11/24

# securemag

Das sind die **häufigsten Gründe für Vertragskündigungen** (Seite 2)

Starke **Strategien zur Re-Absicherung** (Seite 5)

# Cyberversicherung gekündigt – und jetzt?

*Wir thematisieren die Wiederabsicherung*

## Einleitung

In einer Welt, in der Cyberangriffe immer häufiger Schlagzeilen machen, ist die Cyberversicherung für Unternehmen nicht nur eine Vorsichtsmaßnahme, sondern ein strategisches Sicherheitsnetz. Doch was passiert, wenn dieses Netz plötzlich reißt? Der Wegfall einer Cyberversicherung kann für Unternehmen existenzbedrohend sein. Dieses Whitepaper beleuchtet die Gründe, warum Unternehmen ihre Cyberversicherung verlieren können, zeigt die möglichen Folgen auf und bietet innovative Strategien, um den notwendigen Schutz schnell und effektiv wiederherzustellen.

## Häufige Gründe für Vertragskündigungen

Wenn Versicherer eine Cyberversicherung kündigen, muss das nicht unbedingt etwas mit dem Versicherten selbst zu tun haben. Es kann auch vorkommen, dass Versicherer strategische Veränderungen in ihrem Portfolio vornehmen, wie es beispielsweise die AXA im Mai 2024 bekannt gegeben hat. Hier hieß es in einer Mitteilung:

*„Zukünftig wird die **Axa Deutschland** Cyber-Versicherungsschutz **nur noch für Privatkunden** sowie für **Unternehmen** mit einem **Umsatz von unter fünf Millionen Euro** anbieten.“*

Es gab jedoch auch weitere Gründe für proaktive Kündigungen seitens der Versicherer.

**Veränderte Bedrohungslage:**
Die allgemeine Bedrohungslage hat sich signifikant verändert und entwickelt sich kontinuierlich weiter. Dies führt dazu, dass Versicherer entweder höhere Standards anlegen oder Branchenausschlüsse für sich definieren. Ausschlaggebend ist dabei stets die Risikobewertung.

**Rückzug aus der Cyberversicherung:**
Wie im AXA-Beispiel können Versicherer beschließen, sich ganz oder teilweise aus dem Bereich der Cyberversicherung zurückzuziehen. Eine solche strategische Entscheidung hat unmittelbare und oft recht kurzfristige Konsequenzen für die Versicherten.

**Hohes Schadenaufkommen:**
Das allgemeine Schadenaufkommen eines Versicherers kann zu einer Kündigung von Policen führen, wenn es einen definierten Punkt überschreitet. Diese Entscheidung basiert auf einer übergeordneten Risikobewertung.

**Hohe Risikoeinstufung:**
Wenn ein Unternehmen als zu risikoreich eingestuft wird, etwa aufgrund wiederholter Cybervorfälle oder unzureichender Sicherheitsmaßnahmen, handelt es sich um Einzelfallentscheidungen. Dies kann auch dann der Fall sein, wenn vereinbarte Maßnahmen nicht umgesetzt wurden.

**Zu viele Schadensfälle:**
Das Unternehmen hat zu viele oder zu hohe Schäden erlitten, was sich negativ auf die Versicherungskonditionen auswirken kann. Auch in solchen Fällen kann es zu proaktiven Kündigungen kommen, die unmittelbare Konsequenzen nach sich ziehen.

## Konsequenzen der Kündigung

Wenn die Versicherung also wegfällt, stellen sich viele Unternehmen die Frage: Was nun? Denn ein fehlender Cyberschutz hat Konsequenzen.

### Fehlender Versicherungsschutz:

Ohne eine Cyberversicherung ist ein Unternehmen den finanziellen Risiken eines Cyberangriffs vollständig ausgeliefert. Ein Cybervorfall, wie etwa ein Datenleck oder ein Ransomware-Angriff, kann erhebliche Kosten verursachen, die von der Wiederherstellung der Systeme bis hin zu möglichen Rechtsstreitigkeiten und Bußgeldern reichen. Ohne Versicherungsschutz trägt das Unternehmen die gesamte finanzielle Last selbst, was zu einer erheblichen wirtschaftlichen Belastung oder sogar zur Gefährdung der Unternehmensstabilität führen kann.

