Einfach, weil's wichtig ist.

ERGO

A Munich Re company

Kriegsauschlüsse in der Cyber-Versicherung

Eine (komplett unjuristische!) Einordung

Öffentlich

Seit dem 24.02.2022 ist die Welt eine andere

ERGO
A Munich Re company

Schutz bei Cyberattacken

Wie sich die Versicherer vor Zahlungen drücken

Branche Cyber

Cyberattacken russischer Hacker versichert?

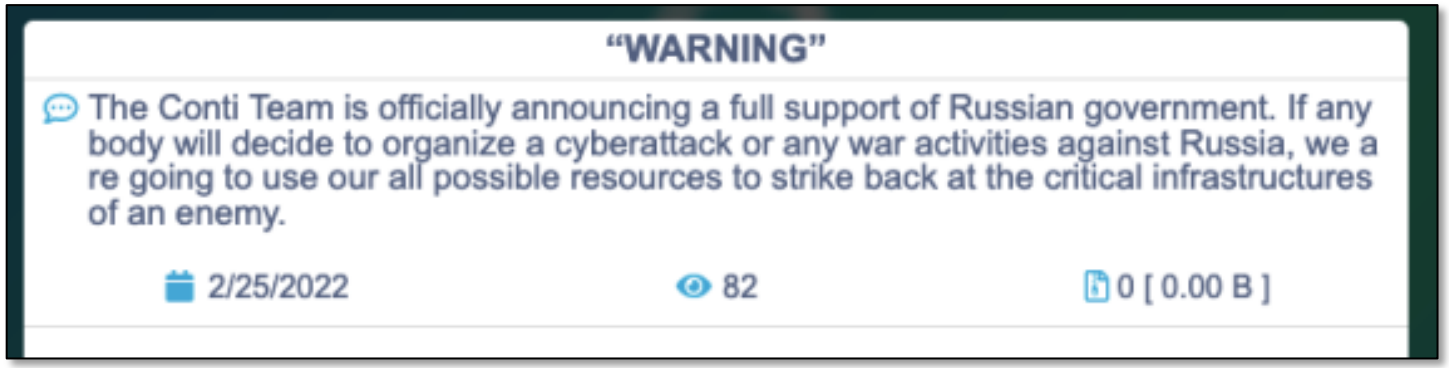
Der Angriff Russlands auf die Ukraine hat – neben der humanitären Katastrophe – auch Auswirkungen auf die Versicherungsbranche. Die Kämpfe finden nicht nur in den Städten der Ukraine statt, sondern Russland führt gleichzeitig einen Cyberkrieg, in welchem Hacker kritische Infrastruktur, Informationstechnologien, Regierungsinstitutionen oder Ministeriumswebseiten der Ukraine gezielt angreifen und lahmlegen wollen.

Cyber

Cyberversicherer berufen sich auf Kriegsausschluss und verneinen Leistungspflicht

Die Auswirkungen auf die Cyber-Versicherung waren zunächst sogar positiv

ERGO
A Munich Re company



Gemeldete Schäden zur Cyber-Versicherung (GDV-Statistik*)

Jahr	Anzahl der Schäden	Veränderung zum Vorjahr
2021	3766	
2022	2276	-39,4%
2023	2903	+27,5%

GROUP	SUPPORTING	ATTACKS	COMMS	LOC	Date started
AgainstTheWest (ATW)	Ukraine	Data Breach & ransomware	Twitter	West Europe	2021
Belarusian Cyber Partisans	Ukraine/Free Belarus	Ransomware	Twitter	Belarus	2020
Anonymous	Ukraine	DDoS	Twitter	Global	FEB 2022
GhostSec	Ukraine	Hack	Telegram	UNK	FEB 2022
IT Army of Ukraine	Ukraine	DDoS	Telegram	Ukraine	FEB 2022
KelvinSecurity Hacking Team	Ukraine	Hack	Twitter	UNK	FEB 2022
BlackHawk	Ukraine	DDoS	Twitter	Georgia	FEB 2022

*) Quellen: GDV, Geschäftsverlauf Cyber-Risikoversicherung 2022 und 2023, https://cyberscoop.com/conti-ransomware-russia-ukraine-critical-infrastructure/

Das Augenintegral zeigt dennoch gut, wo die Reise hingeht

ERGO
A Munich Re company

D.1.14 Schäden durch

a) Krieg, kriegsähnliche Ereignisse, staatlich veranlasste oder politisch motivierte Angriffe, welche sich auf IT-Systeme auswirken;

b) Bürgerkrieg, Revolution, Aufstand, Aufruhr, innere Unruhen, andere feindselige Handlungen, Generalstreik, illegalen Streik;

