

CYBERAUDIT

Mit vereinten Kräften zur Resilienz:
Cyberversicherung & Cybersecurity

WHITEPAPER

sure|secure| X securance

Akt 1

Pain.

Wir schreiben das Jahr 2024 und wieder Mal gibt es ernüchternde Zahlen aus der neusten BitKom Research Studie.

Wieder wird der Schaden durch Cyberkriminelle mit mehr als 200 Mrd. € angegeben.

Damit liegt dieser auf einem ähnlichen Niveau wie im Vorjahr. Aber erfreulich ist, dass die Unternehmen trotzdem deutlich an der eigenen Sicherheit schrauben. Der Budgetanteil für IT-Security steigt deutlich.

Denn die Gefahr ist nach wie vor groß.

Das Business der Hackerbanden ist so professionell und vollautomatisiert, dass sich eigentlich keine Branche, kein Unternehmen sicher sein kann, nicht auch mal Opfer eines Cyberangriffs zu werden.

So stellt sich immer wieder die Frage: Wie kann ich mich eigentlich optimal vor diesem Geschäftsrisiko schützen?


Simpel ist das nicht.

Es braucht Expertise, es braucht Technologien, es braucht die richtigen Menschen an den richtigen Positionen und es braucht zielgerichtete Prozesse. Und auch das kann noch zu wenig sein, da es eine 100%ige Sicherheit nicht gibt.

Es gibt aber darüber hinaus noch die Möglichkeit der Cyberversicherung, sprich Schäden, die durch einen Cyberangriff entstehen, präventiv absichern zu lassen. Aber auch das ist ohne bestimmte Basics im Bereich Cyber-Security kaum noch möglich.

Die Branche veröffentlichte 2022 Ablehnungsquoten von bis zu 70%. Von 100 Unternehmen können also nur 30 überhaupt eine Cyberpolice in Anspruch nehmen.

Warum ist das so und was kann ich als Unternehmer tun, um zu diesen 30% zu gehören?



Jährlich mehr als

200.000.000.000 Euro
(200 Milliarden!) Schaden durch Cyberkriminelle

Ausgangssituation.

Wir erleben im Bereich der IT-Sicherheit einen stark aktivierenden Staat. Das IT-Sicherheitsgesetz 2.0 wird perspektivisch noch ausgebaut werden, mit NIS2 gibt es zudem europäische Auflagen in diesem Kontext, da die erfolgreichen Angriffe noch viel zu hoch sind – **insbesondere im KRITIS-Sektor**.

Steigende Anforderungen.

Die Anforderungen werden auf ein Niveau steigen, welches für die meisten IT-Abteilungen kaum selbst zu administrieren ist. Früherkennungssysteme nach Stand-der-Technik, Netzwerksegmentierungen, Notfallpläne – für alles braucht es Expertise und diese kann so schnell kaum aufgebaut werden.

Komplizierte Prozesse.

Durch steigende Anforderungen wird der Prozess komplizierter. Jede neue Vorschrift landet auch in den Fragebögen der Versicherer und trägt dazu bei die Ablehnungsquote auszubauen. Zudem verzögern lange Fragebögen (teilweise über 200 Prüfparameter) den Prozess stark.

Unsicherheit im Schadensfall.

Komplizierte und teilweise unkonkrete Fragebögen bergen das Risiko, dass man die Fragen des Versicherers nicht in seinem Sinne beantwortet. Dies kann dazu führen, dass der Versicherer eine Police ausstellt, die er so gar nicht ausgestellt hätte.

Wer nicht auf die Details des Fragebogens und der Police achtet, kann im Schadensfall auch nur auf Teilleistungen hoffen oder sogar im schlimmsten Fall mit einer Nichtleistung rechnen. Deshalb ist es wichtig zu verstehen, welchen Hintergrund jede einzelne Frage hat und wann die Police unter welchen Voraussetzungen greift.

Alle Markteinflüsse zusammen führen auch zu steigenden Prämien, weil die Schäden für die Versicherer kaum abzuschätzen sind.

