expertenReport

Quelle: Redaktion experten.de / KI-generiert

Hybride Angriffe: Jedes fünfte Unternehmen spürt bereits starke Folgen

Michael Fiedler

Cyberattacken, Spionage, Sabotage und Desinformation: 19 Prozent der deutschen Unternehmen berichten inzwischen von starken Auswirkungen hybrider Angriffe aus dem Ausland. Bei Großunternehmen sind es sogar 39 Prozent. Die wachsende Bedrohung durch staatliche und staatsnahe Akteure stellt dabei nicht nur die Sicherheitsarchitektur vor neue Aufgaben – sondern berührt auch die Frage, wo bei Cyberversicherungen die Grenze zwischen versichertem Angriff und Krieg verläuft.

Kritische Infrastruktur besonders betroffen

Besonders häufig berichten Unternehmen aus Bereichen von Angriffen, die für das Funktionieren von Wirtschaft und Gesellschaft eine zentrale Rolle spielen. In der Informations- und Kommunikationswirtschaft ist etwa jedes dritte Unternehmen betroffen. In der Energie- und Wasserversorgung berichtet gut jedes vierte Unternehmen von entsprechenden Auswirkungen. In der Industrie sowie bei wirtschaftsnahen Dienstleistern wie Laboren und Unternehmensberatungen ist es fast jedes fünfte. Damit verändert sich nach Einschätzung des IW auch das Motiv hinter den Angriffen. Klassische Wirtschaftskriminalität zielt beispielsweise auf Geld, Geschäftsgeheimnisse oder Technologien. Bei hybriden Angriffen können dagegen politische oder strategische Ziele hinzukommen. Das Bundeskriminalamt beobachtet ebenfalls eine zunehmende Überschneidung. Im Bundeslagebild Cybercrime weist die Behörde darauf hin, dass geopolitische Konflikte zunehmend in den digitalen Raum getragen werden und die Grenzen zwischen finanziell und politisch motivierten Cybergruppen verschwimmen.

Sabotage, Cyberangriffe und Angriffe auf Infrastruktur

Wie breit das Spektrum hybrider Bedrohungen inzwischen ist, zeigt sich besonders an kritischen Infrastrukturen. Unterseekabel und Pipelines in der Ostsee stehen seit mehreren Beschädigungen besonders im Blickpunkt der Sicherheitsbehörden. Die NATO startete Anfang 2025 die Mission „Baltic Sentry“, um kritische Unterwasser-Infrastruktur stärker zu überwachen und potenzielle Saboteure abzuschrecken. Die Bundeswehr bezeichnet Pipelines sowie Strom- und Datenkabel ausdrücklich als mögliche Ziele hybrider Angriffe. Auch im Cyberraum ist die Trennung zwischen gewöhnlicher Kriminalität und geopolitisch motivierten Angriffen schwieriger geworden.

Das BKA spricht von einer erkennbar gestiegenen hybriden Bedrohung. Pro-russische Aktivisten haben beispielsweise mit DDoS-Angriffen deutsche Einrichtungen ins Visier genommen. Diese Attacken verursachten nach Erkenntnissen des BKA bislang meist wenig nachhaltigen technischen Schaden, zielten aber auch darauf, Verunsicherung zu erzeugen und Vertrauen in staatliche Institutionen zu schwächen. BKA-Präsident Holger Münch verwies zudem auf sogenannte „Low-Level-Agents“. Dabei werden beispielsweise Kleinkriminelle über soziale Netzwerke angeworben, um gegen Bezahlung einzelne Handlungen bis hin zu schweren Straftaten auszuführen. Das BKA sieht eine deutlich erhöhte Bedrohung durch Spionage und Sabotage – auch im Cyberraum.

