4. Event „Toprisiko Cyber“

Gemeinsame Veranstaltung des BWV München und der VVB am 14.3.2025

Aus der Idee, 2022 mal gemeinsam, BWV und VVB, eine Cyberveranstaltung zu machen, ist mittlerweile eines der größten Cyberevents in Deutschland geworden. So konnten wir in diesem Jahr mit mehr als 220 Teilnehmerinnen und Teilnehmern zum vierten Mal in Folge einen neuen Rekord bei dieser hybriden Veranstaltung verzeichnen. Das Cyber-Fachkreisleiterteam der VVB ergänzte sich perfekt durch die Präsenz von Michael Steimer vor Ort beim BWV in München sowie durch Danijel Basic im Livestream/Chat via Zoom.

Nach einer kurzen Vorstellung der VVB durch Michael Steimer (inkl. Angebot einer assoziierten Mitgliedschaft an die Teilnehmerinnen und Teilnehmer), stellte Lars Moormann, Geschäftsführer des Gastgebers, das BWV München, die neue Struktur der ehemaligen Fachwirt-Ausbildung, jetzt Bachelor Professional, sowie speziell das Angebot im Bereich Cyber vor, in welchem das BWV München eine mittlerweile bereits zum 4. Mal ebenfalls gut etablierte, praxisorientierte Ausbildung anbietet.

An 5 Nachmittagen (je 5 Std) werden die Teilnehmer hybrid mit allen Aspekten der Cyberversicherung für KMU vertraut gemacht, von „A“ wie AVBs bis „V“ wie Vertriebstipps. Dieser Zertifikatslehrgang „Experte/*in Cyberversicherung (BWV)“ belegt auch Arbeitgebern und Kunden gegenüber ihre Kompetenz in dieser nach wie vor wachsenden Branche mit unverändert riesigem Potenzial.

Fachlicher Leiter, Moderator und Referent der Expertenausbildung ist ebenfalls Michael Steimer, unterstützt von Topreferentinnen und Referenten aus dem deutschen Markt.

Für das „Line-up“ der Vorträge, von der globalen Sicht über konkrete Vertriebsthemen bis zur Schadensituation, konnten wir Referenten von Munich RE, CyberDirekt und Markel gewinnen.

Carsten Topsch, Head of Cyber Reinsurance Underwriting and Business Devolopment bei Munich RE, referierte zu den Herausforderungen und Möglichkeiten der Cyberversicherung aus der Perspektive eines Rückversicherers.

Munich Re ist auch im Bereich Cyberversicherung der global führende Rückversicherer und kann deshalb auf Marktentwicklungen aus erster Hand in fast allen Regionen weltweit analysieren, was bei einer Branche wie Cyber mit globaler Relevanz, wie z.B. auch NatCat, Luft-/Raumfahrt oder Größt-Industrie, Vorteile bei der Bewertung der Risiken sowohl für Munich Re selbst als auch deren Kunden/Zedenten bietet.

Als derzeitige sowie künftige Herausforderungen nannte Topsch:

- höhere Raffinesse der Cyberkriminellen
- KI- und Technologiefortschritte
- Mangel an Cyber-Fachkräften
- Geopolitik
- regulatorische Anforderungen

- Risiken und Abhängigkeiten in der Lieferkette

All dies führt zwangsläufig zu einem höheren Cyberrisiko und mehr Schäden für Unternehmen sowie gleichzeitig zu einer steigenden Nachfrage nach Cyberversicherungen. Letzteres ist eine gute Nachricht vor dem Hintergrund, dass die Marktdurchdringung immer noch sehr gering ist – manche Schätzungen gehen von unter 10 % aus.

Lt. Schätzungen von Munich Re kann man davon ausgehen, dass die globale Marktprämie bis 2027 auf ca. 21 Mrd USD steigen wird (2025: 16,3 Mrd USD/2023 14,3 Mrd USD). In Deutschland könnte das Volumen der Cyberversicherung von heute 700 Mio USD auf ca. 1 Mrd USD steigen. Über 2/3 des Volumens wird in den USA generiert, ca. 1/4 in Europa. Asien/Ozeanien sowie Afrika und weitere Länder sind (noch) deutlich unterrepräsentiert.

