CYBER-RIKS-VERSICHERUNGEN

Cyber-Risk-Versicherungen sind in aller Munde – Ihr Versicherungsberater wird Sie sicher beim nächsten Gespräch darauf ansprechen. Mit vorliegender Zusammenfassung möchten wir Ihnen den Überblick erleichtern.

Cyber-Versicherung – was ist eigentlich versichert?

Je nach Versicherung und Versicherungsprodukt sind unterschiedliche Bereiche und Kostenfolgen gedeckt, darunter können fallen:

- Kosten aus System- und Datenwiederherstellungen
- allenfalls Datenrekonstruktionen
- Gewinn- bzw. Ertragsausfall für die Zeit des Unterbruchs
- Kosten aus Schadenersatzforderungen von Dritten, deren Daten bei einem Angriff entwendet/veröffentlicht/missbraucht/gelöscht wurden
- Verfahrens- und Verteidigungskosten

Die Produkte der einzelnen Anbieter variieren stark: eine detaillierte Prüfung des Angebots auf die versicherten Risiken, Haftung, die Terminologie in Bezug auf Gewinn- oder Ertragsausfall, sowie den Umfang der rechtlichen Leistungen sind im Detail zu prüfen und den Anforderungen Ihres Betriebes gegenüberzustellen.

Steht der Betrieb bei einem Angriff oder einer Infizierung sofort komplett still, weil Maschinen nicht mehr laufen oder Menschen nicht mehr arbeiten können, sehen die Anforderungen an den Versicherungsschutz anders aus, als in einem Betrieb, in welchem zwar während dieser Zeit die Administration stillsteht, jedoch die Produktion oder Dienstleistungen weiterlaufen.

Gemeinsam haben jedoch alle diese Versicherungen, dass Sie Wartefristen, Selbstbehalte und nicht gedeckte Positionen aufweisen und Sie und Ihr Unternehmen ein gewisses Mass an Sicherheitsvorkehrungen getroffen haben müssen. Denn keine Versicherung kann helfen, wenn Ihre Daten unwiederbringlich verloren sind.

Cyber-Attacke – was betrifft mich?

Je nach Art des Angriffs, können die Bedürfnisse anders ausfallen:

Bei einem Angriff mit Schadsoftware und Verschlüsselungstrojanern sind z.B. ausreichende Datensicherungen, starke Passwörter und ein durchdachtes Konzept bei Berechtigungen und Freigaben hilfreich.

Haben Sie umfangreiche Kundendaten gespeichert und es gibt einen Hackerangriff und Datenklau stehen Datensicherheit, Geheimhaltung und Haftungsfragen im Vordergrund.

Liegt die Attacke im Bereich von Missbräuchen von Zugangsdaten z. B. Kreditkartendaten, können finanzielle Aspekte wesentlich sein.

Meine Systeme sind bei SLYNET gehostet – die sind doch versichert?

Die Versicherungen der SLYNET erstrecken sich wie in anderen Branchen auf die Risiken, die in direktem Zusammenhang mit der Infrastruktur (Sachversicherung) und Haftpflicht aus dem Betrieb des Rechenzentrums entstehen.

Diese Haftpflicht erstreckt sich nicht auf allfällige Datenverluste und Wiederherstellungskosten für Kundendaten, welche durch einen Angriff auf die Kundensysteme entstehen. Weiterführende Informationen entnehmen Sie bitte unseren Allgemeinen Geschäftsbedingungen – AGB unter https://www.slynet.ch/firma/agb.

Meine Systeme sind bei SLYNET gehostet – was tun die?

Die bei SLYNET gehosteten Produkte und Softwareangebote werden laufend gewartet und unterhalten, um die Sicherstellung der aktuellsten Sicherheitsstandards zu gewährleisten. SLYNET ist bemüht, sämtliche Systeme laufend zu überwachen, Sicherheitslücken zu schliessen und mit geeigneten Sicherheitsmassnahmen die eigenen sowie die Kundendaten zu schützen. Dazu gehören weiche Komponenten wie z. B. Sicherungskonzepte, Zugriffsschutz und Software (Virenschutz) aber auch Hardwarekomponenten wie Firewalls etc.

Meine Systeme sind bei SLYNET gehostet – was ist mein Risiko?

Gleich hoch jedoch ist die kundenseitige Verantwortung: «starke» Passwörter und deren Geheimhaltung, Verhaltensanweisungen im Mailverkehr und im Umgang mit Mailanhängen. Die SLYNET bietet zudem ergänzende Sicherheitsoptionen, wie:

- Zweifaktorauthentifizierung (analog E-Banking)
- Premium AntiSpam-Service inkl. Virenschutz
- Replikation an einen zweiten / externen Standort
- Tägliches Backup / zusätzliches Halbtages-Backup
- Detaillierte Berechtigungskonzeption

Mit einem regelmässigen Datensicherungskonzept (z.B. täglich) liegt Ihr Risiko bei einer missbräuchlichen Verschlüsselung Ihrer Daten auf einem Cloud-Service der SLYNET

- in den Kosten für die technische Wiederherstellung der Daten (Dienstleistung) auf Basis des letzten verfügbaren Backups.
- und Ihren Personalkosten, die für die Aufarbeitung des Datenverlustes, der zwischen der Datensicherung und dem Verschlüsselungszeitpunkt entsteht, notwendig sind.
- sowie allfälligen Betriebsausfällen durch den Stillstand von Produktionsmitteln und Personal, die unmittelbar von der Verfügbarkeit des Cloud-Service abhängig sind.
- in möglichen Haftungsfragen gegenüber Ihren Kunden.

Cyber-Schutz – was kann ich tun?

Einen hundertprozentigen Schutz gibt es leider nicht – geeignete Vorkehrungen können jedoch das Risiko mindern, oder zumindest den Schaden in Grenzen halten.

Wir unterstützen Sie bei der Evaluation der für Sie relevanten Risiken und definieren die für Sie möglichen und notwendigen Schutzmassnahmen.

Ob eine Cyber-Versicherung für Sie und Ihr Unternehmen notwendig, richtig und wertvoll ist, sollten Sie anhand Ihres eigenen Anforderungsprofils abwägen. Bestehen Faktoren, die sich über die rein technische Risikokomponente hinausbewegen, ist eine detaillierte Prüfung sicher angezeigt.

Wir unterstützen Sie gerne, fragen Sie uns!