D.1.14 Versicherungsfälle oder Schäden aufgrund von

a) Krieg, kriegsähnlichen Ereignissen, Bürgerkrieg, Revolution, Rebellion oder Aufstand, auch wenn diese Versicherungsfälle oder Schäden aufgrund einer in Vertragsteil A, B und/oder C definierten Ursache (nachstehend Informationssicherheitsverletzung genannt) durch einen Staat, im Auftrag oder unter Kontrolle eines Staates im Verlauf eines Krieges entstanden sind.

b) Informationssicherheitsverletzungen, die durch einen Staat, im Auftrag oder unter Kontrolle eines Staates verursacht worden sind, wenn dadurch auch kritische Infrastrukturen im Umfang der Regelungen des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) in diesem oder einem anderen Staat ausgefallen oder beeinträchtigt sind.

Die Voraussetzungen dieses Ausschlusses liegen insbesondere dann vor, wenn eine IT-forensische Untersuchung der informationsverarbeitenden Systeme des Versicherungsnehmers oder bei der Informationssicherheitsverletzung verwendeter Systeme oder Hilfsmittel objektive Hinweise auf die Beteiligung, Urheberschaft oder Steuerung der Informationssicherheitsverletzung durch einen Staat, im Auftrag oder unter Kontrolle eines Staates ergeben.

Das ist unter anderem dann der Fall, wenn eine Beteiligung von Gruppen oder Personen nachgewiesen werden kann, die in der Vergangenheit bereits an entsprechenden Handlungen dieses Staates beteiligt waren.

Zuschreibung von Informationssicherheitsverletzungen, die durch einen Staat, im Auftrag oder unter Kontrolle eines Staates verursacht worden sind:

Bei der Feststellung der Zuschreibung an einen Staat trägt der Versicherer die Beweislast. Ungeachtet dessen können Versicherer und Versicherungsnehmer alle ihnen zur Verfügung stehenden objektiv angemessenen Beweismittel berücksichtigen. Unter allen rechtlich zulässigen Beweismitteln kann dies auch die offizielle Zuschreibung durch staatliche Stellen des Staates, dessen kritische Infrastrukturen durch die Informationssicherheitsverletzungen beeinträchtigt worden sind, an einen anderen Staat oder zu Gruppen oder Personen, die auf seine Anweisung oder unter seiner Kontrolle handeln, umfassen.

Was bedeutet das aber in der Praxis für Sie? 1/2

ERGO
A Munich Re company

Cyber

Der neue Cyber-Kriegsausschluss – eine Kampfansage

Eine wesentliche Neuerung der jüngst vom Versicherverband GDV vorgelegten Musterbedingungen für die Cyberrisikoversicherung betrifft den Kriegsausschluss. Die neuen AVB Cyber erweitern den Ausschluss gegenüber den Musterbedingungen aus dem Jahr 2017 und marktüblichen Bedingungswerken erheblich. Die Neugestaltung schafft nicht nur rechtliches Konfliktpotenzial, sondern wirft die grundsätzliche Frage auf, ob Versicherer die faktisch bestehenden Cyberrisiken der Unternehmen eigentlich noch versichern wollen.

Systemische Risiken dieser Größenordnung sind in der Breite nicht versicherbar!

Was bedeutet das aber in der Praxis für Sie? 2/2

ERGO
A Munich Re company

1) Verunsicherte Kunden: Was passiert nun mit meinem Versicherungsschutz? Wird jeder Hackerangriff einer russischen Ransomware-Truppe zukünftig vom Versicherungsschutz ausgeschlossen?

- Betroffenheit von kritischen Infrastrukturen gibt Hinweis auf wesentliche Beeinträchtigung der gesamten Wirtschaft
- Objektive Hinweise aus forensischen Gutachten

2) Verunsicherte Kunden: Was bedeutet „im Auftrag von“ oder „unter Kontrolle“ eines Staates? Wer soll das beweisen?

- Beweislast liegt grundsätzlich beim Versicherer
- Das Wording gibt einen Rahmen, was der VR als objektive Hinweise deuten möchte bzw. wird: „…offizielle Zuschreibung durch staatliche Stellen…“, „…in der Vergangenheit bereits an entsprechenden Handlungen dieses Staates beteiligt waren…“

Auch wenn Sie keine 100% absolute Aussage bekommen werden – fragen Sie im Zweifel den/die Anbieter Ihrer Wahl, wie man zu diesen Graubereichen steht.

