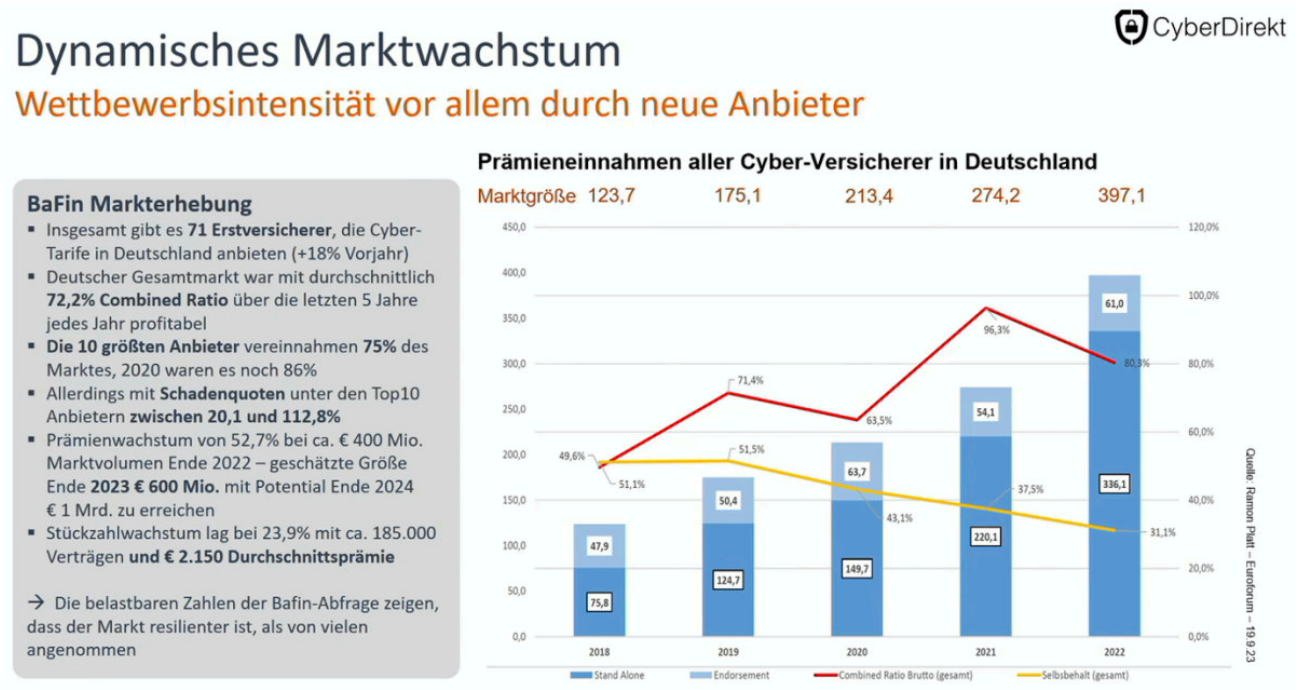
# CyberDirekt rechnet mit einer Mrd. Euro Prämienvolumen in der Cyberversicherung bis Ende des Jahres

7. Juni 2024


Hanno Pingsmann ist Gründer und Geschäftsführer von CyberDirekt und seit 15 Jahren im Finanz- und Versicherungsbereich tätig (Bildquelle: CyberDirekt)

Die Prämieneinnahmen der Cyberpolicen haben laut der Ratingagentur S&P weltweit ein Volumen von rund 15 Mrd. Dollar (13,8 Mrd. Euro) erreicht. Hierzulande dürften sie Ende 2024 bei einer Mrd. Euro liegen, prognostiziert CyberDirekt-Geschäftsführer Hanno Pingsmann auf dem MCC-Event „IT-Optionen für Versicherungen“. Er kann Versicherer durchaus verstehen, die Lösegeld zahlen, da es im Schadenfall günstiger sei als pro Woche 200.000 Euro an Deckungsbeitragsverlust hinzunehmen. Schließlich kassiert ein IT-Forensiker 400 Euro die Stunde.

