Häufig gestellte Fragen.

Finlex

Schadenbeispiele Cyber

Das Wirtschaftsleben wird aufgrund steigender Datenvolumina und zunehmender Vernetzung in der Wertschöpfungskette stets digitaler. Für Unternehmen birgt dies Chancen und Risiken. IT-, Cyber- und Informationssicherheit hat sich mittlerweile zu einem der Top-Themen für Geschäftsleiter entwickelt. Selbst bei festgelegter Strategie zur IT-, Cyber- und Informationssicherheit und einer ordnungsgemäßen Delegation der Umsetzung an Mitarbeiter oder externe Dienstleister verbleibt die finale Gesamtverantwortung und die Haftung bei der Geschäftsleitung.

Cyber-Vorfälle sind längst keine Seltenheit mehr und betreffen jedes Unternehmen – unabhängig von Größe und Branche. Die Schadenursachen reichen vom fahrlässigen Umgang der Mitarbeiter mit mobilen Geräten, wie z.B. Smartphone oder Laptop, bis hin zu gezielten und teils über einen langen Zeitraum vorbereiteten, professionellen und kriminell motivierten Attacken auf die IT-Infrastruktur eines Unternehmens.

Es existieren unzählige möglichen Schadensszenarien von Cyber-Vorfällen. Wir haben im Folgenden eine Auswahl typischer Schadenfälle zusammengestellt, in denen der Cyber-Versicherer Deckung gewährt hat.

→ Malware:

Durch Anklicken eines infizierten E-Mail-Anhangs wurde das System (einschließlich Produktions-IT) eines Automobilzulieferers mit Malware infiziert. Infolgedessen standen die Maschinen tagelang still. Die Kosten für die Bereinigung und Wiederherstellung des Systems sowie des Betriebsunterbrechungsschadens betrugen mehrere hunderttausend Euro.

→ Microsoft-Sicherheitslücke:

Aufgrund einer Microsoft-Sicherheitslücke gelangte ein Schadprogramm in das System einer Wohnungsbaugesellschaft (Hafnium Hack). Das Schadprogramm wurde jedoch noch nicht aktiviert und konnte durch IT-Forensiker aus dem System beseitigt werden. Die Kosten für die Beseitigung beliefen sich auf mehrere zehntausend Euro.

→ Versand von Spam-Mails:

Durch einen gezielten Angriff auf die Onlinepräsenz eines Handwerkbetriebs wurde der Server manipuliert und zum Versenden von Spam-Mails missbraucht. Verschiedene Kunden beschwerten sich über die unseriösen Mails und drohten mit Klage. Der vom Versicherer empfohlene IT-Forensiker konnte die Ursache schnell finden, das System bereinigen und den Versand stoppen. Eine PR-Agentur steuerte die Entschuldigung bzw. Rechtfertigung gegenüber den Kunden.

→ Lösegeld I – Verschlüsselung:

Aufgrund einer Sicherheitslücke konnte sich eine Hackergruppe Zugang in das IT-System eines mittelständischen Maschinenbauers verschaffen und eine Verschlüsselungssoftware installieren. Der Betrieb stand mehrere Tage still. Nach der Zahlung eines Lösegeldes entschlüsselten die Hacker die Systeme wieder. Die Kosten für das Lösegeld und die Betriebsunterbrechung betrugen mehrere Millionen Euro.

→ Lösegeld II – Veröffenlichung von Daten:

Eine Hackergruppe verschaffte sich gezielt Zugang zu sensiblen Kundendaten eines mittelständischen Industrie-Unternehmens. Die Hacker drohten mit der Veröffentlichung der Daten, was zu einen erheblichen Reputationsschaden und

zum Verlust großer Aufträge geführt hätte. Durch die Zahlung eines Lösegeldes in Millionenhöhe konnte die Veröffentlichung verhindert werden.

