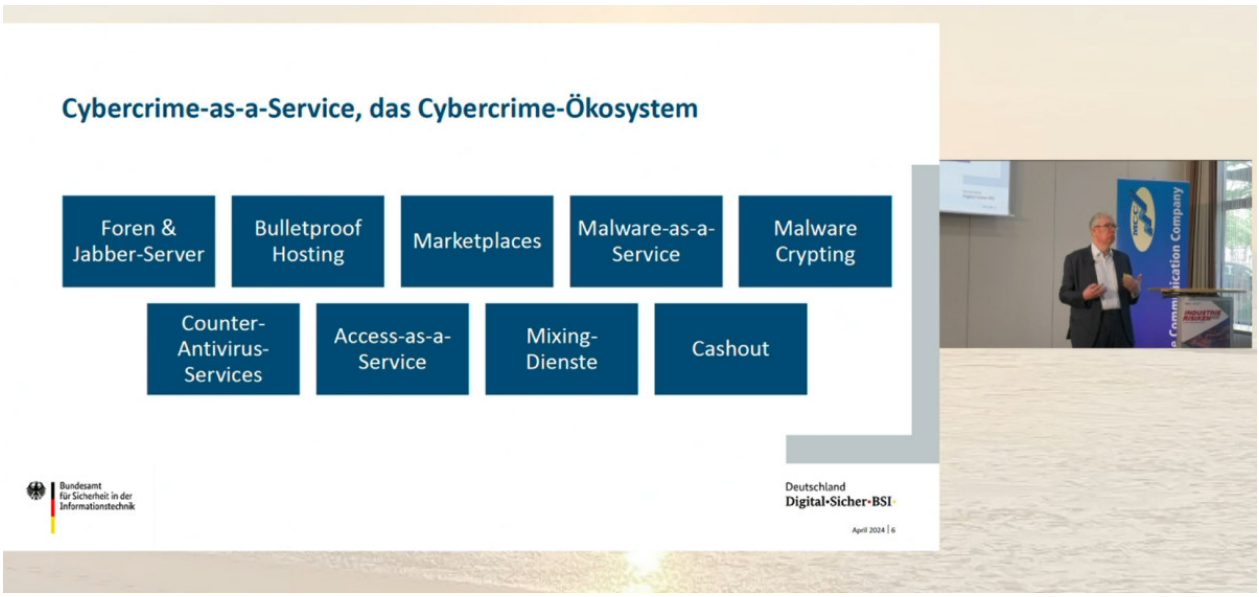
Cyber-Experte Erichsen: „Einen Großteil der Cyberschäden kann man verhindern, also kann man sie auch versichern“

11. April 2024

Auf dem MCC-Event "Industrierisiken" sprachen u.a. Dr. Harald Niggemann vom BSI sowie Dr. Sven Erichsen von der Finlex GmbH. (Bildquelle: MCC; dg)