Zum Schluss: Ein kleiner Ausblick in 4 Thesen

ERGO
A Munich Re company

These 1: Mehr Sicherheit wird erst ein Urteil zum Kriegsausschluss in einer Cyber-Versicherung geben

- Viele Unschärfen geben nur eine Ahnung, wann ein Ausschluss gezogen werden kann
- Es hängt – wie immer – viel von der Regulierungspraxis in den einzelnen Häusern ab

These 2: Die Datenqualität wird besser, und Kumule (vermeintlich) durch Modelle beherrschbarer

- Anbieter für parametrische Deckungen oder dezidierte Kriegsereignisse werden die Lücke schließen
- Durch mehr Sicherheit in den Modellen wird Pricing und Exposure stabiler und erfährt mehr Vertrauen

These 3: Große Kumule werden nicht „aus Versehen“ auftreten

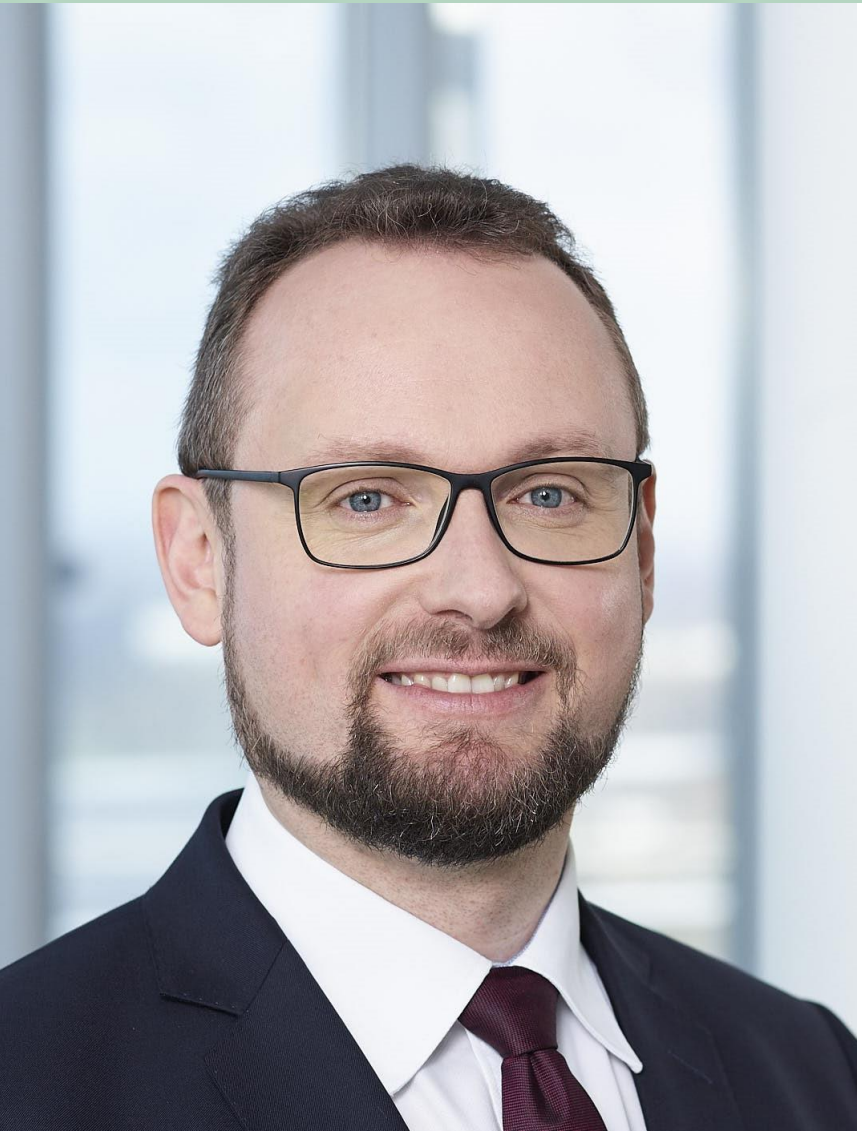
- Es ist nach wie vor ein hoher Aufwand nötig, um Angriffe mit möglichst viel Durchschlagskraft zu orchestrieren
- Es liegt nicht im Interesse eines wirtschaftlich orientierten Angreifers, alles zu zerstören
- Siehe „Crowdstrike“: Die Selbstheilungskräfte sind nicht zu unterschätzen

These 4: Kumule werden weiterhin passieren und das Angebot an Versicherungsschutz formen

- Cyber ist und bleibt einer hohen Dynamik unterworfen
- Der Markt wird auch zukünftig volatil bleiben und sich auf die Veränderungen einstellen müssen (Stichwort: Deckung für technische Probleme)

Vielen Dank für Ihre Aufmerksamkeit! Fragen?

ERGO
A Munich Re company



Alexander Schudra

Abteilungsleiter Cyber-Versicherung

alexander.schudra@ergo.de

Telefon: 0211/477-7916
Mobil: 0172/6594400