09/24

secure mag

Der Risikodialog *als zentrale Herausforderung*
(Seite 2)

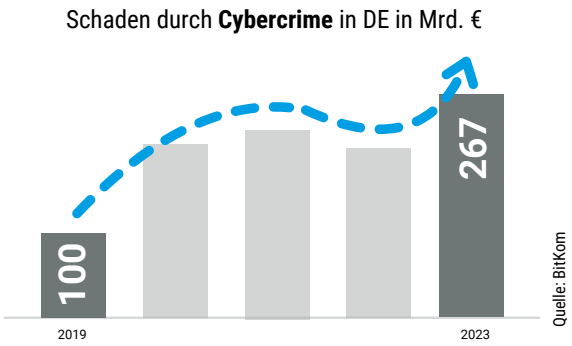
Versicherbarkeit ist keine Pauschalreise - worauf zu achten ist
(Seite 6)

Grenzen der Cyber-Versicherbarkeit

Warum manche Unternehmen nicht versichert werden können – *oder etwa doch?*

Einleitung

Die digitale Transformation ist noch lange nicht abgeschlossen. Neue Technologien und die zunehmende Vernetzung münden in der Implementierung neuer Prozesse. Mit zunehmender Digitalisierung steigt aber auch die Angriffsfläche für Cyberkriminelle. Cybercrime ist ein voll automatisierter Prozess und ein professionelles Business, gegen das es keinen 100%igen Schutz gibt.
BitKom beziffert den Schaden durch Cybercrime an der deutschen Wirtschaft im Jahr 2023 auf stolze 267 Milliarden €. Das bedeutet ein Wachstum von mehr als 60 Mrd. € und das obwohl die Awareness doch deutlich gestiegen ist.



Cyberversicherungen sind deshalb beliebt, um das Risiko der Folgeschäden durch Cyberangriffe deutlich zu reduzieren. Aber zur Wahrheit gehört auch: Eine passende Police zur erhalten ist gar nicht mehr so einfach. Versicherungsgesellschaften haben eine klare Vorstellung davon, welche Rahmenbedingungen für eine Policierung gegeben sein müssen. Bei sogenannten Red-Flags droht eine Ablehnung und der Status: nicht versicherbar. Die Gründe dafür sind vielfältig und reichen von Komplexität der Infrastruktur, über Sicherheitsstandards bis hin zu pauschalen Branchenausschlüssen.

Der Risikodialog als zentrale Herausforderung

Die Ablehnung durch die Versicherungsgesellschaft erfolgt in den meisten Fällen nachdem ein Fragebogen und/oder Risikodialog durchgeführt wurde. Hier ist das Unternehmen in der Regel mit verschiedenen Fragen konfrontiert, die lediglich mit ja oder nein beantwortet werden können. Ohne Erklärungen, erweist dich dieser Schritt bereits als große Hürde.
Die im Anschluss folgende Ablehnungen werden teilweise nicht begründet oder es wird lediglich auf kritische Punkte hingewiesen, die noch umgesetzt werden müssen.

Die Unternehmen stehen dann vor erheblichen Herausforderungen, da IT- und OT-Systeme oft über Jahre gewachsen sind und nicht einfach ersetzt oder erweitert werden können. Das Budget, die technische Machbarkeit oder der Faktor Zeit können solche Veränderungen erschweren, insbesondere wenn der Abschluss einer Cyberversicherung innerhalb eines Jahres angestrebt wird. In vielen Fällen ist es jedoch nicht möglich, die erforderlichen Maßnahmen innerhalb dieses Zeitraums umzusetzen.
Und weil das so ist, bleibt die Ablehnung bestehen. Wir wollen die häufigsten Ablehnungsgründe etwas intensiver beleuchten.

Gründe, warum ein Unternehmen als ‚nicht versicherbar' gilt

Falsche Branche. Pech gehabt?