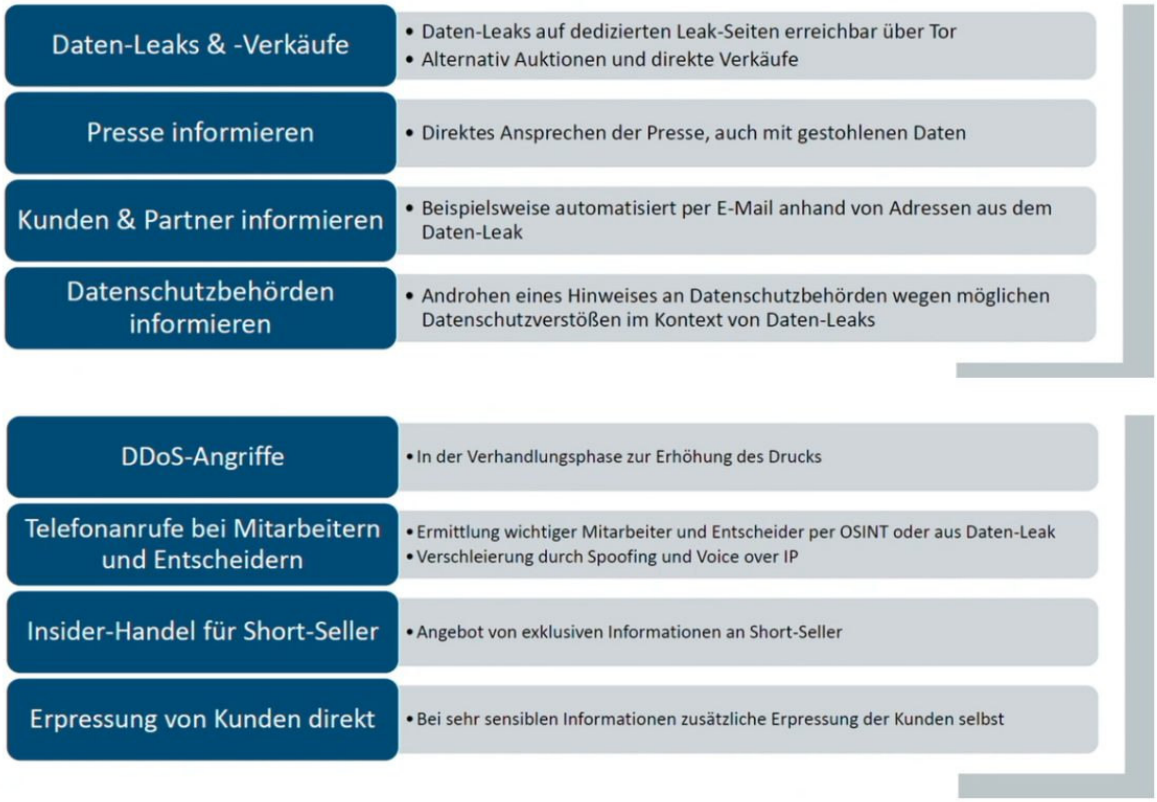
Der zweite Tag des MCC-Events zu „Industrierisiken“ widmete sich u.a. der Cyberversicherung. Dr. Harald Niggemann, Cyber Security Strategist beim Bundesamt für Sicherheit in der Informationstechnik, sprach über die aktuelle Gefahrenlage und das Ökosystem der Täter, die wählerischer und professioneller geworden sind. Wird mit der rasanten KI-Entwicklung noch alles schlimmer? Sven Erichsen von der Finlex GmbH sieht die Schadenseite derzeit jedoch unter Kontrolle. Mit der richtigen Prävention lasse sich jeder Angriff abwehren. Vor diesem Hintergrund wird die Cybersparte seiner Meinung nach weiter boomen.

Hacker haben ihr Geschäftsmodell so arbeitsteilig aufgebaut, wie man das aus der realen Geschäftswelt kennt, sagt Dr. Harald Niggemann vom Bundesamt für Sicherheit in der Informationstechnik. Und all diese Dienstleistungen könne man einkaufen. Beim „Access-as-Service“ holt man sich etwa Leute, die als Erstes den Fuß in die Tür bekommen. „Und danach laufen dann weitere Angriffsschritte ab, wie das laterale Ausbreiten im Unternehmensnetzwerk, das Infiltrieren der Server, das Filtrieren der Endgeräte und das Ausbreiten des Chart-Codes und so weiter.“



So gebe es auch Menschen, die im Rahmen des Hackerangriffs die Kommunikationsdienstleistung bereitstellen. „Es gibt diejenigen, die Server bereitstellen für Kriminelle, die nicht von Strafverfolgungsbehörden erkannt oder stillgelegt werden können, sogenannte Bulletproof Hosting Services. Es gibt Marktplätze, wo kriminelle Dienstleistungen angeboten und versteigert oder verkauft werden.“

Bei den Trends erkennt er das Big-Game-Hunting: „Die Tätergruppen wollen ihren Aufwand, ihr Gewinnaufwandsverhältnis verbessern, indem sie gezielt Organisationen angreifen, die sie auch als zahlungskräftig und zahlungswillig einstufen.“ Da gebe es auch viele Methoden, um entsprechenden Druck auszuüben. Die Hacker würden sofort die Datenschutzbehörden, die Presse oder die Kunden informieren, auch Insider-Informationen für Shortseller werden bereitgestellt.



