Krieg im Cyberland

Der Krieg in der Ukraine betrifft auch Bereiche, die nicht auf den ersten Blick im Fokus stehen. Die Möglichkeit von staatlichen Angriffen auf die Cyber-Infrastruktur eines anderen Landes ist real. Ein Krieg im Cyberland kann verheerende Folgen haben und auch die Cyberversicherer in Mitleidenschaft ziehen.

Eigentlich funktioniert die Cyberversicherung wie jede andere Versicherung auch. Es gibt eine Definition der versicherten Schäden. Im Wesentlichen geht es dabei um Haftpflichtschäden, wie z.B. die Verteidigung gegen den Vorwurf von Datenschutzverstößen infolge des Verlusts von sensiblen Kundendaten, oder Eigenschäden (z.B. Erpressung (Ransomware-Attacken) oder Betriebsunterbrechung und Assistance-Dienstleistungen (z.B. Krisenmanagement nach einer Attacke, auch Kundenansprache durch Callcenter nach Verlust von Kundendaten).

Bei den Ausschlüssen vom Versicherungsschutz geht es zwar um im Prinzip versicherbare Schäden, die jedoch entweder ein einzelner Versicherer aufgrund seiner individuellen Geschäftspolitik oder alle Versicherer aufgrund fehlender Versicherbarkeit nicht versichern wollen. Einer der ältesten Versicherungsausschlüsse ist der Ausschluss für Krieg an Land.

Der Cyberkrieg kommt nach Deutschland

Der klassische Kriegsausschluss ging von feindlichen Truppen aus, die eine Ländergrenze überschreiten. Dies ist bei der Ukraine gegeben. Alle Schäden dort sind nicht versichert. Auch bedurfte es früher einer offiziellen Kriegserklärung, damit man sich im Krieg befand. Das wird bei der „Spezialoperation“ der russischen Streitkräfte schon von russischer Seite bestritten. Krieg liegt im Auge des Betrachters könnte man sagen. Im weltumspannenden Cyberland gelten diese Kriterien nicht mehr. Auch können auf einmal nichtstaatliche Organisationen wie „Anonymous“ einen „Krieg“ gegen ein Land erklären. So geschehen am 24.02.2022: „The Anonymous collective is officially in cyber war against the Russian government.“. Muss es sich Deutschland als Land zurechnen lassen, wenn ein Mitglied von „Anonymous“ Deutscher ist oder in Deutschland lebt?

Hinzu kommt, dass eine Zahlung von Lösegeld nach einer Ransomware-Attacke (Verschlüsselung von Programmen zur Erzielung eines „Lösegelds“ zu Freischaltung) bei staatlichen russischen Tätern schwierig werden dürfte. Grundsätzlich sind Zahlungen dieser Art in den meisten Cyberversicherungen abgedeckt. Steht irgendein Beteiligter auf der Sanktionsliste, kann dies eine Zahlung verhindern. Das Ergebnis ist, dass der Code für das Entsperren der verschlüsselten Software nicht erlangt werden kann und damit von einer dauerhaften Verschlüsselung und Unbrauchbarmachung auszugehen ist. Dies ändert die Gefährdungssituation jedes Unternehmens erheblich. Ein Treffer genügt, um versenkt zu werden, um in dem Bild des Krieges zu bleiben.

Wann ist Deutschland im „Cyberwar“?

Was müsste passieren, damit deutsche Cyberversicherer den in den Bedingungen vorhandenen Kriegsausschluss ziehen und dadurch leistungsfrei sein können? Der Cyberausschluss wird in dem Moment greifen, in dem Russland als Staat eine offizielle Kriegserklärung abgibt, dann liegt die sogenannte „Zwischenstaatlichkeit“ vor. Dies ist extrem unwahrscheinlich. Wenn aber in allen anderen Fällen plötzlich kritische Infrastrukturen angegriffen werden und wenn Sicherheitsdienstleister ihr Personal nicht mehr disponieren können, weil ihre IT nicht mehr funktioniert und wenn dies von russischen Cyberkriminellen verursacht wurde, ist dies schon Cyberkrieg? Und woher wissen wir, dass es sich um russische Täter handelt, wo doch die manipulierbaren Spuren auch absichtlich in diese Richtung deuten können? Und ist es eine Frage, ob 10, 1.000 oder 100.000 Unternehmen betroffen sind? Geht es um Quantität oder Qualität? Ist die neue Schadsoftware Hermetic Wiper, die alle Daten eines Computers unwiderruflich löscht und damit ganz klar nicht im Hinblick auf die Erzielung von Lösegeld entwickelt wurde, eine Kriegswaffe? Ist ein massiver Angriff auf das IT-System des Deutschen Bundestages eine Kriegserklärung an Deutschland? Und wenn ja, von wem? Das eröffnet viel Raum für Interpretationen.