Einige Branchen, die stark regulierte oder risikobehaftete sind, werden von Versicherungsgesellschaften ausgeschlossen. Sektoren wie Gesundheitswesen, öffentliche Einrichtungen, Logistik, Chemie und E-Commerce sind schwerer zu versichern, da sie komplexe IT- und OT-Systeme sowie internationale Niederlassungen umfassen und oft unzureichend gesichert sind. Das produzierende Gewerbe und der Dienstleistungssektor gelten zwar als leichter versicherbar, stehen jedoch ebenfalls vor Herausforderungen wie der Integration unterschiedlicher IT/OT-Systeme, mangelnder Standardisierung und umfangreichen Sicherheitszertifizierungen.

Keine Security – keine Versicherung.

Laut dem Allianz Risk Barometer 2023 sind Cyberrisiken nach wie vor die größte Bedrohung für die globale Wirtschaft. Der Anstieg der Schadensfälle hat dazu geführt, dass Versicherer strengere Anforderungen stellen. Als Beispiel ist die Mehrfaktor-Authentifizierung (MFA) heute ein absolutes Must-have für jede Cyberversicherung genauso wie fundierte Prozesse zur Erfüllung der DSGVO. Weitere Sicherheitsstandards wie regelmäßige Updates und effektive Bedrohungserkennung sind ebenfalls zu unverzichtbaren Anforderungen geworden, um den steigenden Risiken und Schadenspotenzialen zu begegnen.

Compliance, Zertifizierungen und Standards:

Das Fehlen anerkannter Sicherheitszertifizierungen oder die Nichteinhaltung von Standards wie ISO 27001 oder dem NIST Cybersecurity Framework kann die Versicherbarkeit beeinträchtigen. Diese Zertifizierungen sind für Versicherer ein Indikator für ein hohes Sicherheitsniveau und die Umsetzung von Best Practices im Bereich der Cybersicherheit. Ohne diese Zertifizierungen kann es schwierig sein, Versicherungsschutz zu erhalten, da das Risiko höher eingeschätzt wird. Perspektivisch werden weitere Richtlinien für einige Branchen relevant werden.

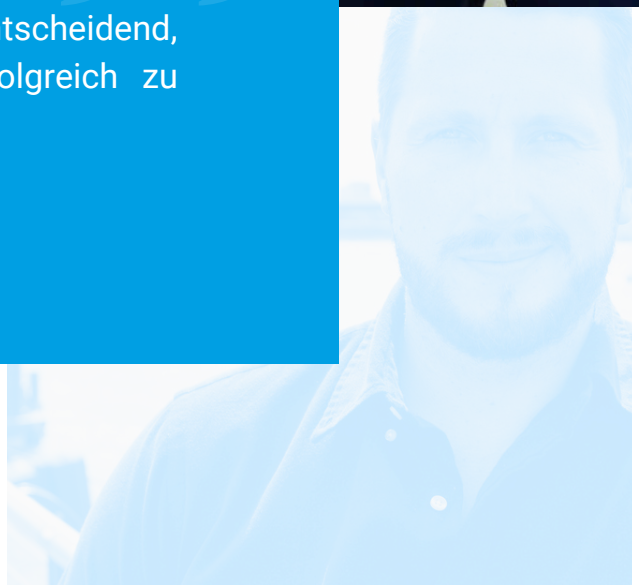
Mit ***NIS2*** kommen insbesondere für die Unternehmen der kritischen Infrastruktur weitere Auflagen und durch ***DORA*** für den Finanzsektor, die ebenfalls von ***NIS2*** betroffen sind.

Kürzlich erst gehackt? Dann wird's schwer.

Dein Unternehmen hatte kürzlich eine Cyberattacke? Das ist in der Regel keine wirklich gute Situation, um eine Cyberversicherung abzuschließen.
In den meisten Risikodialogen ist mit „kürzlich" ein Zeitraum von 5 Jahren gemeint. Der Versicherer interpretiert in diese Aussage, dass das Cybersecurity-Konzept kein gutes sein kann, sonst wäre der Vorfall nicht geschehen.
Dieser Punkt führt zu einer schlechteren Risikobewertung.

Die echte Herausforderung liegt oft in der Anpassung bestehender Strukturen an neue Sicherheitsanforderungen. Ein klarer Plan und transparente Kommunikation sind entscheidend, um den Versicherungsprozess erfolgreich zu gestalten.