Trends bei Erpressung im Big Game Hunting (Folien: BSI)

Mit ein Grund, warum es so viele erfolgreiche Hackerangriffe gibt, ist laut Niggemann die fehlende Kenntnis von der Software-Lieferkette. Wie bei einer echten Lieferkette haben sie bei einer Software-Lieferkette kaum einen Überblick über deren Bestandteile. Und weil es bei einer Software viele Zulieferer und Entwickler gibt, „ist es oft überhaupt gar nicht mehr möglich nachzuvollziehen, was dann da überhaupt nachher am Ende des Tages alles drin ist.“

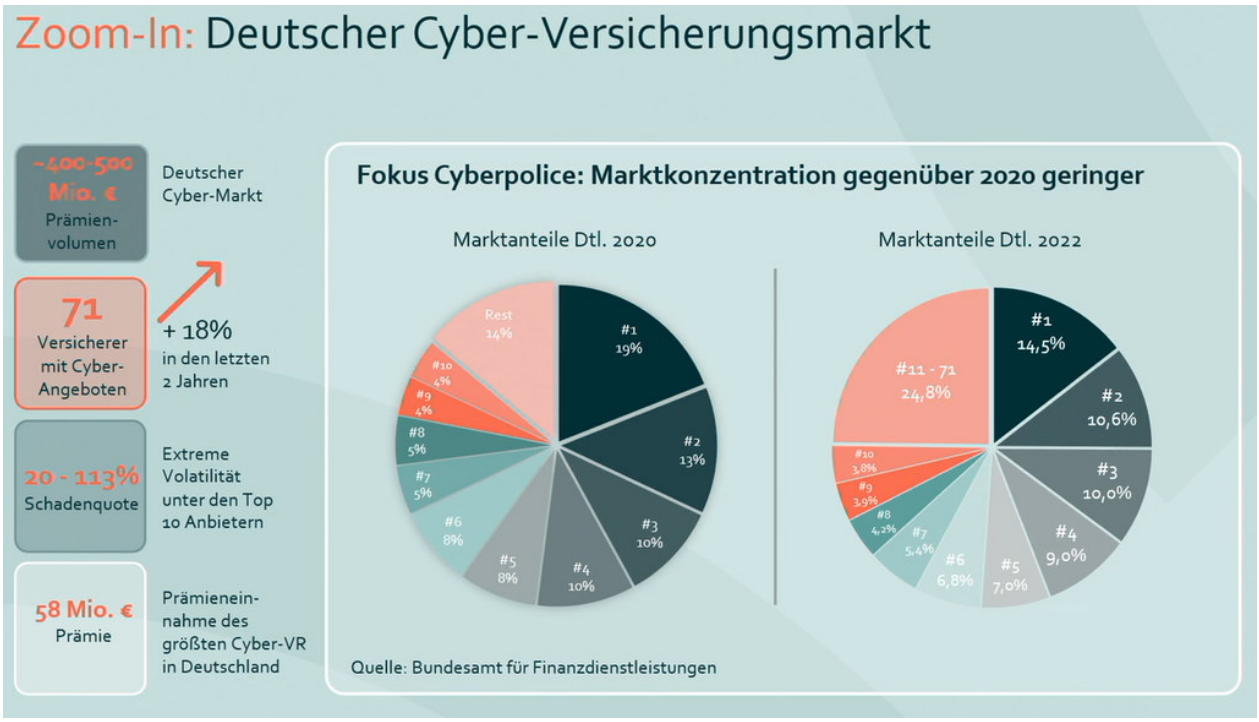
Prognose: Hacker werden die Input-Daten der KI angreifen

Dadurch hole man sich unter Umständen Sachen ins Haus, wo man gar nicht wusste, dass man das hatte. Das sei ein Riesenthema in der Cyber Security. Man müsse dazu kommen, dass man nachvollzieht, welches Stück Software eigentlich aus was zusammengebaut ist, denn eine Software habe Schwachstellen. „Und Schwachstellen ermöglichen es den Tätergruppen, ins Unternehmensnetzwerk reinzukommen, auch solche Schwachstellen, die tief verborgen in der Lieferkette eines Softwareproduktes drin sind."

