BERNHARD

ASSEKURANZMAKLER
SEIT 1950

Ein funktionierendes IT-Sicherheitskonzept ist die Basis eines guten Cyberschutzes

Cyber-Vorfälle werden immer häufiger und ausgeklügelter. Viele Unternehmen und gemeinnützige Einrichtungen denken, dass sie als Ziel für Hacker-Angriffe nicht interessant oder groß genug sind. Damit wiegen sie sich in falscher Sicherheit. Denn viele Hacker-Angriffe erfolgen gar nicht gezielt, sondern betreffen ihre IT bei einer breitangelegten Aktion eher zufällig.

Nachlässigkeiten in den Bereichen Datenschutz und IT Sicherheit können schnell Auswirkungen im operativen, reputativen und finanziellen Bereich haben. Zudem können durch Hackerangriffe personenbezogene Daten an die Öffentlichkeit gelangen.

Eine Cyberpolice schützt Ihre Organisation vor den finanziellen Folgen bei einem Angriff auf Ihre IT-Sicherheit. Zudem enthalten gute Cyberversicherungen auch Service-Leistungen, wie IT-Risikoanalysen im Vorfeld und leisten Unterstützung bei der Krisenkommunikation im Schadenfall.

Die Cyberversicherung sollte in jedem Fall mehrere Bereiche wie Eigenschäden, Drittschäden, Abwehrkosten, Erpressung und Lösegeld abdecken. Zudem gibt es weitere Aspekte, auf die Sie achten sollten, z.B. im Zusammenhang mit der DSGVO.

Je nach Risiko-Analyse gehört eine Cyber-Police inzwischen zu den **Top 5** der Versicherungen, deren Abschluss ein Unternehmen bzw. eine NPO in Betracht ziehen sollte.

Für diejenigen Kunden, die bereits eine Cyber-Versicherung haben:

Für Sie und Ihre Organisation ist es eine Beruhigung zu wissen, dass Sie als „zweite Verteidigungslinie“ eine Cyber-Versicherung im Rücken haben.

Wichtig ist auch die erste Verteidigungslinie, nämlich dass Ihre Organisation so gut wie möglich **IT-Sicherheits-Vorkehrungen** trifft. Das ist primär in Ihrem eigenen Interesse. Im Cyber-Schadenfall wird der Versicherer auch prüfen, ob Sie die Mindestanforderungen eingehalten haben. Beispiele:

- Sensibilisierung/ Schulung aller ehrenamtlich und hauptberuflich-Tätigen zu den Themenfeldern Cyber, Datenschutz/Datensicherheit
- Erstellen von Handlungsrichtlinien für Mitarbeiter
- Benennung eines für Cyber-Fragen verantwortlichen Mitarbeiters als Ansprechpartner im Falles eines Cyberangriffs
- Liste wichtiger Fachleute mit Telefonnummern IT-Leiter, IT-Dienstleister, Datenschutzbeauftragter
- Organisation: wer ist für was zuständig
- Übersicht über die Daten und deren Speicherung:
  welche Daten wo und wann gespeichert werden
- Regelmäßige Erstellung von Datensicherungen
- Wirksamer Schutz gegen Schadsoftware (Firewall, Antivirensoftware)
- Überwachung externer Zugänge zum Netzwerk

- Prüfung mindestens 1 x im Jahr, ob die TOM dem aktuellen Stand der Cyber-Sicherheits-Anforderungen entsprechen.

Sollte es tatsächlich mal zu einem (wenn auch nur vermeintlichen) Cyber-Versicherungsfall kommen, dann ist es wichtig, dass Sie immer zuerst sofort die Schadenshotline des Cyber-Versicherers anrufen. Dessen Assistance steht Ihnen dann mit Rat und Tat zur Seite. Sie finden die Telefonnummer auf Ihren Versicherungsunterlagen, die sollten Sie griffbereit haben.
Bitte verständigen Sie im Schadenfall auch Ihre internen und externen Mitarbeiter, die für IT zuständig sind, die Geschäftsführung, und last but not least: uns.

Heike Weber, Februar 2020