Cyberrisiko – ein Großschaden-Risiko wird unterschätzt

In der Liste der aktuell größten Gefahren scheint das Risiko gehackt zu werden stets unter den Top 3 auf: Dennoch werden Cyberrisken im Sicherheitskonzept von Unternehmungen selten ausreichend berücksichtigt. Das bedeutet, dass im Falle eines Hackerangriffs ein betroffenes Unternehmen sehr oft völlig überfordert ist und die Kosten der Schadensbehebung Existenz gefährdend sein können: Die Gefährdung ist vergleichbar mit der Auswirkung eines großen Feuerschadens.

Welche Unternehmen sind besonders gefährdet?

Potenziell gefährdet sind alle Unternehmen: Je intensiver ein Betrieb von der EDV abhängig ist, umso höher wird ein Cyber-Schaden ausfallen: das trifft Produktionsbetriebe genauso wie Dienstleister: Für erstere werden hohe Kosten durch beschädigte Produktionsanlagen und deren Ausfall entstehen, für andere Betriebe wird der Diebstahl von - eventuell sensiblen - Daten und deren Veröffentlichung extreme Kosten verursachen. Auch ist es für gehackte Unternehmen ohne funktionsfähige EDV kaum möglich, binnen 4 Tagen einen umfangreichen Bericht mit Analyse und Maßnahmen zur Unterstützung der betroffenen Kunden an die Datenschutzbehörde zu übermitteln.

Unsere IT-Abteilung trifft alle Maßnahmen und wird im Ernstfall Cyber Schäden bewältigen!

Das stimmt so leider nicht: die IT-Abteilung eines Unternehmens wird im Schadensfall Spezialisten zur Analyse sowie Schadensbehebung benötigen und bei der Bewältigung aller Folgen zur Seite stehen: nicht nur die IT ist wieder in Funktion zu bringen, auch die Datenschutzbehörde ist zu informieren, ebenso Kunden nachweislich über Ausmaß des Datenmissbrauchs und geeignete Maßnahmen zur Risikobewältigung, zudem muss die Öffentlichkeit sachlich informiert werden, um das Schadenausmaß möglichst gering zu halten und Strafen zu vermeiden. Dazu reichen die Kapazitäten eines Unternehmens selten.

Cyber-Angriffe können nicht zu 100% vermieden werden, wie viele Beispiele aus den Medien zeigen.

Wie können Sie Ihr Unternehmen richtig versichern?

Schäden durch Cyber-Angriffe sind in konventionellen Versicherungspolizzen nicht versichert!
Nach einer genauen Risikoanalyse wird eine Kombination folgender Bausteine empfohlen:

1. Eigenschaden: Wiederherstellung der EDV samt Daten sowie Produktionsmittel, Erpressung, Reputationsschaden, Betriebsunterbrechung, Vertrauensschadendeckung
2. Schaden an Dritten: Deckung von Haftungsansprüchen Dritter, Abwehr unberechtigter Ansprüche, Versicherungsschutz für unverschuldete Haftungen in Sachen Datenschutz.
3. Soforthilfe 24/7 nach Hacker- Angriffen, Koordination mit Spezialisten eines Netzwerkes, Vorsorge für Cyberfälle – vor allem Awareness-Schulung der Belegschaft.

Es sollten alle verbundenen Unternehmen mitversichert werden.

Ein Cyber-Schutz ist auf bestehende Polizzen abzustimmen, die Versicherungssumme sollte ausreichend dimensioniert werden.

Was kostet ein Cyber-Versicherungsschutz?

Die Prämien richten sich vorrangig nach Umsatz und Branche und sind jedenfalls bezahlbar. Ein nicht versicherter Schaden ist wesentlich teurer.
Für ein Angebot fragen Sie Ihren guten Versicherungsmakler – zu finden auf seiversichert.at

Verfasst:
Johann Mitmasser (MAConsulting Versicherungsmakler GmbH, Walding)
Obmann Fachgruppe OÖ Versicherungsmakler
Linz, 6.12.2022