Die Bafin fragt in regelmäßigen Abständen Cyberversicherer nach ihrem Geschäft ab. Die letzten Daten stammen aus dem Jahr 2022 und besagen, dass es hierzulande 71 Anbieter gibt, die 2022 auf ein Prämienvolumen von 400 Mio. Euro kamen. 2023 dürften es etwa 600 Mio. Euro sein und Ende 2024 knackt man wahrscheinlich die 1-Mrd. -Euro-Marke. Davon ist CyberDirekt-Geschäftsführer Hanno Pingsmann überzeugt, schließlich beobachtet er ein jährliches Wachstum von 50 Prozent in dieser Sparte. Aber es sei ein dynamisches Umfeld. „Es treten regelmäßig neue Anbieter ein, gerade ausländische Versicherer und Assekuradeure. Es treten auch regelmäßig wieder welche aus“, sagte er auf der MCC-Fachkonferenz „IT-Optionen für Versicherungen“. Er findet es bedauerlich, dass Axa Deutschland Cyberpolicen für Unternehmen mit einem Umsatz von über 5 Mio. Euro werden zum 1. Juni dieses Jahres eingestellt hat. „Ich bin sicher, dass andere Versicherer ähnliche schmerzhafte Entscheidungen in der Zukunft tätigen müssen“, so seine Einschätzung.



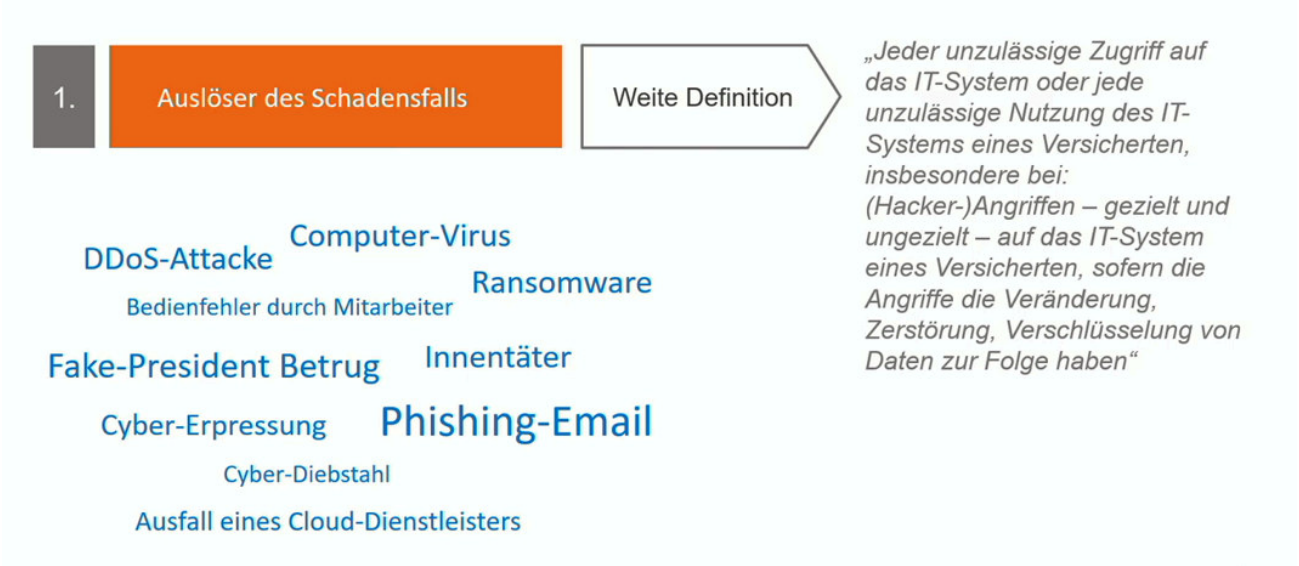

## Lösegeldzahlungen wohl günstiger als eine langwierige Schadenregulierung

Er betont, dass der Markt insgesamt in den vergangenen fünf Jahren mit einer Combined Ratio knapp über 70 Prozent profitabel war. Aber den Cybermarkt dominieren nur wenige Anbieter. Die zehn größten Anbieter vereinnahmen 75 Prozent des Marktes. Wer genau diese Anbieter sind, teilt die Bafin nicht mit. Auch Pingsmann nannte keine Namen. Aber für die in der Cybersparte tätigen Manager ist das kein Geheimnis, es sind die üblichen Verdächtigen. In der Top Ten sind etwa HDI, Allianz, Ergo, Hiscox und auch die AIG vertreten.

