Auswirkungen auch für die Versicherungswirtschaft.

Für Versicherer ist die Entwicklung von besonderer Bedeutung. Cyberangriffe gehören zu den am stärksten wachsenden Risikofeldern. Policen für Unternehmen müssen zunehmend auch Szenarien wie digitale Sabotage, Ransomware oder Ausfälle kritischer Infrastruktur abdecken. Die Forderung nach einem Nationalen Cyberlagebild, das Bedrohungen in Echtzeit erfasst und Informationen zwischen Behörden und Wirtschaft teilt, könnte deshalb auch die Risikoeinschätzung und Modellierung in der Versicherungsbranche maßgeblich beeinflussen.

Wintergerst plädiert für eine enge Zusammenarbeit: „Der Nationale Sicherheitsrat muss die digitale Gefahrenlage in seine Analysen und Entscheidungsprozesse einbeziehen und auf die entsprechende Expertise zurückgreifen, etwa die des Bundesamts für die Sicherheit in der Informationstechnik (BSI) oder des Bundesdigitalministeriums.“ Auch die Einbindung der Digitalwirtschaft sei entscheidend, um technologische Trends – etwa im Bereich Künstliche Intelligenz – frühzeitig zu berücksichtigen.

Mit Blick auf den Versicherungsmarkt bleibt entscheidend, wie verlässlich und aktuell die Bedrohungseinschätzungen ausfallen. Nur wenn die Lagebilder Risiken transparent machen, lassen sich Cyberversicherungen risikoadäquat kalkulieren und Kapazitäten am Markt ausbauen.

Versicherungs- und Finanznachrichten

expertenReport



<https://www.experten.de/id/4941330/Cyberangriffe-Die-Antwort-auf-hybride-Kriegsfuehrung-muss-hybride-Sicherheit-sein/>