BERND M. SCHÄFER

GESCHÄFTSFÜHRENDER GESELLSCHAFTER DER ATLAS VERSICHERUNGSMAKLER FÜR SICHERHEITS- UND WERTDIENSTE GMBH

Konsequenzen für Cyber-Versicherungen

Es ist jedoch festzuhalten, dass ein Versicherer, der sich auf den Kriegsausschluss beruft, das Vorliegen der in den Bedingungen definierten Kriterien auch beweisen muss. Und daran wird er regelmäßig scheitern, solange es keine Kriegserklärung von Russland gibt. Da es sich aber aus Sicht eines Versicherers möglicherweise um ein existenzgefährdendes Risiko (Kumulrisiko) handelt, wird er es häufig versuchen, versuchen müssen. Weiterhin wird sich die Anzahl der Versicherungsverträge verkleinern. Zum einen, weil der Beitrag für die Cyber-Versicherungen steigen wird und weniger Unternehmen diese Deckung kaufen. Zum anderen aber auch, weil sich Versicherer aus diesem Geschäftsfeld zurückziehen werden, woraus wieder steigende Beiträge bei den verbliebenen Versicherern resultieren.

Skurrile Konsequenzen: „Kauft nicht beim Russen“

Das Bundesamt für Sicherheit und Informationstechnik (BSI) hat am 15.03.2022 die Empfehlung ausgesprochen, die Virenschutzsoftware des Herstellers „Kaspersky“ nicht mehr zu nutzen. Begründet wird dies mit dem Zweifel an der Zuverlässigkeit des russischen Herstellers, der allerdings nicht näher ausgeführt wird. Kaspersky verteidigt sich: „Kaspersky ist ein privat geführtes globales Cybersicherheitsunternehmen, und als privates Unternehmen hat Kaspersky keine Verbindungen zur russischen oder einer anderen Regierung.“ Weiter wird ausgeführt, dass die Server in der Schweiz stünden und den höchsten Sicherheitsstandard erfüllen würden. Kein neutraler Betrachter kann auf Basis belastbarer Fakten entscheiden, was die richtige Entscheidung ist. Es geht hierbei um die Existenz eines großen Unternehmens versus die Sicherheit der Nutzer der angebotenen Produkte in Zeiten eines Krieges. Der Krieg ist angekommen im Cyberland. Und der Wechsel der Virenschutzware bedeutet für Unternehmen zusätzliche Aufwendungen für neue Lizenzen und das Implementieren der neuen Lösung. Noch haben die deutschen Cyberversicherer davor zurückgescheut, dies ihren Versicherungsnehmern als deckungsrelevante Auflage (Obliegenheit) aufzuerlegen, wenngleich es Äußerungen gibt, wonach ein Festhalten an der Kaspersky-Software zu Problemen im Schadenfall führen kann. Aber es erscheint zum Zeitpunkt des Verfassens dieses Artikels nur eine Frage der Zeit zu sein, bis dies der Fall ist. Denn die Aufwendungen für die Umrüstung tragen die Unternehmen, die Schadenaufwendungen die Versicherer. Und die werden eher die Aufwendungen externalisieren als sehenden Auges ein durch eine solche Maßnahme vermeidbares Risiko einzugehen.