### Vertrauensverlust:

Die Kündigung einer Cyberversicherung kann das Vertrauen von Kunden, Partnern und Investoren in die Sicherheits- und Stabilitätsmaßnahmen des Unternehmens erheblich beeinträchtigen. Kunden und Partner könnten befürchten, dass das Unternehmen nicht über ausreichende Schutzmaßnahmen verfügt, um die Sicherheit ihrer Daten zu gewährleisten. Investoren könnten die Kündigung als Warnsignal interpretieren und an der langfristigen Stabilität und Sicherheit des Unternehmens zweifeln. Der Vertrauensverlust kann zu einem Rückgang der Geschäftsmöglichkeiten und zu erschwerter Kundenbindung führen.

### Schwierigkeiten bei der Wiederbeschaffung des Versicherungsschutzes:

Die Suche nach einem neuen Versicherer zwingt Unternehmen dazu, bei null anzufangen. Es beginnt eine neue Evaluierungsphase von Anbietern, es müssen neue Risikodialoge geführt, neue Risikobewertungen durch Dritte durchgeführt und neue Verhandlungen geführt werden.

Denn die Einschätzung des Risikos basierend auf der bisherigen Schadenshistorie oder Bedrohungslage kann anders ausfallen und zu teilweise deutlich höheren Prämien führen. Je nach Bewertung könnten auch neue Sicherheitsmaßnahmen gefordert werden, was zusätzliche Kosten verursacht.

„Der Verlust einer Cyberversicherung kann für Unternehmen gravierende Auswirkungen haben. Es ist entscheidend, die Konsequenzen zu verstehen und schnell zu handeln, um den Schutz wiederherzustellen. Eine durchdachte Strategie zur Re-Absicherung ist der Schlüssel, um sich gegen zukünftige Risiken abzusichern und das Vertrauen zurückzugewinnen."

**Philipp Skucha**
CEO securance GmbH

## Strategien zur Re-Absicherung

Was ist nun die richtige Vorgehensweise, wenn ich mich in dieser Situation befinde? Wir raten dazu, die Dinge vor allem selbst in die Hand zunehmen. Das bedeutet, dass ein Bewusstsein für das eigene Risiko geschaffen werden muss. Wir starten also mit einer Bestandsaufnahme:

### Durchführung einer umfassenden Sicherheitsanalyse

Damit diese möglichst fundiert und realistisch ausfällt, empfehlen wir auf einen unabhängigen Cybersecurity-Dienstleister zurückzugreifen. Dieser kann eine Analyse von IT- und OT-Infrastruktur durchführen und auch Nebeneffekte wie z. B. Branchen-zugehörigkeit in die Bewertung mit einfließen lassen. Durch die Dokumentation der Findings gibt es eine transparente Auflistung der Schwachstellen und Risiko-bereiche. Darüber hinaus wird es mit Sicherheit Handlungsempfehlungen geben, um die Cyber-Resilienz zu steigern und damit in eine bessere Verhandlungsposition zu gelangen.

### Optimierung der Kommunikation mit Versicherern

Diese Analyse erleichtert den Einstieg in konstruktive Verhandlungen mit den Versicherern. Die transparente Darstellung der Maß-nahmen und das Bewusstsein über die eigenen Stärken und Schwächen schafft Vertrauen und eine solide Basis für einen kontinuierlichen Dialog über das eigene Risiko.

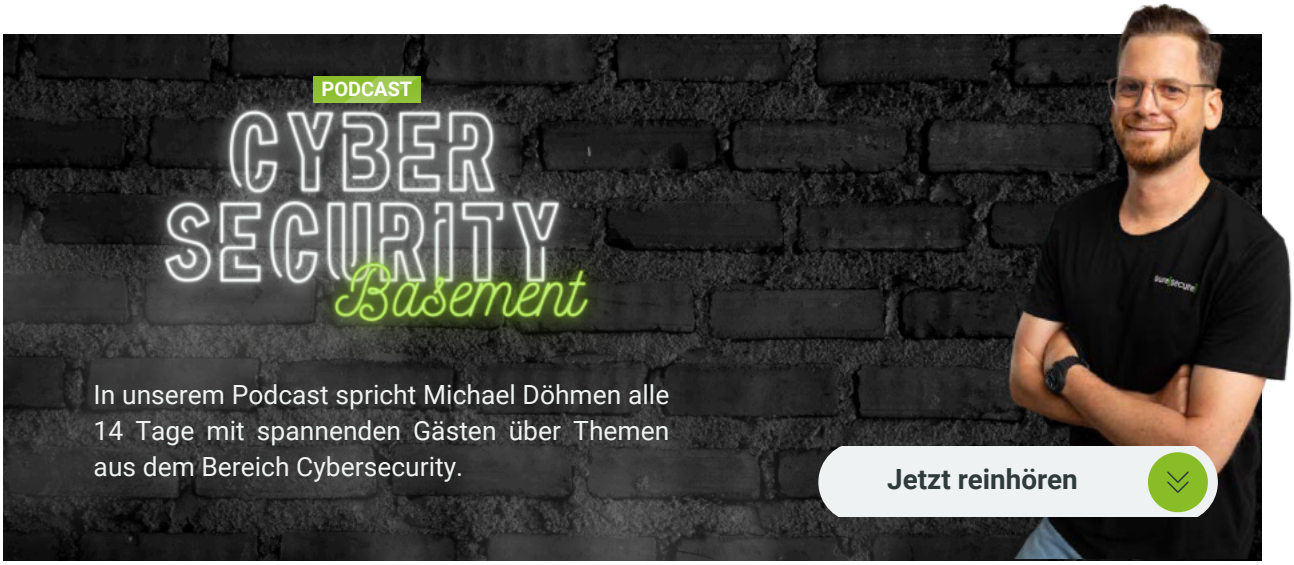
## Etablierung einer Sicherheitskultur im Unternehmen

