Recht

Kriegsausschluss in der Cyber-Versicherung – Sind Cyberattacken z.B. russischer Hacker versichert?

Der Angriff Russlands auf die Ukraine hat – neben der humanitären Katastrophe – auch Auswirkungen auf die Versicherungsbranche. Dr. Marcel Straub und Dennis Wrana vom langjährige AVW-Kooperationspartner für die Financial Lines Sparten Finlex gehen dem Thema auf den Grund und haben folgendes zu berichten:

Dennis Wrana ist Product Manager Cyber bei Finlex. Foto: Finlex

Wolf-Rüdiger Senk ist Prokurist bei AVW und Bereichsleiter Versicherungsrecht E-Mail: wolf-ruediger.senk@avw-gruppe.de

Dr. Marcel Straub ist Head of Legal und Schadenexperte bei Finlex. Foto: Finlex

„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. Auch westliche Einrichtungen und Unternehmen wurden im Rahmen des Konflikts bereits Opfer von russischen Cyberangriffen. Konnten sich die angegriffenen Unternehmen in der Vergangenheit bei der Bewältigung des Schadens durch den Cyberangriff noch auf ihre Cyber-Versicherung verlassen, ist zukünftig damit zu rechnen, dass sich Cyberversicherer auf den sog. Kriegsausschluss berufen werden und eine Leistungspflicht verneinen. Dies mag auf den ersten Blick zwar nachvollziehbar sein, kann auf den zweiten Blick aber nicht überzeugen.

Kriegsausschlussklausel

Üblicherweise finden sich in den Bedingungen von Cyber-Versicherungen sog. Kriegsausschlussklauseln, wonach Schäden durch Krieg oder kriegsähnliche Ereignisse nicht versichert sind. Bereits vor dem Angriff Russlands auf die Ukraine versuchten Versicherer Cyberangriffe als Ereignisse einzustufen, die unter die Ausschlussklausel fallen und führten an, es handele sich um einen Cyberkrieg. **Dr. Marcel Straub, Head of Legal und Schadenexperte bei Finlex sieht dies anders:** „Verfangen hat diese Argumentation nicht, denn regelmäßig fehlte es bei den Angriffen an der zielgerichteten Handlung eines angreifenden Staates. Zudem ist herrschende Meinung, dass sich der Kriegsausschluss vornehmlich auf physische Kriegsakte bezieht."

Ukrainekrieg

Im Ukrainekrieg ist die Ausgangslage jedoch eine andere und es ist zu erwarten, dass sich Cyberversicherer vermehrt auf eine Leistungsfreiheit aufgrund des Kriegsausschlusses berufen werden. Es handelt sich vorliegend um einen hybriden Krieg, in dem der Cyberkrieg den physischen Kriegshandlungen beigemischt wird. „Vereinzelte Versicherer haben bereits angekündigt, dass sie die Kriegsausschlussklausel im Zusammenhang mit dem Ukrainekrieg grundsätzlich für anwendbar halten. Ein Angriff russischer Hacker auf deutsche Unternehmen wäre bei einer solchen Auslegung nicht versichert“, **so Dennis Wrana, Product Manager Cyber bei Finlex.**

Versicherungsvertragliche Einschätzung

Die Ansicht der Versicherer kann jedoch nicht überzeugen. Zum einen fehlt es bei den Angriffen an dem Merkmal der Zwischenstaatlichkeit, welches für die Bejahung eines Kriegs im Sinne der Kriegsausschlussklausel grundsätzlich notwendig ist. Insbesondere wenn der Cyberangriff von nicht-staatlichen Hackergruppen ausgeht, liegt keine zielgerichtete Handlung eines angreifenden Staates vor, und somit kein Krieg im Sinne der Definition. Zum anderen befindet sich Russland „lediglich“ mit der Ukraine im Krieg und nicht mit anderen Ländern. Selbst wenn ein Cyberangriff auf ein deutsches Unternehmen staatlich gelenkt sein sollte, so fehlt es weiterhin an einer offiziellen Kriegshandlung.