Das ist für Niggemann der aktuelle Stand der Gefahrenlage und mit der KI-Entwicklung kommen weitere Trends hinzu. Auf der Haben-Seite können Unternehmen mithilfe von KI die Detektion und die Vorhersage verbessern. Die Gegenseite werde auch diese KI als Waffe einsetzen, sodass man noch besseres Targeting und noch bessere Angriffsmethoden sehen werde. Man werde seiner Meinung nach auch Angriffe auf die KI sehen bzw. man wird versuchen, die Input-Daten der KI zu manipulieren. Dadurch könne man vielleicht nicht direkt die KI kompromittieren, „aber Hacker können diese Informationsquellen vergiften, sodass bei ihnen im Unternehmen die KI falsche Entscheidung trifft".

Die Schäden sind gleich und Deutschland ist für Hacker besonders attraktiv

Die Cyberversicherung wird in der heutigen Zeit als die Feuerversicherung des 21. Jahrhunderts bezeichnet. Auch der ausgewiesene Experte Dr. Sven Erichsen, der bei Aon, Hendricks & Co GmbH und nun bei der Finlex GmbH seine Erfahrung mit einbringt, hält die Parallele mit der Feuersparte für sinnvoll, „weil die Mechanismen so ähnlich sind". In der Sachversicherung spricht man viel über Lieferketten, ebenso bei Cyber. Erichsen blickte zurück auf die Anfangsjahre, wo es vor zehn Jahren nur wenige Anbieter gab. Seitdem habe sich das Prämienwachstum stark beschleunigt und liegt in Deutschland derzeit bei 500 Mio. Euro. Die 1-Mrd.-Euro-Marke dürfte in ein paar Jahren geknackt sein. Inzwischen gibt es nach seinen Berechnungen 71 Versicherer, die hierzulande Cyberpolicen anbieten. Die Kapazitäten dieser Anbieter variieren stark, je nachdem, wie stark sie zuletzt von Schäden betroffen waren. Auf der Finlex-Plattform würden KMUs in der Regel mit einem Umsatz bis 3 Mrd. Euro nach einer Deckung zwischen fünf und 10 Mio. Euro nachfragen.



Die Schadenquoten der 71 Versicherer reichen von 28 Prozent bis 113 Prozent. Er merkt an, dass die Schadenursachen und die Schäden an sich eigentlich einheitlich seien und die Angriffe nach demselben Prozess ablaufen. Das bedeutet seiner Meinung nach, dass sich Investitionen in Cybersicherheit für Unternehmen lohnen. Nach einer kurzen Delle nach Beginn des Ukraine-Krieges sind laut Erichsen die Schäden weiterhin auf hohem Niveau. Im Übrigen deutet diese Delle seiner Meinung nach darauf hin, dass die Hacker aus Osteuropa und Russland agieren.

Bei Finlex wurde die Erfahrung gemacht, dass man in 40 Prozent die Schäden reguliert und in 25 Prozent das Problem über die Hotline lösen kann. Erneut hier der Vergleich: „Wie in der Feuerversicherung bringt der Cyber-Versicherer die Feuerwehr mit und sie bezahlt auch." Das heißt, die Assistance-Leistung ist mit eingebaut. „Und das scheint ja auch ganz gut zu wirken." Global gesehen ist die deutsche Schadenstatistik schlechter als in der restlichen Welt, gemäß der Zahlen der Bafin. „Kleiner Trost: In der Rückversicherung ist es noch schlechter", so Erichsen. Er schließt daraus, dass der deutsche Markt für Kriminelle sehr attraktiv ist, weil man konsistent hohe Großschäden hat. Aber Erichsen vertritt die These, dass man jeden Schaden verhindern kann, wenn man sauber genug aufgestellt sei. „Weil die Angriffe bisher so relativ einheitlich ablaufen, bleibt es auch versicherbar."

Autor: David Gorr