Philipp Skucha
CEO securance GmbH



Versicherbarkeit ist keine Pauschalreise – worauf zu achten ist:

Springen wir noch einmal zu Punkt 1: dem Fragenkatalog oder oft bereits dem Risikodialog. Hier möchte der Versicherer ein Verständnis dafür bekommen, mit welcher Risikomasse er es zu tun hat. Das Abfragen von Risiken mit Ja- oder Nein-Fragen bietet jedoch nur eine sehr eingeschränkte Sicht auf die Dinge. Ein Beispiel aus einem solchen Katalog:

„Verfügen Sie über ein Team, welches die Meldungen von Sicherheitstools überwacht und alle Anomalien untersucht?"

Diese Frage lässt viel Interpretationsspielraum. Oft wird angenommen, wenn ich da kein 6-köpfiges Team mit dedizierter Security-Expertise vorhalte, muss es ein ‚Nein' sein.

Eine konservative Herangehensweise ist bei den Risikodialogen nicht immer förderlich. Es braucht eine faire Risikobewertung und das Mindset, dass nicht alle Punkte nach Best Practices erfüllt sein müssen.

Zudem ist es wichtig, bei der Risikobetrachtung sowohl die technischen als auch die organisatorischen Faktoren des Unternehmens zu berücksichtigen.

Expertise und Netzwerk

Nicht alle Makler haben alle Versicherer im Portfolio. Das bedeutet auch, dass ein Branchenausschluss bei Versicherer A bei Versicherer B vielleicht nicht gilt.

Der Makler sollte daher ein breites Portfolio haben, um solche Ablehnungen richtig einordnen zu können. Zudem ist es entscheidend, dass der Makler gute Beziehungen zu den Versicherern pflegt. In der Regel bedeutet das, dass der Makler über echte Expertise verfügt, die Risikolandschaft einschätzen kann und deshalb in der Lage ist, Verhandlungen im Sinne des Kunden zu führen. Wenn also Maßnahmen in der Zukunft noch umgesetzt werden müssen, kann der Versicherungsschutz trotzdem bereits direkt beginnen.

Beispiel: Ein Unternehmen hat ein Red Flag im Bereich MFA. Eigentlich würde das bedeuten, dass das Unternehmen nicht versicherbar ist. Wenn wir dem Versicherer jedoch zusichern, dass ein MFA-Projekt innerhalb der nächsten sechs Monate umgesetzt wird, kann der Versicherungsschutz in der Regel dennoch bereits direkt starten – und zwar in vollem Umfang. Den Nachweis über die Implementierung reicht der Makler dann entsprechend der Vereinbarung beim Versicherer ein.

Fremdbild vs. Selbstbild.

Gerade bei der Risikobewertung liegen die Einschätzungen oft auseinander. Während sich das Unternehmen möglicherweise „ganz gut aufgestellt“ sieht, hat der Versicherer möglicherweise bei manchen Angaben ein mittleres bis großes Problem.