> *» Das Thema Kumulrisiken wird oftmals sehr kritisch gesehen. Lt. Munich Re sind Kumulrisiken in vielen Bereichen berherrschbar, z. B. solche durch weit verbreitete und sich selbst verbreitende Malware, durch Cloud-Ausfall, Ausfall eines großen IT-Dienstleisters und gezielte Angriffe auf zahlreiche Versicherte. «*

Nicht versicherbar sind hingegen Schäden durch den Ausfall kritischer Infrastrukturen sowie Schäden durch Krieg und staatlich gesponsorte Cyberoperationen.
KI wird erhebliche Auswirkungen auf die Versicherungswirtschaft haben, zum einen durch Nutzung in der Branche und zum anderen sowohl bei Angriffs- als auch Verteidigungsmustern in der Cyberversicherung. Lt. McKinsey ist in 2024 die Anzahl von Phishing-Angriffen seit der Einführung kommerzieller generativer KI-Tools um 1.265 % gestiegen! Es wird erwartet, dass es beim Zugang zu KI-Technologie eine Kluft zwischen Individuen, Unternehmen und Nationalstaaten geben wird.

Ransomware (Erpressungssoftware) ist größter Risiko- und Schadentreiber, was sich auch in 2025 fortsetzen wird (Wachstum von 81 % von 2023 auf 2024). Durchschnittliche Lösegeldzahlungen haben sich verdoppelt (global auf 4 Mio USD lt. Sophos); deutliche Erhöhung der Ausfallzeit durch BU (Betriebsunterbrungen) auf jetzt 16 Tage; viele neue oder „umfirmierte“ professionelle Bedrohungsgruppen, die insgesamt fast 5.500 Leaks im Darknet veröffentlichten.

> » Wichtig im Zusammenhang mit KMU: Neben „Big Game Hunting“ zielen Ransomware-Gruppen zunehmend auf kleinere Unternehmen, da diese weniger Ressourcen zur Cybersicherheit zur Verfügung haben «

Das Cyber-Risikomanagement bleibt eine Herausforderung in jeglicher Hinsicht. Interessant ist die These, dass es 2025 Fortschritte im Bereich der Quantencomputing-Technologie geben könnte, mit einem Übergang zu quantensicheren Verschlüsselungsalgorithmen. (UN hat 2025 zum „Interntionalen Jahr der Quantenwissenschaft und Technologie“ erklärt.)

Ein positiver Ausblick auf die Cyberversicherung kommt auch vom World Economic Forum 2025. Es zeigt sich, dass eine Cyberversicherung Unternehmen dabei hilft, widerstandsfähiger zu werden. Unter als hoch resilient eingestuften Unternehmen hatten nur 7% keine Cyberversicherung.

Dies nur als kurze Zusammenfassung des spannenden Vortrages, bei dem natürlich auch diskutiert und viel gefragt wurde. Die Präsentation von Munich Re sowie auch die der anderen Referenten finden Sie als PDF zum Download beim BWV München sowie im internen Teil der VVB-Plattform.

Björn Blender, Leiter Maklervertrieb bei CyberDirekt, Berlin, gab einen Praxiseinblick zur Vertragserneuerung 2025 „An der Schnittstelle zwischen Anbieter und Vertrieb“. Der Rückzug oder das Insolvenzverfahren von Anbietern stellte Herausforderungen dar, und hinzu kamen noch Sanierungsschritte mit anbieterseitigen Kündigungen, die sowohl Makler als auch VN nicht ausnahmslos hinnehmen wollten.

