Cyber-Versicherung – Schadenbeispiele

E-Mail an falschen Verteiler geschickt

Eine Arzthelferin schickt versehentlich Informationen über Patientenabrechnungen statt an die Krankenkasse an einen externen E-Mail-Verteiler. Der Arzt muss alle betroffenen Patienten sowie die zuständigen Datenschutzbehörde informieren. Darüber hinaus war die Beratung durch eine Fachanwaltskanzlei zur Abstimmung aller erforderlichen Schritte nötig.

Diebstahl von Firmenvermögen

Ein Mitarbeiter in der Buchhaltung öffnet versehentlich einen E-Mail-Anhang, der ein Schadprogramm enthält. Mittels diesem gelingt es Unbekannten die Bankzugangsdaten zu erlangen und 200.000 € von den Firmenkonten ins Ausland zu überweisen.

Betriebsstillstand durch Hackerangriff

Ein mittelständischer Betrieb, der seine Produktion mittels IT steuert wird Opfer eines Hackerangriffs. Dem Angreifer gelingt es die IT für 5 Tage lahmzulegen und viele Daten zu zerstören. Der Betrieb erleidet einen Betriebsunterbrechungsschaden und muss das System durch einen externen Dienstleister komplett neu wiederherstellen lassen.

Hacker erbeuten Kreditkartendaten

Unbekannte verschaffen sich mittels eines Schadprogrammes rechtswidrig Zugang zum online-basierten Abrechnungssystem für Kreditkarten eines Hotels. Dabei werden über 15.000 Kreditkartendaten von Kunden abgegriffen und unrechtmäßig genutzt. Dem Hotel entstand dadurch ein sehr hoher finanzieller Schaden.

Ransomware (WannaCry)

Durch Unachtsamkeit aktiviert ein Mitarbeiter eine in einer E-Mail enthaltene Schadsoftware, die Daten im System des Unternehmens verschlüsselt und teilweise zerstört. Es wird Lösegeld gefordert.

Geschäftsgeheimnis

Einen Hacker gelingt es in das Computersystem eines Architektenbüros einzudringen und die noch internen Bau- und Subventionspläne des Auftragsgebers des Architekten einzusehen und zu kopieren.

Cyberdiebstahl durch Virus

Unbekannten gelingt es mittels eines Virus in das Computersystem eines Unternehmens einzudringen. Vom E-Mail Account des Geschäftsführers schicken sie eine E-Mail an sein Büro mit der Bitte um Geldüberweisung auf ein Konto. Die Assistentin überweist den Betrag auf das Hacker-Konto.

Mitarbeiter greift in die Kasse

Ein Mitarbeiter erlangt mittels eines in das Computersystem des Unternehmens eingespielten Trojaners die Zugangsberechtigung für mehrerer Unternehmenskonten. Über einen längeren Zeitraum überweist er sich kleinere Beträge auf sein Privatkonto. Innerhalb eines Jahres entsteht somit ein Schaden von über 20.000 €

Denial of Service Attacke (DDOS)

Ein Unternehmen wird mit einer Vielzahl an Anfragen bombardiert um das Computersystem zu überlastet. Es kommt dadurch zu einem kompletten Ausfall des Call-Centers. Der softwaregestützte Geschäftsbetrieb (PC, Telefon) steht für 3 Tage still. Die Kosten für die Betriebsunterbrechung und Wiederherstellung des Computersystems belaufen sich auf 130.000 €.