Dr. Marcel Straub kommt daher zu dem Schluss: „Solange sich Deutschland nicht im Krieg mit Russland befindet, ist die klassische Kriegsausschlussklausel daher nicht einschlägig. Darüber hinaus muss der Versicherer den Nachweis führen, dass es sich bei dem Cyberangriff um einen staatlich gelenkten Angriff handelt, wenn er sich auf den Leistungsausschluss berufen möchte. Der Nachweis wird dem Versicherer aber nur schwerlich gelingen, denn Hacker geben in der Regel nicht Preis, dass sie für eine Regierung handeln."
„Darüber hinaus ist es zumeist unmöglich, den tatsächlichen Ursprung des Angriffs zu lokalisieren. Die Möglichkeiten der technischen Verschleierung der Hacker wurden perfektioniert und in der Regel laufen diesbezügliche forensischen Untersuchungen ins Leere", **ergänzt Dennis Wrana**.

Lösegeldzahlungen bei Ransomware-Angriffen

Auswirkung auf die Cyber-Versicherung könnte der Ukrainekrieg jedoch auf die Zahlung von Lösegeld in Ransomware-Fällen haben. Hierbei greifen Hacker-Gruppen gezielt Unternehmen an und verschlüsseln deren Daten oder Systeme. **Dennis Wrana**: „Durch den Stillstand der Systeme droht den Unternehmen ein erheblicher finanzieller Schaden und ein eklatanter Reputationsverlust. Dies machen sich die Hacker zunutze und fordern von den angegriffenen Unternehmen Lösegelder in Millionenhöhe. Die Lösegeldzahlung ist grundsätzlich versicherbar und Policen, die einen solchen Baustein zur Zahlung von Lösegeldern enthalten, sind am Markt weit verbreitet und durchaus üblich."

Handelt es sich bei den Erpressern um russische Hackergruppen ist jedoch zu erwarten, dass Versicherer keine Zahlungen leisten werden. Vor der Zahlung eines Lösegeldes führen die Versicherer einen Sanktions- und Compliance-Check durch. Dieser hat unter anderem zum Inhalt, dass geprüft wird, ob die Angreifer auf einer Sanktionsliste stehen und somit keine Zahlungen an diese geleistet werden dürfen. Denn anderenfalls droht dem Versicherer und dem Unternehmen die Gefahr, selbst auf eine Sanktionsliste gesetzt zu werden. Aufgrund der umfassenden Sanktionen gegen Russland sind Lösegeldzahlungen an russische Hackergruppen in der Regel sanktionsbewährt und werden von Versicherern daher ggf. nicht mehr übernommen.

Fazit

Cyberattacken russischer Hacker gegen deutsche Unternehmen sind nach unserer Einschätzung weiterhin versichert. Die klassische Kriegsausschlussklausel ist nicht einschlägig, da es an dem Merkmal der Zwischenstaatlichkeit fehlt und sich Russland nicht im Krieg mit Deutschland befindet. Zudem ist der Versicherer dafür beweisbelastet, dass es sich bei dem Cyberangriff um einen staatlich gelenkten Angriff handelt. Die angegriffenen Unternehmen können sich bei der Bewältigung des Schadens durch den Cyberangriff daher weiterhin auf ihre Cyber-Versicherung verlassen. Erwähnenswert ist jedoch, dass es am Markt eine Vielzahl verschiedener Kriegsausschlussklauseln gibt. Es ist daher nicht auszuschließen, dass einzelne Kriegsausschlussklauseln anwendbar sind und sich der Versicherer zu Recht auf seine Leistungsfreiheit beruft. Zu Leistungsausschlüssen kann es zudem in Fällen von Ransomware-Lösegeldzahlungen kommen. Fallen die Hacker unter Sanktionen, dürfen keine Zahlungen geleistet werden."

Quelle: Finlex, Wolf-Rüdiger Senk