CyberDirekt, gegründet 2018 und seither stetig wachsend, versteht sich als „Ausgelagerte Cyberabteilung“ des Vertriebs. CyberDirekt bietet einen umfassenden, automatisierten und übersichtlichen Marktvergleich (inkl. Rating) ein eigenes Präventionsangebot sowie Begleitung bei Schadenfällen. Insgesamt sind 30 Anbieter im Portfolio, bei 18 ist ein digitaler Abschluss möglich, fast 2.000 Vermittler sind angeschlossen. Bei aller Digitalisierung, die den Abschluss einer Cyberversicherung in weniger als 10 Minuten ermöglicht, ist trotzdem auch immer eine qualifizierte Beratung/ ein Austausch von bzw. mit den Experten im Team von Björn Blender möglich. Gute Voraussetzungen also, um sich ein realistisches Bild hinsichtlich der Marktsituation an der Schnittstelle zwischen Anbieter und Vertrieb zu machen.

Björn Blender berichtete, dass mehrere Dynamiken ineinandergreifen. Zum einen gibt es weitgehende Marktanpassungen durch Bedingungsanpassungen und Änderungskündigungen (Gothaer, beazley, Victor) oder Wegfall/Rückzug des Anbieters wie Cogitanda oder AXA, zum anderen etablieren sich neue Anbieter im Markt, meist Assekuradeure, wie Corvus, Baobab, stoik oder Coalition. Versicherer lernen aus Schadenfällen und passen die Risikoprüfung und auch -fragen an, wovon auch die Unternehmen durch einen besseren Schutz profitieren. Die Risikoerhebung wird insgesamt komplexer.

Björn Blender, CyberDirekt, Dauerthema im Vertrieb: Risikofragen

85 % der Anbieter haben in den ersten 3 Quartalen 24 eine Tarifanpassung vorgenommen (AVB, Kapazität, Risikoprüfung, Prämie). Risikofragen und Mindestanforderungen sind extrem uneinheitlich (es gibt keine Riskofrage, die von allen Anbietern gleich gestellt wird), wie die gesamte Struktur der Cyberversicherung überhaupt, was es für einen Makler, der neben Cyber noch andere Branchen betreut, extrem schwer macht, den Überblick zu behalten. Ärgerlich ist, dass von den Anbietern immer noch kaum bei den Risikofragen nach Branchen oder Unternehmensgröße unterschieden wird. Aus der Diskussion ergab sich, dass klare und wenn möglich wenige klar verständliche Risikofragen ein positiver Wettbewerbsfaktor sein können.

Neu ist der Trend zu automatisierten Scans zur Risikobeurteilung. Die meisten Anbieter, die neu in den Markt auf die CyberDirekt-Plattform gekommen sind, nutzen solche Scans.

Insgesamt wird der Risikoappetit der im Markt verbliebenen Anbieter ab der Jahreswende 24/25 größer und die Kapazitäten und die Flexibilität im Underwriting nehmen wieder zu. Auch die Präsentation von Björn Blender mit zusätzlich diversen Hinweisen zu den unterschiedlichsten Fragebögen finden Sie beim BWV oder bei der VVB intern zum Download.