Also macht eine Versicherung jetzt doch keinen Sinn?
Doch, gerade jetzt. Aber wenn – dann sollte das Projekt richtig aufgesetzt werden und mit einer Auditierung starten.

Auditier mich.

Erster Grundsatz:

Eine Auditierung zur Versicherbarkeit oder von einer bestehenden Police sollte unter keinen Umständen ohne IT-Security Know-How stattfinden.

Es braucht definitiv Fachpersonal, um eine fundierte Bewertung abgeben zu können.

Zweiter Grundsatz:

Versichert sein ist gut, versichert bleiben noch viel besser. Deshalb gilt darauf zu achten, welche neuen Anforderungen hinzukommen und proaktiv darauf einzuwirken, um Stresssituationen zu vermeiden.

Jeder Versicherer definiert diese Fragebögen individuell, aber es gibt auch Spezialmakler am Markt, die diese migrieren und mit den Versicherern abgestimmt haben.

Welche Bereiche sollten in den Fragebögen auf jeden Fall enthalten sein:

- Organization
- Data Handling
- Technical Security
- Organizational Security
- Detection & Response
- Cashless Payment
- Continuity Management
- Operational Technology
- External Service Provider

Die Prüfung geht also weit über das klassische Verständnis der IT-Security hinaus. Viel mehr hat ein vernünftiges Audit den Anspruch eine Versicherbarkeit unter Berücksichtigung aller Rahmenbedingungen festzustellen.

Das Audit liefert somit einen ganzheitlichen Einblick in die Cybersicherheitsstruktur und hilft bei der Identifizierung von Schwachstellen.

Akt 3

Mach's maxi.

Der Output eines Cyberpolicen-Audits hilft ganz unterschiedlichen Bereichen. So gibt es einen maximalen Output für das gesamte Unternehmen.

Versicherungsabteilung/Rechtsabteilung:

- Gutes Gefühl für die aktuelle Police (richtige Deckungssumme, akzeptable Prämie, richtige Bausteine, Leistung im Schadensfall)
- Check der Versicherbarkeit per Status Quo
- Abdeckung der finanziellen Schäden
- Sicherheit im Schadensfall

IT-Abteilung:

- Identifizierung von Schwachstellen
- Einteilungsmöglichkeiten für eine Roadmap
- Budgetierungshilfe
- Besserer und einfacherer Prozess bei Fragebögen durch unser Audit
- Sicherheit bei der Beantwortung von Fragen -> speziell im Schadensfall!

Geschäftsführung:

- Impact-Minimierung durch Kombination aus guter IT-Security und Absicherung der finanziellen Schäden
- Absicherung des Unternehmens im digitalen Zeitalter
- Sicherung der Arbeitsplätze im Unternehmen

Klingt alles super, aber es bleibt die Frage:

Akt 4

Wie läuft das eigentlich ab?

Best-Practice ist die Bereitstellung eines securance eigenen Fragebogens. Dieser wird benötigt, um die Evaluierung der Cybersicherheits-Architektur zu bewerten. Ein Cyber-Security Consultant bespricht den Fragebogen mit Ihnen vorab in einem Onboarding Termin, damit Sie genau verstehen, wie diese zu beantworten sind. Im nächsten Schritt prüft er die Antworten, um dann einen Audit-Dialog mit Ihnen durchzuführen.

Hier werden offene Fragen beantwortet und es findet ein intensiver Austausch zu den bereitgestellten Informationen statt. Im nächsten Schritt wird noch ein Externer Security Scan durchgeführt, der Ihre von außen ersichtlichen Informationen auf Schwachstellen überprüft. Im Anschluss daran, wird ein ausführlicher Report erstellt, der sich aus unseren Analysen ergibt.

Dieser enthält alle oben genannten Prüfparameter sowie eine Management-Summary, Handlungsempfehlungen und eine Einschätzung zur Versicherbarkeit. Darauf folgt, bei Bedarf, eine Angebotserstellung und der Abschluss der Police. Dieser Prozess dauert in der Regel wenige Wochen.