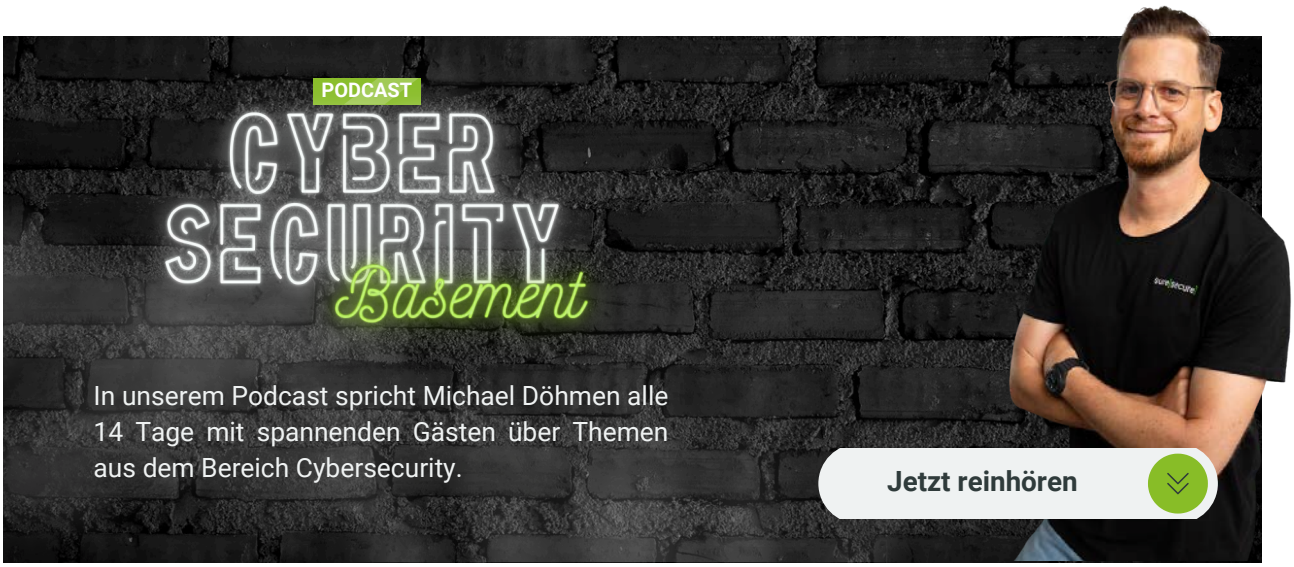
Diese Dissonanz kann nur überwunden werden, wenn die Struktur des Kunden und die Anforderungen der Versicherer zusammengebracht werden. Daraus entsteht dann die bestmögliche Cyberversicherung.

Deshalb ist es immer enorm wichtig, das Gespräch mit den Versicherern zu suchen, um genau diese Details zu verstehen und anschließend spezifische Lösungen zu diskutieren. Das gilt auch dann, wenn es in den letzten Jahren eine Cyberattacke gab.

Viele Versicherer sind oft zurückhaltend, geschädigte Unternehmen zu versichern, da das Risiko eines erneuten Angriffs auf den ersten Blick groß erscheint. Was viele Versicherer jedoch nicht direkt erkennen, ist die Tatsache, dass eine Cyberattacke mehr Chance als Risiko sein kann.

Denn aus einem Cyberangriff resultiert in der Regel eine deutlich stärkere Cybersecurity. Die gewonnenen Erkenntnisse führen dazu, dass wichtige Maßnahmen umgesetzt werden, was die Cyberresilienz verbessert.

Wird dieser Hintergrund im Detail mit dem Versicherer besprochen, kann das sogar zu einer besseren Versicherbarkeit zu optimalen Konditionen führen. Mit einer fundierten Analyse und einer klaren Roadmap kann ein spezialisierter Makler erfolgreich mit den Versicherern verhandeln. Gute Beziehungen zu den Versicherern und eine detaillierte Darstellung der Sicherheitsmaßnahmen erhöhen die Chancen auf einen passenden Versicherungsschutz.



Key-Take-Aways:

- Suche dir einen Cyberversicherungs-Experten
- Nicht-Versicherbarkeit nicht akzeptieren, sondern hinterfrage
- Bewusstsein und Transparenz für das eigene Risiko gewinne
- Strategische Entwicklung einer Cyberresilienz

Wir halten fest:

Die Nichtversicherbarkeit von Unternehmen ist häufig auf spezifische Herausforderungen und Anforderungen zurückzuführen. Durch eine gezielte Risikobeurteilung und die Entwicklung einer klaren Roadmap können Unternehmen ihre Versicherbarkeit jedoch verbessern. Ein spezialisierter Makler kann dabei helfen, den passenden Versicherungsschutz zu finden und die notwendigen Maßnahmen effizient umzusetzen.

Weitere Informationen zum Thema:

Podcast-Folge:

Mit Cyberaudit und IT
Sicherheit auf der sicheren Seite

Whitepaper:

Cyberaudit
Mit vereinten Kräften zur Resilienz:

securance GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 211 88 23 02 84

E-Mail: kontakt@securance.de
www.securance.de

Sidney Bauer
Cyber Specialist

Telefon: +49 (0) 2156 959 45 38
E-Mail: sidney.bauer@securance.de