Bei all den Playern sind die Kosten bei einem Schadenfall ähnlich (siehe Folie). Pingsmann nimmt beispielhaft ein mittelständisches Unternehmen mit 20 Mio. Euro an Umsatz, das von einer Ransomware-Attacke betroffen ist. Die ersten Kostenblöcke, 200.000 für Krisenmanagement und IT-Forensik seien schnell ausgegeben. Schließlich kassieren IT-Forensiker in der Regel 400 Euro die Stunde, lässt Pingsmann wissen. 200.000 durch 400 geteilt, ist man bei 500 Stunden und bei einem Sechs-Mann-Team sind das 80 Stunden. „Das heißt, das ist eine Woche IT-Forensik und Krisenmanagement, weil die Arbeitswoche ist natürlich dann dementsprechend auch intensiv, wenn ein Unternehmen in so einer Notlage ist“, rechnet Pingsmann vor.

Für wichtig hält er auch bei den Kosten für die PR nicht zu sparen. In den ersten Tagen dürfe man in diesem Zusammenhang bloß nicht verraten, „wie viel Daten abgeflossen sind, ob sensible Daten abgeflossen sind.“ Zum Punkt „Kosten durch Datenschutzverletzung“, sagt er: „Wir haben mittlerweile leider die Situation, dass in Deutschland sich sehr viele Rechtsanwalte oder Dienstleister in dem Umfeld darauf fokussieren, Verbraucher zu ermutigen, Schadensersatz aufgrund von Datenschutzverletzungen einzufordern.“ Zusammengefasst kann er verstehen, warum manche Versicherer lieber ein Lösegeld zahlen. Denn deren Überlegung sei: „Erleiden wir weiter 200.000 Euro Deckungsbeitragsverlust pro Woche oder zahlen wir am Ende einer Verhandlung mit einem Kriminellen ein Lösegeld von 100.000 Euro in der Hoffnung, dass wir zu 70, 80% alle Daten schnell wiederherstellen können?“ Er schätzt, dass etwa 20 Prozent der Versicherer im deutschen Markt Lösegeldzahlungen nicht übernehmen. Diejenigen, die das covern, erheben Auflagen, die zum Beispiel die Kunden dazu zwingen, absolutes Stillschweigen über diese Vereinbarung zu versprechen.

Pingsmann ging auch darauf ein, was eine Cyberversicherung alles abdecken sollte. Er empfiehlt dabei Tarife zu wählen, die den Auslöser des Schadenfalls möglichst weit definieren. „Die Versicherer, die das Geschäft seriös betreiben wollen, haben eigentlich keine andere Möglichkeit, weil die Dynamik der Angriffsszenarien ist so hoch, dass sie theoretisch alle sechs Monate Ihr Bedingungswerk aktualisieren müssten, wenn Sie eine abschließende Aufzählung, wie es in anderen Spaten üblich und Standard ist, hier durchsetzen wollen würden.“




## Einhaltung der IT-Mindestanforderungen ist das größte Problem der Sparte

Bei den Ausschlüssen zählt er 55 Varianten, die Versicherer in der Cybersparte wählen, aber nur drei sind in jedem Bedingungswerk enthalten, dazu zählen Vorsatz, Infrastruktur und Krieg. Pingsmann erläuterte aber, dass bis zum Ausbruch des Ukrainekriegs der Kriegsausschluss „mehr oder weniger im Copy-Paste-Verfahren von anderen Bedingungswerken auch in die Cyber-Versicherung übernommen wurde und da nicht ausreichend spezifiziert war, wie genau jetzt Krieg zu verstehen ist. Das Problem der Versicherer war natürlich, dass eine Definition von Krieg auf eine physische Kriegshandlung quasi abgestellt ist.“


Die faktische Grenze des Versicherungsschutzes ist seiner Meinung eigentlich gar nicht in den Bedingungen oder in den Limiten zu sehen, „sondern bei vielen Unternehmen, die wir

über unsere Makler kennenlernen, sind es die IT-Mindestanforderungen.“ Die Auslöser für einen Cyberschaden sind in der Regel weitgehend abgedeckt durch die breiten Schadensfalldefinitionen der Versicherer. „Es kommt darauf an, ob das in dem Fragebogen, was das Unternehmen angeben musste und was der Vorstand unterschrieb, ob das tatsächlich dann auch so der Realität entsprochen wird.“

Autor: David Gorr



---