Akt 5

Versicherer-Dschungel. Wo bin ich?

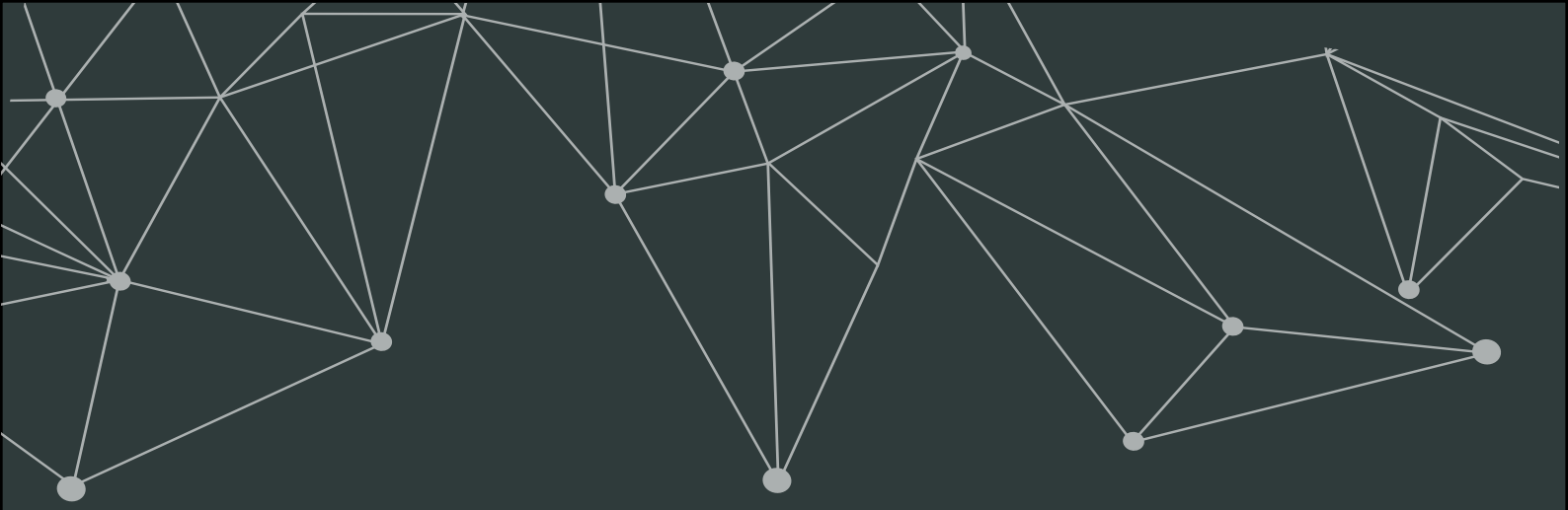
Spezialmakler oder einen der großen Player, den ich schon lange kenne?
Das ist nicht die entscheidende Frage.

Vielmehr muss es darum gehen, wo erhält mein Unternehmen den Schutz, den es wirklich benötigt und leistet meine Versicherung auch im Schadenfall. Wie so oft bei Trend-Themen, gibt es eine Police mittlerweile bei fast jedem großen Versicherer.

Aber nicht alle Makler und Versicherer haben auch Cybersecurity Know-How. Dies ist aber erforderlich, um nicht nur irgendeine Police zu erhalten, sondern eine preislich und leistungsmäßig passende Police zu haben – und zwar dauerhaft. Eine die leistet, eine deren zukünftige Anforderungen man frühzeitig kennt, eine deren Preis nicht jedes Jahr exorbitant steigt.

Wichtig ist, dass der Versicherer das richtige Verständnis für das Kundenrisiko hat, um dadurch eine faire Policierung anbieten zu können. Auf diesem Weg können auch Spezialvermittler eine hilfreiche Unterstützung sein.





suresecure GmbH

Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60
E-Mail: kontakt@suresecure.de

www.suresecure.de

securance GmbH

Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 211 88 23 02 84
E-Mail: kontakt@securance.de

www.securance.de