Cyberversicherung ist unverzichtbar

Aus dem Vorgenannten könnte man zu dem Schluss kommen, dass eine Cyberversicherung unnötig sei, weil sich der Versicherer im Schadenfall einfach aus dem Staub machen könnte. Das wäre ein falscher Schluss. Zum einen werden in dem vorliegenden Artikel vor allem die möglichen Auswirkungen des in der Cyberversicherung üblichen Kriegsausschlusses betrachtet. Die „normalen“ Kriminellen gehen ihrem kriminellen Gewerbe nach wie vor nach und verursachen „normale“ Schäden, so dass hierfür immer auch ein entsprechender Schutz erforderlich ist. Notwendig ist hingegen noch mehr als bisher die sofortige Unterstützung in der Krise eines Angriffs auf das firmeneigene IT-System durch die Assistance-Dienstleister der Versicherer. Alles andere kann von Juristen später verhandelt werden. Besser ist es, man streitet sich über eine Deckung, als wenn gar kein Vertrag vorhanden ist. Sinnvoll ist es weiterhin, eine Firmenrechtsschutzversicherung einzudecken, die auch Deckungsklagen gegen einen Versicherer abdeckt, wodurch Waffengleichheit hergestellt wird. Bei Klagen bis zum BGH ist dies eine sinnvolle Vorsichtsmaßnahme. Aber auch beim Firmenrechtsschutz gibt es einen Kriegsausschluss.

Wenn die Queen auf dem Tisch tanzt

Peter Niggl
Chefredakteur

Sehr geehrte Leserin, sehr geehrter Leser,

wir leben in unruhigen Zeiten. Nein, damit meine ich nicht die alltäglichen Horrorberichte über Krieg und Pandemie, die längst unseren Alltag beherrschen. Hinter den beunruhigenden Schlagzeilen gibt es – oft nur als Randnotiz – Meldungen, die es wert sind, gleichfalls Beachtung zu finden. Die Ablenkung durch das große Weltgeschehen ist der Nebel, in dem Fälscher ihr Handwerk zu neuen „Glanzleistungen“ perfektionieren. Langer Rede kurzer Sinn: Es geht um Deepfake. Der Begriff Deepfake ist ein Kofferwort aus Deep Learning und Fake. Dabei werden mit Hilfe von künstlicher Intelligenz Bilder, Audio- oder Videofälschungen gefertigt, die echte Inhalte vortäuschen. Eine Entwicklung, die noch ganz am Anfang steht und dennoch beängstigende Ergebnisse erzielt.

Das beste Beispiel für die Möglichkeiten der Deepfake-Manipulation war Mitte März, als auf Facebook ein Videoclip auftauchte, der eine vermeintliche Ansprache des ukrainischen Präsidenten Wolodymyr Selenskyj zeigte, in der er die Soldaten seines Landes aufforderte, die Waffen niederzulegen und zu kapitulieren. Eine Fälschung, die zwar von Facebook und seinem Mutterkonzern Meta identifiziert und entfernt wurde, aber über Stunden viral ging.

Der Vorgang verdeutlicht, wie mit Deepfake Nutzer des Netzes an der Nase herumgeführt werden können. Natürlich nutzen innovative Betrüger diese neuen technischen Möglichkeiten. Schon vor einiger Zeit ereignete sich ein Vorfall, bei dem ein britisches Tochterunternehmen vom Chef der deutschen Muttergesellschaft zu einer Zahlung aufgefordert wurde. Die Story kurzgefasst: In Germany sei es schon nach 16 Uhr, im Vereinigten Königreich eine Stunde früher. Da man unbedingt noch eine Zahlung leisten müsse, solle das die Firma in England übernehmen. Damit waren 220.000 Euro unwiederbringlich futsch.

Die Briten waren von der vertrauten Stimme ihres deutschen CEO hinters Licht geführt worden – sie wurde vom Computer imitiert, Deepfake. Hätten sie damals schon das YouTube-Video gesehen, in dem die Queen während der Weihnachtsansprache auf dem Tisch tanzt, wären sie vielleicht stutzig geworden. Bei genauem Hinsehen, ist zu erkennen, dass der Deepfake-Queen einige Sorgenfalten des Originals fehlen, abgesehen von dem Unfug den sie da redet. Spätestens beim royalen Tabledance muss dann jedem ein Licht aufgehen, dass dies für die über 90-Jährige ein bisschen zu viel des Flotten ist.

Je größer der Bildschirm, auf dem solche Deepfakes zu sehen sind, umso schneller müssen Zweifel aufkommen. Dort lässt sich schneller erkennen, welche Attribute der Kunst-Person fehlen, zum Beispiel das übliche Blinzeln. Dass viele Social-Media-Nutzer sich inzwischen mit dem Display ihres Smartphones begnügen, spielt den Fälschern in die Hände. Ganz abgesehen davon, mit welcher fast kindlichen Gutgläubigkeit sich mancher Zeitgenosse auf die Flimmerkästen einlässt!

