

Grenzen von Cyberversicherungen zur Risikovermeidung

written by Christian Hafner | 31 März, 2023



Riskmanagement & IKS News

Grenzen von Cyberversicherungen zur Risikovermeidung

Blosses Auslagern von IT-Risiken an Versicherungsgesellschaften genügt nicht.

Cyberversicherungen können dazu beitragen, Unternehmen vor den finanziellen Auswirkungen von Cyberangriffen zu schützen. Sie können jedoch nicht alle Risiken vermeiden, die mit der Nutzung von IT-Systemen verbunden sind.

Grenzen von Cyberversicherungen zur Risikovermeidung:

1. **Kein Schutz vor allen Cyberangriffen:**

Cyberversicherungen bieten in der Regel Schutz gegen bestimmte Arten von Cyberangriffen, wie z.B. Phishing, Malware und Ransomware. Es ist jedoch unwahrscheinlich, dass sie alle Arten von Angriffen abdecken, insbesondere wenn es sich um neuere und ausgeklügelte Angriffe handelt.

2. **Kein Ersatz für IT-Sicherheitsmassnahmen:**

Eine Cyberversicherung ersetzt nicht die Notwendigkeit, robuste IT-Sicherheitsmassnahmen zu implementieren. Unternehmen müssen weiterhin in die Sicherung ihrer Netzwerke, Daten und Systeme investieren, um das Risiko von Cyberangriffen zu minimieren.

3. **Kein Schutz vor internen Bedrohungen:**

Cyberversicherungen bieten in der Regel keinen Schutz gegen interne Bedrohungen, wie z.B. Mitarbeiter, die absichtlich oder unabsichtlich sensible Daten preisgeben oder stehlen.

4. **Kein Schutz vor Reputationsschäden:**

Auch wenn eine Cyberversicherung finanzielle Verluste abdeckt, kann sie nicht den Ruf des Unternehmens schützen, der durch einen Cyberangriff beschädigt werden kann.

5. **Kein Schutz vor rechtlichen Konsequenzen:** Cyberversicherungen können finanzielle Schäden abdecken, aber sie können nicht vor rechtlichen Konsequenzen schützen, die aus einem Cyberangriff resultieren können, wie

1. b. Schadensersatzforderungen von Kunden oder Vertragsstrafen.

Insgesamt können Cyberversicherungen ein wichtiger Bestandteil der Cybersecurity-Strategie eines Unternehmens sein, aber sie sollten nicht als einzige Schutzmassnahme betrachtet werden. Unternehmen sollten weiterhin in IT-Sicherheitsmassnahmen investieren und sicherstellen, dass sie über eine umfassende Incident-Response-Strategie verfügen, um schnell auf Angriffe zu reagieren.

Fazit: Mit der Versicherung werden die Risiken nicht vermieden, sondern nur der Schaden vermindert. Und auch nur bis zu einer begrenzten Summe, die kaum je die operativen Schäden, die Reputationsschäden etc. abdecken kann.

Im schlimmsten Fall führt es zu einem falschen Sicherheitsgefühl und damit zu einem verminderten Elan, aktiv mit den Risiken umzugehen durch

- **abwälzen** -> z.B.: Outsourcing
- **begrenzen** -> z.B.: fragmentierte Architektur der Systeme
- **vermeiden** -> z.B.: Schwachstellen erkennen, organisatorische und technische Massnahmen treffen, Umsetzung und Ergebnisse
- **überwachen** -> z.B. Überwachungs-Tools einsetzen, Warnmeldungen, Login-Daten monitoren, Systemaktualisierungen

Schliesslich sollten Risikoidentifikation und -bewertung sowie deren Behandlung und Überwachung systematisch, verlässlich und nachweisbar erfolgen. Deshalb braucht auch das Management von IT-Risiken ein veritables RMS – Risk Management System.