sure[secure] your security operations center x securance

secure mag

Warum brauche ich eigentlich eine Cyberversicherung?

Zwischen Cybersecurity und Versicherung: Warum beides notwendig ist

Einleitung

Eine Cyberversicherung wird dann relevant, wenn ein Unternehmen über sein eigenes Risiko nachdenkt. Cyberangriffe sind auch 2024 laut Allianz Risk Index das größte Geschäftsrisiko der Welt. Wer über Risikomanagement nachdenkt, kommt am Thema Cyberversicherung nicht vorbei. Keine Cybersicherheitsstrategie und kein Dienstleister der Welt kann eine 100%ige Sicherheit garantieren. Mit einer Cyberversicherung kann ich mein Unternehmen gegen die meisten entstandenen Schäden eines erfolgreichen Cyberangriffs finanziell absichern.

Denn ein Cyberangriff kann schwerwiegende Folgen haben wie z. B. den Datenverlust, Betriebsunterbrechungen oder Reputationsverlust. Darüber hinaus können zusätzliche Kosten entstehen, beispielsweise durch die Beauftragung von Dienstleistern, Gerichtskosten, finanzielle Entschädigungen oder die Zahlung von Lösegeld.

All diese Kostenpositionen können durch eine Cyberversicherung abgedeckt werden. Obwohl der Nutzen einer Cyberversicherung offensichtlich ist, werden wir oft gefragt, warum sie überhaupt notwendig ist. Immer wieder hören wir: „Dieses Geld könnte doch besser in Cybersecurity investiert werden."

Und dem können wir nur zustimmen. Denn die eigene Cyber-Resilienz ist die Grundlage dafür, überhaupt eine Versicherung zu erhalten. Aber schauen wir uns das genauer an:

Das Offensichtliche: Finanzielle Risiken absichern

Das größte Risiko bei einem Cyberangriff ist ein großer finanzieller Schaden. Durch die Deckung von anfallenden Kosten können Unternehmen das Risiko reduzieren und schneller wieder zur Wertschöpfung zurückkehren. So wird aus einem unkalkulierbaren Risiko ein planbares Risiko. Ergo steht die finanzielle Absicherung klar im Fokus.

Ein Beispielszenario:

Ein mittelständisches Unternehmen aus dem produzierenden Gewerbe mit 1.500 Mitarbeitenden wird vollständig verschlüsselt. Das Unternehmen generiert einen monatlichen Umsatz i. H. v. 7,5 Mio. Euro.

- Schaden durch Produktionsausfall, Umsatzverluste
- Schaden durch Vertragsstrafen, da vertraglich zugesicherte Lieferungen nicht eingehalten werden können
- Schaden durch den Abfluss von Daten
- Kosten für Dienstleister für Incident Response Maßnahmen
- Kosten für Beratung bzgl. Legal und Kommunikation
- Kosten für neue Lizenzen und Hardware für die Wiederherstellung
- Kosten für eine neue Security-Infrastruktur

Bei dieser Liste wird schnell klar, dass die Summe dieser Punkte auch eine Bedrohung für die Existenz des Unternehmens sein kann. Insebsondere der Produktionsausfall darf auf keinen Fall zu lange andauern, da der fehlende Umsatz gefährlich sind.

Aber es gibt noch weitere Gründe, warum es sinnvoll ist, sich auf den Weg zu einer Cyberversicherung zu machen.

Steigende Anforderungen der Versicherer und warum das gut ist

Mit zunehmender Bedrohung steigen auch die Anforderungen an den Abschluss einer Cyberversicherung. Mit anderen Worten: Ohne eine starke Cybersicherheit bekomme ich gar kein Angebot für eine Versicherung. Wenn ich also darüber nachdenke, muss ich mir zwangsläufig intensive Gedanken zu meiner Resilienz und Angriffsfläche machen. Mittlerweile gibt es klare Red-Flags für Ausschlüsse wie z. B.:

Cybersicherheitsmaßnahmen, die im Voraus festgelegt werden sollten:

- Regelmäßige Sicherheitsupdates und Patches
- Multi-FaktorAuthentifizierung
- Datensicherungen durch Backup-Strategie
- Security Awareness Programme
- Erstellung und Testen von Notfallplänen
- 24/7 Überwachung - Erkennung und Abwehr von Cyberangriffen

Sind diese Maßnahmen erfüllt, wird das Risiko für beide Parteien kalkulierbarer. Unternehmen, die in Prävention investieren, profitieren dann durch Transparenz, ein reduziertes Risiko und können zusätzlich Nachlässe auf die Versicherungsprämie oder höhere Deckungssummen erwarten. Genau aus diesem Grund führen alle Versicherer Risikodialoge durch, um ein Verständnis über das potenzielle Risiko zu gewinnen.

Netzwerkzugriff und direkte Ansprechpartner

Viele Cyberversicherungen enthalten Notfallnummern von Dienstleistern aus dem Netzwerk der Versicherer. Dabei kann es sich um IT-Forensiker, Rechtsexperten oder Kommunikationsberater handeln, die im Krisenfall unterstützen.

Bei einigen Versicherern besteht die Verpflichtung, sich auch an diese zu wenden. Dies sehen wir kritisch. Wir empfehlen daher genau zu prüfen, ob die Dienstleister auch geeignet sind. Das ist vergleichbar mit der Option zwischen freier Werkstattwahl oder Vertragswerkstatt. Wir empfehlen, sich im Vorfeld Gedanken über einen passenden IR-Partner zu machen, denn die Dienstleister der Versicherer kennen das Unternehmen nicht. Wenn ich einen vertrauenswürdigen Partner an meiner Seite habe, kann ich mit diesem bereits Prozesse abstimmen und habe über einen Rahmenvertrag fest zugesicherte SLAs für den Notfall. Damit ist sichergestellt, dass ein möglicher Vorfall effizient, sauber und ohne größeren Reputationsschaden aufgearbeitet werden kann.

