Akquisegrund Cyberdeckung – Jeder braucht es, nur wenige haben es!

Cyber Risiken sind die Kehrseite der Digitalisierung:

Wertschöpfungsketten und Geschäftsmodelle bewegen sich von analog zu digital. Alles wird vernetzt.

Achtung!
Klassische Deckungen laufen meist ins Leere, d. h. kein Versicherungsschutz bei sog. „klassischen“ Versicherungen wie:

- Betriebshaftpflicht
- Sach-Inhalt
- Betriebsunterbrechung
- Elektronik

Versicherungsmakler

Welche Daten verarbeitet ein Unternehmen?

Versicherungsmakler

Deckungsumfang einer Cyber-Versicherung

Drittschäden

- Personen- und Sachschäden / Haftung aus dem Verlust von Daten

Eigenschaden

- Sachschäden und Wiederherstellung der IT Infrastruktur
- Der Versicherer erstattet u. a. Eigenschäden wie Kosten für Krisenberatung, IT-Forensik, begleitende PR-Maßnahmen, die Wiederherstellung der Daten und des IT-Systems (inkl. Wiederherstellungskosten für IT-Hardware/ ggf. auch Lösegeldzahlung), die Kosten für die Benachrichtigung der Betroffenen sowie die Aufwendungen für Datenschutzanwälte, Strafrechtsschutz und eine nachgelagerte Sicherheitsanalyse.

Betriebsunterbrechung

- Ausfallzeit bei Betriebsstillstand

Ergebnis:

Umfassender Schutz physischer und elektronischer Daten: Laptop, Smartphone oder Papierakte – man leistet, wenn physische oder elektronische Daten abhandengekommen, nicht mehr verfügbar sind oder missbraucht wurden.

Bürorisiko | - Verschlüsselungstrojaner 200.000 € Umsatz, 4 Mitarbeiter

Schadenhergang

Ein Mitarbeiter erhält eine E-Mail, deren Anhang mit der Schadensoftware infiziert ist. Beim Öffnen der E-Mail wird im Hintergrund die Schadensoftware heruntergeladen und installiert. Der betroffene Rechner wird sofort verschlüsselt und es gibt keinen Zugriff mehr. Kurz danach werden sämtliche Systeme sowie auch Rechner des Büros infiziert und verschlüsselt. Back-Up-Systeme werden zusätzlich kompromittiert und sind nicht mehr wiederherstellbar. Lösegeldforderung für die Entschlüsselung erscheint auf den Rechnern. Die Praxis ist vollständig handlungsunfähig.

Schadenaufwendungen: 82.000 €

Versicherungsmakler

Arztpraxis | | - Datenschutzvorfall 300.000 € Umsatz, 6 Mitarbeiter

Schadenhergang

Über eine Brute-Forcing-Attacke (Passwort bzw. Benutzername konnte gehackt werden) konnte sich ein Trojaner unbemerkt in das System einschleusen. Der Trojaner ist dafür bekannt, sich unauffällig in den Systemen zu bewegen sowie nach und nach wichtige Daten (z. B. Patientendaten, Passwörter) abzuziehen. Vor allem Patientendaten sind auf Schwarzmärkten (DarkNet) sehr beliebt.

Aufgrund des Datenabflusses muss eine Meldung bei der zuständigen Datenschutzbehörde innerhalb von 72 Stunden erfolgen. Zusätzlich müssen sämtliche Patienten sowie Geschäftspartner über den Datenabfluss informiert werden.

Schadenaufwendungen: 72.000 €

Einzelhändlerrisiko | | | - Haftpflichtschadenfall 500.000 € Umsatz, 10 Mitarbeiter

Schadenhergang

Über eine Sicherheitslücke wird versucht in das System des Kunden einzudringen. Hacker konnten sich unberechtigt einen vollständigen Zugriff auf die Systeme des Einzelhändlers verschaffen und somit sämtliche E-Mails sowie Korrespondenz abgreifen. Die Kontakte sowie die E-Mails werden genutzt um im Namen des Einzelhändlers E-Mails mit schadhaftem Anhang an Patienten und Geschäftspartnern zu verbreiten. Die Betroffenen melden sich bezüglich der schadhaften E-Mails. Einige Rechner sind durch das Öffnen der täuschend echten E-Mails mit einem Banking-Trojaner infiziert worden.