Das Ziel sollte sein, dass Du in deinem Unternehmen eine eigene Sicherheitskultur etablierst. Denn eines ist elementar: Nachhaltigkeit. Das Bewusstsein für die Wichtigkeit von Cybersecurity im Unternehmen sollte nicht nur isoliert in einigen Abteilungen oder Personen fest verankert sein, sondern im gesamten Unternehmen.
Dabei kann es helfen, Partnerschaften mit Cybersecurity Anbietern einzugehen, um kontinuierlich an der Verbesserung und dem Bewusstsein zu arbeiten.

Mit diesem Dienstleister können auch definierte Sicherheitsrichtlinien und Notfallpläne erarbeitet werden. Die regelmäßige Überprüfung und Aktualisierung dieser Richtlinien entsprechen den neuesten Bedrohungen und Entwicklungen.

## Verhandlungen über individuelle Versicherungsverträge

Damit die Verhandlungen ideal geführt werden können, macht es durchaus Sinn mit spezialisierten Maklern zusammenzuarbeiten. Diese verfügen in der Regel über sehr gute Beziehungen zu den Ansprechpartnern bei den Versicherern und können dabei helfen, maßgeschneiderte Verträge auszuhandeln. Das umfasst die Aushandlung von Bedingungen, die den spezifischen Anforderungen und Sicherheitsmaßnahmen des Unternehmens entsprechen.



## Key-Take-Aways:

- Teilweise ziehen sich Versicherer aus dem Cybermarkt zurück oder stufen Unternehmen als zu risikoreich ein
- Ohne Versicherung drohen hohe Kosten und Vertrauensverlust
- Unternehmen müssen nach Kündigung rasch handeln, um neuen Schutz zu finden
- Eine Analyse hilft, Schwachstellen zu erkennen und bessere Versicherungsverhandlungen zu führen
- Eine starke Sicherheitskultur im gesamten Unternehmen ist entscheidend

## Fazit

In diesem Whitepaper wurden die häufigsten Gründe für die Kündigung einer Cyberversicherung aufgezeigt und die möglichen Folgen ausführlich beleuchtet. Es wurde auch dargestellt, dass der Weg zurück in den Versicherungsschutz nach einer Kündigung nicht einfach, aber durchaus machbar ist. Durch gezielte Maßnahmen wie die Durchführung umfassender Sicherheitsanalysen, die Optimierung der Kommunikation mit den Versicherern und die Etablierung einer soliden Sicherheitskultur im Unternehmen können Unternehmen ihre Position stärken und sich erfolgreich neu versichern. Die beschriebenen Strategien bieten eine klare Anleitung, wie Unternehmen ihre Risiken minimieren und ihre Cyber-versicherung erfolgreich erneuern können. Es liegt in der Verantwortung jedes Unternehmens, die notwendigen Schritte zu unternehmen, um in einer zunehmend digitalen Welt sicher und geschützt zu bleiben. Mit der richtigen Vorbereitung und einem proaktiven Ansatz kann der Versicherungsschutz nicht nur wiederhergestellt, sondern auch langfristig gesichert werden.

## Weitere Informationen zum Thema:


**Podcast-Folge:**

**Mit Cyberaudit und IT**
Sicherheit auf der sicheren Seite

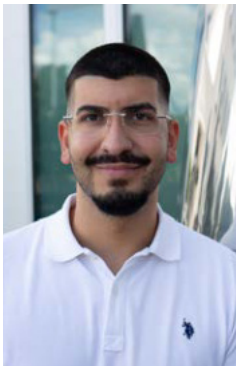

**Whitepaper:**

**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