→ Verdachtsfall:

Eine Anwaltskanzlei hatte die Befürchtung, von einem Cyberangriff betroffen zu sein. Nach einem Anruf bei der Cyber-Incident-Hotline des Versicherers und der daraufhin erfolgten Untersuchung durch den vom Versicherer empfohlenen IT-Dienstleister konnte Entwarnung gegeben werden. Es handelte sich lediglich um einen Softwarefehler.

→ Datenschutzbehördliche Ermittlung:

Ein Finanzdienstleister wurde Ziel eines Cyberangriffes, bei dem personenbezogene Daten abgeflossen sind. Die Sicherheitslücke wurde durch den IT-Dienstleister des Versicherers geschlossen und der Vorfall wurde ordnungsgemäß den Datenschutzbehörden gemeldet. Diese leiteten daraufhin ein datenschutzrechtliches Verfahren gegen den Finanzdienstleister ein. Der Versicherer übernahm die Kosten einer auf Datenschutzrecht spezialisierten Kanzlei. Die Verhängung eines Bußgelds konnte verhindert werden.

→ Schmerzens- und Bußgeld:

Ein Telekommunikationsunternehmen gab widerrechtlich Kundendaten an nicht befugte Dritte weiter. Der betroffene Kunde machte Schmerzensgeld geltend, die Datenschutzbehörde verhängte ein Bußgeld. Der Versicherer übernahm sowohl die Anwaltskosten der erfolglosen Verteidigung gegen das Schmerzens- und das Bußgeld als auch das letztlich zu zahlende Schmerzens- und Bußgeld.

→ Überweisung auf ein falsches Konto:

Der E-Mailzugang des Mitarbeiters eines Einzelhändlers wurde gehakt. Der Angreifer verschickte vom E-Mailaccount des gehackten Mitarbeiters eine manipulierte Rechnung an einen Kollegen aus der Finanz-Abteilung des Einzelhändlers. Dieser überwies daraufhin mehrere zehntausend Euro auf das Konto des Angreifers, weil er dachte, es handele sich um eine korrekte Rechnung des Kollegen. Aufgrund einer optionalen Deckungserweiterung war der Sachverhalt versichert.

→ Fehlbedienung:

Der Mitarbeiter eines Spielwarenhändlers veränderte aus Versehen diverse Einstellungen in der Konfiguration des Onlineshops, so dass dieser für mehrere Tage nicht erreichbar war. Die Kosten für die Wiederherstellung und der Betriebsunterbrechungsschaden betrugen mehrere tausend Euro.

→ DDOS-Attacke:

Ein Online-Shop wurde Opfer einer Denial-of-Service-Attacke. Der Online-Shop war für Kunden mehr als zwei Tage nicht verfügbar, obwohl das interne IT-Team sowie der IT-Spezialist des Versicherers auf Hochtouren an der Abwehr des Angriffs arbeiteten. Die Kosten beliefen sich mitsamt des Betriebsausfallschadens auf über hunderttausend Euro.

→ Ausfall der Cloud-Dienste:

Die Plattform eines Lieferantendienstes wird über die Cloud-Dienste eines großen Anbieters betrieben. Der Cloud-Dienst war für fast einen Tag teilweise nicht verfügbar, so dass viele Bestellungen nicht bei dem Lieferdienst ankamen. Der Versicherer kam für einen Teil des entgangenen Gewinns auf.

→ Manipuliertes Kartenlesegerät:

In einem Kaufhaus wurde das Kreditkartenlesegerät von Unbekannten mit dem Ziel manipuliert, an Kreditkartendaten von Kunden zu gelangen. Die betroffenen Kunden stellten Schadensersatzforderungen an den Inhaber. Darüber hinaus war es notwendig, die Kreditkarten der Kunden zu überwachen, um einen weiteren Missbrauch zu vermeiden. Die Kosten für die Schadensersatzzahlungen, Rechtsanwälte und die Überwachung beliefen sich auf mehrere hunderttausend Euro.