Erichsen

Cyber – IT-Risiken in einer neuen Dimension

Nahezu sämtliche unternehmerischen Aktivitäten sind heute abhängig vom Austausch elektronischer Informationen über Datenleitungen im Cyberraum—Tendenz steigend. Doch kein Datentransfer ist sicher genug. Kriminelle und Unbefugte sind jederzeit in der Lage, sich in fremde IT-Systeme einzuschleusen und dort großen Schaden zu stiften. Unternehmen haben daher eine anspruchsvolle Aufgabe, wenn sie versuchen, die Sicherheitsrisiken ihrer Informations- und Technologielandschaft zu managen.

Nach dem Eintreten eines Cyber-Vorfalls macht die Cyber-Versicherung einen Unterschied ; sie unterstützt Ihr Unternehmen dabei, konkurrenzfähig zu bleiben.

Häufigkeit und Schweregrad von Cyberschäden steigen, Unternehmen sind gefordert, in ihrem **Risikomanagement** sicherstellen, dass operative, finanzielle und reputationsrelevante Aspekte von Cyber-Risiken fokussiert, hinterfragt und für ein Unternehmen weitestgehend kalkulierbar werden.

Was passieren kann, passiert…

Beispiele zu Risiken, die heute fast jedes Unternehmen bedrohen und über eine Cyber-Versicherung weitgehend versicherbar sind:

Cyber - Haftung

Schadenersatzansprüche Dritter wegen

- ◊ Sicherheitsverletzungen im Cyber-Raum , z.B. fehlgeschlagene Abwehr eines Hackerangriffes
- ◊ Verletzung von Datenschutz– oder Vertraulichkeitspflichten
- ◊ unerlaubter Medienaktivität, z.B. Verstoß gegen Marken- , Persönlichkeits- oder Wettbewerbsrechte

Cyber– Eigenschaden

Kosten und Verlust von Einnahmen

- ◊ Entgehende Einnahmen bei Betriebsunterbrechung infolge IT-Systemausfall , z.B. durch Denial of Service– oder Hackerangriffe oder interner Sabotage
- ◊ Wiederherstellungs– und Rekonstruktionskosten bei Verlust oder Beschädigung von Daten
- ◊ Verlust digitaler Gelder, Waren und Wertpapiere
- ◊ Erpressung

Zusätzliche Kosten

… unfreundliche Begleitp(k)osten im Schadenfall

Bei der Bewältigung der Krise fallen meist weitere Kosten an, z.B. für Krisenmanagement, PR-Berater, Information betroffener Dateninhaber, IT-Forensik und sonstige Sachverständige...

Erichsen

Benötigt Ihr Unternehmen eine Cyber-Versicherung?

Werden in Ihrem Unternehmen sensible Daten (personenbezogene oder sonstige vertrauliche) von Kunden, Mitarbeitern, Patienten, Vertragspartnern gespeichert, bearbeitet oder verwaltet? Werden in Ihrem Unternehmen wichtige Prozesse und Transaktionen IT-und / oder web-gestützt gesteuert oder durchgeführt?

Was kann versichert werden?

Cyber-Haftpflicht

- ◊ Prüfung des Anspruches
- ◊ Abwehr unberechtigter Ansprüche
- ◊ Befriedigung berechtigter Ansprüche

Cyber- Eigenschäden

- ◊ Wiederherstellungskosten bei Verlust oder Beschädigung von Daten
- ◊ entgehender Gewinn und Mehrkosten bei cyber-bedingter Betriebsunterbrechung
- ◊ monetärer Gegenwert bei Cyber-Verlust von Geldern, Waren und Wertpapieren
- ◊ Erpressungsgelder

Kosten

… im Zusammenhang mit einem Cyber-Schadenfall

- ◊ IT-Forensik
- ◊ Rechtsberatung
- ◊ Krisenmanagement
- ◊ PR-Beratung
- ◊ Information von einer Datenschutzverletzung Betroffener
- ◊ PCI-Vertragsstrafen

Gute Gründe für Ihre Cyber-Versicherung

- ◊ Daten sind eines Ihrer wichtigsten Güter, jedoch über konventionelle Versicherungen nicht oder nur bruchstückhaft versichert.
- ◊ Reibungslos funktionierende IT-Systeme sind für das tägliche Gelingen Ihrer Geschäfte unverzichtbar. Cyber-bedingte Betriebsunterbrechungen sind über traditionelle Betriebsunterbrechungsversicherungen jedoch nicht gedeckt.
- ◊ *Cybercrime* ist die weltweit am schnellsten wachsende Verbrechenssparte.
- ◊ Daten und Informationen werden immer wertvoller; für den Verlust fremder Daten kann Ihr Unternehmen zur Verantwortung gezogen werden. Bei Verlust von Kreditkartendaten drohen harte Strafen der Kreditkartenindustrie.
- ◊ Image ist das Kapital Ihres Unternehmens, Sie sollten es schützen. Unbefugter Zugriff auf Ihre *Social Media Accounts* oder der Verlust sensibler Kundendaten kann Ihrer Reputation erheblich schaden.
- ◊ Portable Laufwerke vervielfältigen die Gefahr von Verlust oder gar Diebstahl. Zunehmende Nutzung von Smartphones und die Verwendung von Cloud-Anwendungen im Unternehmen bieten eine weitere Angriffsfläche für Cyber-Kriminelle.