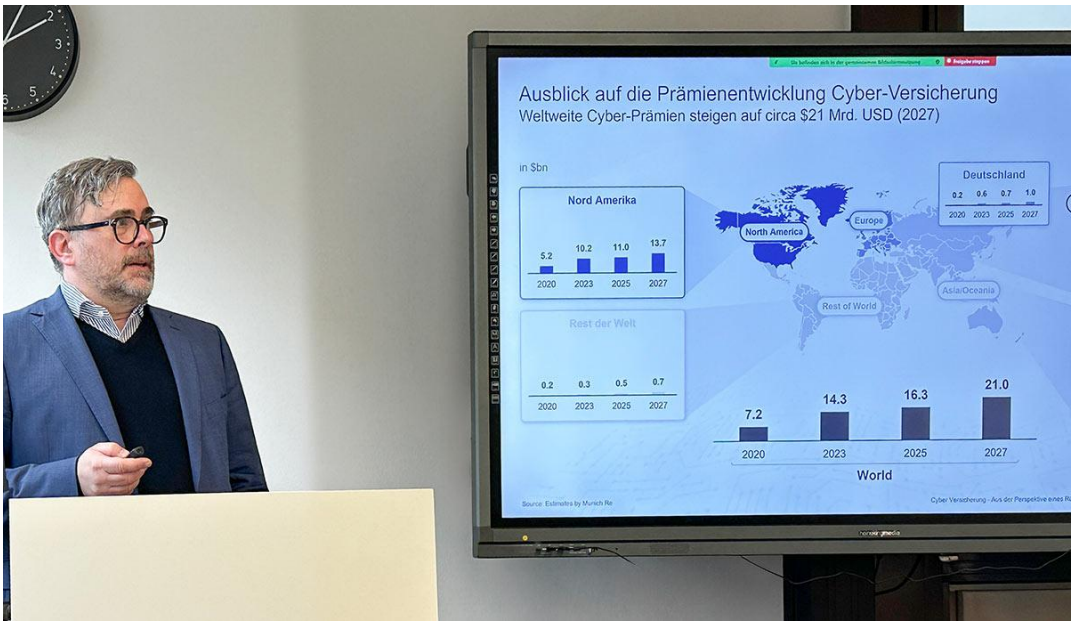
Michael Vogl, Senior Claims Handler und Marvin Knorr, Legal Claims Handler bei Markel Insurance, München, gaben uns ein Update zur Schadensituation/-praxis in der Cyberversicherung sowie am Ende nochmals einen bildhaften Überblick über das Leistungssprektrum bzw. die Deckungselemente einer Cyberversicherung anhand eines konkreten Schadenablaufs.

Markel ist ein amerikanischer Spezialversicherer mit einer langen Historie im deutschen Markt und hat hier, in München, auch sein europäisches Headoffice. Markel war zusammen mit Hiscox einer der Pioniere im deutschen Cybermarkt. Die gut strukturierte Police von Markel mit wenigen verständlichen Risikofragen findet bis heute viele Freunde im Vertrieb, zum einen wegen der Übersichtlichkeit, zum anderen auch, weil einzelne Module leicht ab- oder zugewählt werden können.

Michael Vogl und Marvin Knorr werden im nächsten VVBmagazin einen umfassenden Beitrag zu Ihrem Vortrag verfassen, deshalb nur ein ganz kurzer Überblick:

Wie schon von Munich Re gehört, ist Ransomware die häufigste Schadenursache; bei Markel liegt der Durchschnittsschaden bei ca. 55 Tsd.Euro. Schäden/Kosten entstehen durch Wiederherstellung der Systeme, Wiederbeschaffung verlorener Daten, Mehraufwand, Betriebsunterbrechung, Kosten für externe Dienstleister, Schadenersatzansprüche Dritter, z.B. Geschäftspartner.