Den Deepfakes, schon als Social Engineering 2.0 apostrophiert, wird den Sicherheitsverantwortlichen verstärkte Aufmerksamkeit abverlangen.

Ihr

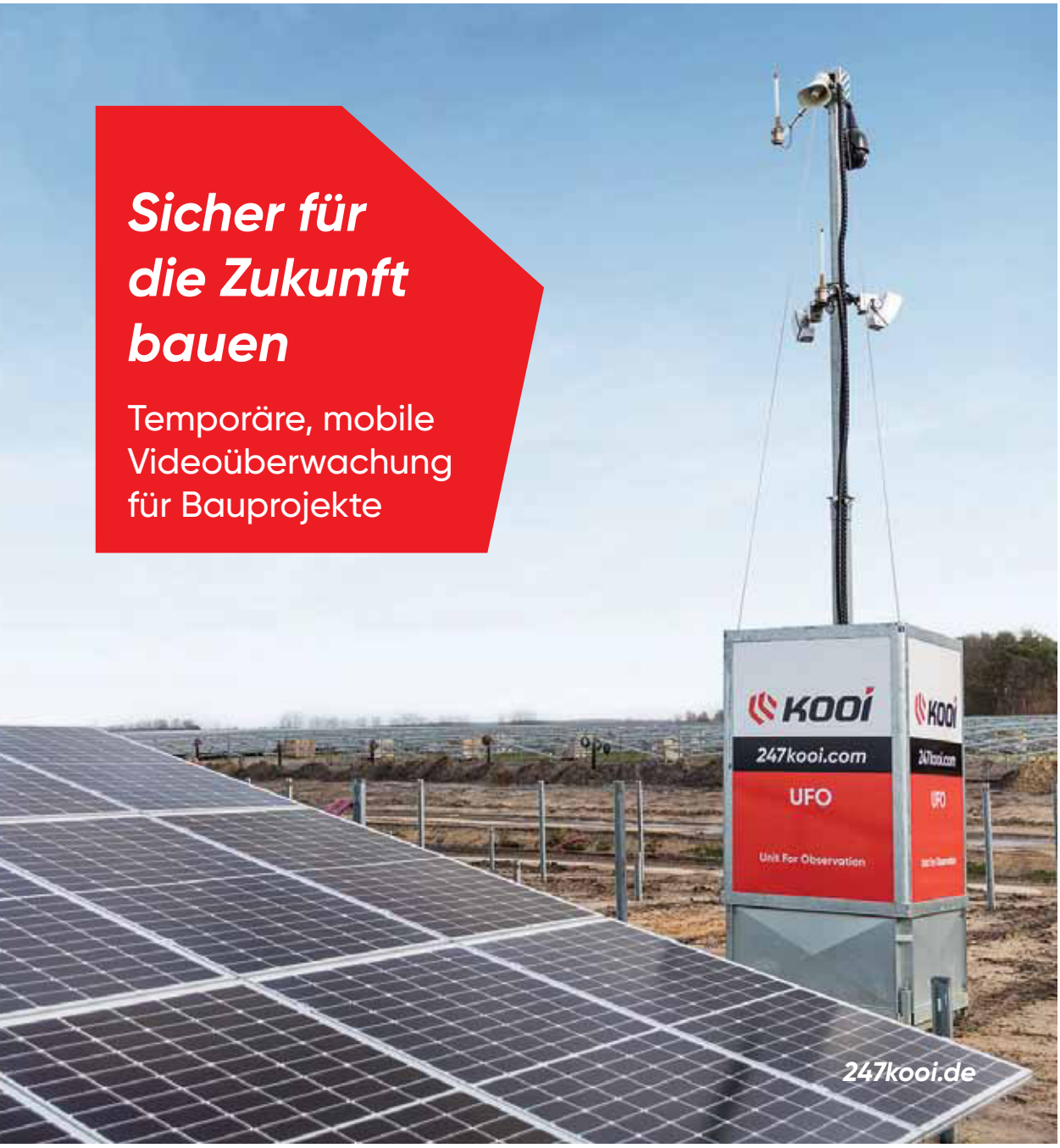
Peter Niggl

77500

ISSN 1866-2420

SECURITY INSIGHT

FACHZEITSCHRIFT FÜR UNTERNEHMENSSICHERHEIT UND WIRTSCHAFTSSCHUTZ



März/April
02/ 2022
EPr. 15,– €

www.prosecurity.de