Wenn der Cyberangriff zum Versicherungsfall wird

Für Unternehmen entsteht daraus eine zusätzliche Schwierigkeit. Denn die Frage, wer hinter einem Angriff steht und welchem Zweck er dient, kann auch für den Versicherungsschutz relevant werden. Cyberversicherungen decken grundsätzlich zahlreiche Folgen von Angriffen auf IT-Systeme ab. Gleichzeitig enthalten Versicherungsbedingungen Ausschlüsse für Krieg und bestimmte staatliche Angriffe. Wie schwierig diese Grenze selbst für Versicherer zu ziehen ist, zeigte eine experten.de-Anfrage an den GDV: Insbesondere bei Cyberangriffen lasse sich nicht eindeutig bestimmen, wann aus einem Angriff eine Kriegshandlung wird. Die aktuellen unverbindlichen Musterbedingungen des GDV machen dabei deutlich, dass Krieg im Sinne einer Cyberversicherung nicht zwingend mit Panzern, Raketen oder anderen physischen Waffen geführt werden muss. Auch mit digitalen Mitteln geführte Kriegshandlungen können unter den Ausschluss fallen. Darüber hinaus sehen die Musterbedingungen einen Ausschluss für bestimmte Informationssicherheitsverletzungen vor, die durch einen Staat, in dessen Auftrag oder unter dessen Kontrolle verursacht werden und zugleich kritische Infrastrukturen erheblich beeinträchtigen oder ausfallen lassen. Damit wird die Attribution eines Cyberangriffs im Schadenfall potenziell entscheidend: War es gewöhnliche Cyberkriminalität, ein staatsnaher Akteur, eine staatlich gesteuerte Operation oder bereits Teil eines Krieges?

Kriegsausschluss ist keine automatische Hintertür

Dass ein Cyberangriff möglicherweise aus Russland, China oder einem anderen Staat stammt, bedeutet allerdings nicht automatisch, dass der Versicherungsschutz entfällt. Der GDV hatte bereits im Zusammenhang mit dem Ukraine-Krieg darauf hingewiesen, dass nach seinen Musterbedingungen der Versicherer nachweisen müsse, dass tatsächlich eine vom Ausschluss erfasste Kriegshandlung vorliegt. Dem Verband war seinerzeit kein deutscher Fall bekannt, in dem ein Cyberversicherer erfolgreich den Kriegsausschluss geltend gemacht hatte. Gerade hybride Angriffe erschweren diese Abgrenzung. Sie bewegen sich häufig bewusst unterhalb der Schwelle eines offenen militärischen Konflikts und lassen Verantwortlichkeiten im Unklaren.

IW fordert stärkere Rolle des Bundes

Für Unternehmen hat diese Entwicklung eine Grenze: Gegen gewöhnliche Cyberkriminalität können sie ihre IT-Sicherheit verbessern, Notfallpläne entwickeln und Versicherungsschutz einkaufen. Staatlichen oder staatsnahen Akteuren können einzelne Unternehmen jedoch nur begrenzt etwas entgegensetzen. „Gegen die neue Gefahrenlage durch staatliche Akteure kann nur der Bund etwas ausrichten“, sagt IW-Experte Simon Gerards Iglesias. Das geplante KRITIS-Dachgesetz sei ein erster Schritt, bleibe bei Zuständigkeiten und konkreten Maßnahmen aber zu vage. Der Bund müsse nach Ansicht des IW stärker für Abwehr und Aufklärung aufkommen und enger mit Ländern und Unternehmen zusammenarbeiten. Die Herausforderung reicht damit inzwischen weit über klassische IT-Sicherheit hinaus. Je stärker Cyberangriffe, Sabotage, Spionage und staatliche Einflussnahme ineinandergreifen, desto schwieriger wird nicht nur die Abwehr. Auch die Grenze zwischen versicherbarem Unternehmensrisiko und staatlichem Konflikt wird schwieriger zu ziehen.

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4951756/Hybride-Angriffe-Jedes-fuenfte-Unternehmen-spuert-bereits-starke-Folgen/