Schadenaufwendungen: 93.000 €

Versicherungsmakler

Allgemeines Firmenrisiko IV: Laptop mit Kundendaten verloren

7.000.000 € Umsatz, 25 Mitarbeiter

Schadenhergang

Ein Mitarbeiter eines Telekommunikationsunternehmens verliert seinen unverschlüsselten Laptop mit sensiblen Kundendaten in der Bahn. Gemäß geltendem Datenschutzrecht müssen daraufhin alle betroffenen Kunden über den Verlust informiert werden. Außerdem werden die Kunden aufgefordert, ihre Zugangsdaten zu erneuern. Accounts, für die das Passwort innerhalb einer Frist nicht geändert wurde, werden automatisch gesperrt.

Ein externes Callcenter wird damit beauftragt, Anfragen der Kunden zu übernehmen. Die Aufwendungen für Krisenmanagement, Rechtsberatung und Callcenter-Leistungen belaufen sich insgesamt auf **354.000 Euro.**

HACKERANGRIFF nach DDoS-Attacke

(Denial of Service bezeichnet in der Informationstechnik die Nichtverfügbarkeit eines Internetdienstes, der eigentlich verfügbar sein sollte. Häufigster Grund ist die gezielt gesteuerte Überlastung des Datennetzes.)

Schadenhergang

Der Kunde betreibt einen Online-Shop für gewerbliche Abnehmer. Mit einer Distributed-Denial-of-Service-Attacke (DDoS) überlasten Hacker von mehreren Rechnern gleichzeitig ausgehend die Domain des Unternehmens. Das Unternehmen ist für 36 Stunden nicht erreichbar. Es können weder neue noch laufende Aufträge bearbeitet werden. Neben dem Ertragsausfall entsteht ein mittelgroßer Imageschaden in der Branche.

Neben dem Eigenschaden (Wiederherstellung der IT-Infrastruktur) ist auch der Ertragsausfall versichert. Zusätzlich wurden dem Kunden Empfehlungen zur Verbesserung der IT-Infrastruktur sowie der IT-Sicherheit unterbreitet. Ferner übernimmt eine PR-Agentur die Behebung des Imageschadens.

Kostenaufteilung des Hackerangriffs: Die Folge war ein Ertragsausfall in Höhe von 25.000 Euro. Für forensische IT-Dienstleistungen und Beratung fielen 35.000 Euro an. Die PR-Agentur macht für die Wiederherstellung der Reputation des Unternehmens 50.000 Euro geltend.

HACKERANGRIFF durch Datenmissbrauch

Schadenhergang

Datenmissbrauch hat ebenfalls viele Gesichter. Am häufigsten ist hier der betrügerische Missbrauch von Bank- und Kreditkartendaten der Kunden eines Unternehmens, da hiermit sehr schnell Geld ergaunert werden kann. Auch das Ausspionieren eines Unternehmens („Industriespionage“) fällt unter diese Kategorie der Cyber-Risiken.

Zugang kann der Täter über Schadsoftware (z. B. Keylogger), Hardware (z.B. gestohlener PC) oder über Mitarbeiter (z. B. „geborgten“ Zugang) erhalten.
Schadenbeispiel: Die Kundendatenbank eines Autohauses wird gehackt. Dabei erbeuten die Täter u. a. sämtliche gespeicherten Kreditkartendaten der Kunden. Dem Autohaus entstehen Kosten für Forensik, technische Optimierung, Schadenersatzforderungen der betroffenen Banken, etc.

HACKERANGRIFF durch digitale Erpressung

Schadenhergang

Digitale Erpressung kann in verschiedenen Formen auftreten. Die größte Verbreitung findet über sog. „Ransomware“ statt, Schadprogramme wie z. B. der bekannte „BKA-Trojaner“. Hier wird in der Regel der Zugriff auf den eigenen Rechner blockiert und suggeriert, dass diese Blockade aufgehoben wird, wenn man eine Zahlung tätigt (z. B. als Bußgeld „getarnt“). Allerdings gibt es natürlich auch Fälle, in denen Firmen mit angedrohten DDoS-Attacken zur Lösegeldzahlung erpresst werden. Auch die Drohung, erbeutete Kundendaten zu veröffentlichen, etc. ist ein häufiger Erpressungsansatz.

Vielen Dank für Ihre Aufmerksamkeit!

Für Rückfragen stehe ich Ihnen gerne zur Verfügung.