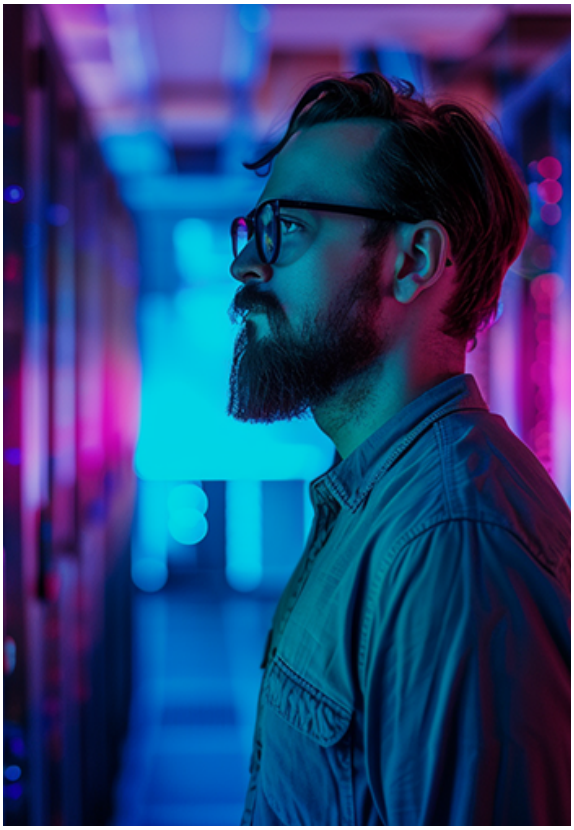
Eine Cyberversicherung ist also nicht nur eine Police, sondern auch ein Enabler für die eigene Cyber-Resilienz. Der Wunsch nach finanzieller Absicherung gegen Cyberangriffe zwingt das Unternehmen, sich mit den digitalen Risiken und Schwachstellen auseinanderzusetzen. Das steigert die gesamte digitale Souveränität der deutschen Wirtschaft.

Natürlich gibt es auch einige Punkte, die beim Abschluss zu beachten sind. Wichtig sind die beschriebenen Bestandteile und deren Ausgestaltung.

Deckungssummen

Bei der finanziellen Absicherung spielt die Höhe der Absicherung eine große Rolle. Was ist tatsächlich möglich und wo setzen Versicherer bewusst Grenzen? Das hängt von verschiedenen Faktoren ab, wie z. B. Unternehmensgröße, Umsatzpotenzial oder auch die Branche. Mittelständische Unternehmen können hier i. d. R. zwischen einer und fünf Millionen Euro absichern. Die Höhe der Deckungssummen ist aber auch an bestimmte Bedingungen geknüpft. Ein Eigenverschulden oder eine Fahrlässigkeit können dazu führen, dass die Versicherung eine Schadensdeckung ablehnt. Deshalb sollten die Bedingungen an die Leistung genau geprüft werden.

Die Prüfung sollte ebenfalls für alle anderen Bausteine erfolgen, um sicherzustellen, dass die wichtigsten Risiken abgedeckt sind. Denn die Bedingungen entscheiden letztlich darüber, ob die Kosten auch wirklich übernommen werden.



Sicherheit in der Leistungsübernahme durch Sicherheit in IT und OT

Ein intensiver und ehrlicher Risikodialog ist also keine künstliche Barriere, sondern bildet die Basis für eine transparente Risikobewertung. Je mehr Verständnis der Versicherer für mein Unternehmen, meine Branche und meine Infrastruktur hat, desto besser wird die Police ausfallen und desto wahrscheinlicher ist es, dass die Leistungen im Schadensfall auch wirklich erbracht werden.

Phishing-Attacken sind nach wie vor das häufigste Einfallstor für Schadcode. Deshalb bestehen die Versicherer auch darauf, dass Security Awareness Maßnahmen durchgeführt werden. Unter Umständen muss ich dann auch nachweisen können, dass diese durchgeführt werden.

Fazit:
Warum eine Cyberversicherung dennoch sinnvoll ist

Cyberversicherungen bieten finanziellen Schutz bei Cyberangriffen, die zu erheblichen Schäden wie Datenverlust, Betriebsunterbrechungen, Reputationsschäden oder Kosten für externe Dienstleister führen können. Investitionen in die Cybersecurity sind essentiell, aber eine Cyberversicherung ist eine Ergänzung zu den Schutzmaßnahmen und macht die Risiken kalkulierbar.

Die Anforderungen an den Abschluss einer Cyberversicherung fördern außerdem die Cyber-Resilienz, da Unternehmen Sicherheitsmaßnahmen wie regelmäßige Updates, Multi-Faktor-Authentifizierung, Backups und Notfallpläne etablieren müssen. Versicherer bieten im Schadensfall Zugriff auf Netzwerke von Spezialisten, wie IT-Forensiker und Rechtsexperten.

Deckungssummen hängen von der Branche und der Unternehmensgröße ab und liegen meist zwischen einer und fünf Millionen Euro. Transparenz und ein offener Risikodialog mit dem Versicherer erhöhen die Wahrscheinlichkeit einer umfassenden und wirksamen Schadensdeckung.

Insgesamt ist eine Cyberversicherung mehr als ein finanzieller Schutz – sie treibt die digitale Souveränität und Sicherheitsstrategie eines Unternehmens voran.

Weitere Informationen zum Thema:

Podcast-Folge:

Mit Cyberaudit und IT-Sicherheit auf der sicheren Seit

securance GmbH
Dreischeibenhaus 1
40211 Düsseldorf

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

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