Michael Steimer, Einführung in den Tag

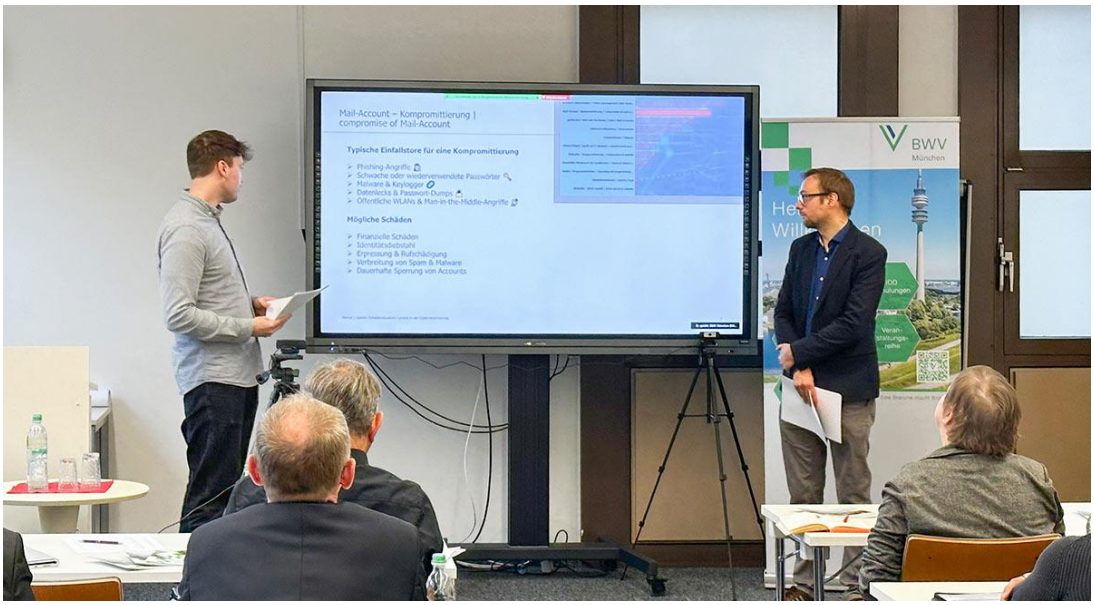


Carsten Topsch, Munich Re, Cyber bleibt auf Wachstumspfad

Wie auch schon in den letzten Jahren entspann sich beim Thema Lösegeld eine engagierte Diskussion. Nach wie vor gibt es valide Argumente dafür und dagegen. Im Falle einer drohenden Insolvenz eines VN ist es jedoch als Ultima Ratio und nach Ausschöpfung aller Abstimmungsobliegenheiten aus Sicht des VN günstig, wenn der darauf zurückgreifen könnte. Eine Reihe von Versicherern decken Lösegeld. Rechtlich spricht Stand heute nichts dagegen (§ 34 StGB).

Ein stark wachsender Bereich ist die sog. E-Mail-Account-Kompromittierung. Dabei kommt es zu einer Kompromittierung des E-Mail-Accounts durch einen Phishing-Angriff, ein Datenleck, schwache Passwörter oder die Nutzung öffentlicher WLANs ohne eigenen Schutz, z. B. VPN. Die Folgen können finanzielle Schäden, Identitätsdiebstahl, Erpressung oder Verbreitung von Spam oder Malware sein.

Weiter wachsend sind die Fälle, bei denen der E-Mail-Account eines Kunden, z. B. Zulieferers, kompromittiert wird. Es wird dann vom Server eines Geschäftspartners oder Dritten (z. B. angeblicher Insolvenzverwalter, Gericht) eine komplett gefälschte Rechnung versendet oder – die perfidere, intelligentere Variante – bei einer echten Rechnung wird lediglich die Konto-Nr. geändert. Bei der Diskussion ergab sich, dass es Gesellschaften gibt, die eine solche Zahlung an ein falsches Konto decken (also ohne eigene Informationssicherheitsverletzung), während andere dies nicht tun. Vermittler sollten darauf achten.



Michael Vogl und Marvin Knorr von Markel, zum Thema häufiges Schadenmuster, E-Mail-Account-Kompromittierung

Zum Schluss nahmen uns die Claims-Spezialisten von Markel- mit in eine virtuelle Geschichte, basierend auf einer Neflix-Serie (Zero-Day). Anhand der Abläufe einer Ransamware Attacke ermittelten die Teilnehmer die einzelnen Bestandteile/Leistungen einer Cyberversicherung. Das war spannend, und es wurde klar: Cyberversicherung ist viel mehr als finanzielle Entschädigung, sondern auch Krisenbewältigung, psychologische Hilfe, Existenzsicherung und vieles mehr.
Wir danken sehr herzlich allen Teilnehmerinnen und Teilnehmern für ihr Engagement, ihre Fragen und insbesondere unseren Referenten für spannende, praxisrelevante Vorträge. Wir freuen uns auf die nächste Veranstaltung im März 2026. Bis dahin, bleiben Sie gesund und in jeder Hinsicht virenfrei.

v.l. Lars Moormann, Marvin Knorr, Michael Vogl, Björn Blender, Carsten Topsch, Michael Steimer
Auch dem Osterhasen hat's gefallen, kleiner Dank an die Referenten für spannende und relevante Vorträge