# Schadenbeispiele

**Hackerangriff**
Ein Hacker verschafft sich Zugang zu Ihrem Computersystem, kann Ihre Daten und Geschäftsgeheimnisse einsehen und verändern.

**Übertragung von Viren**
Ein neuer Mitarbeiter loggt sich mit seinem Laptop ins Firmennetzwerk des Kunden ein. Dabei wird ein bis dato nicht registrierter Virus ins Netzwerk des Auftraggebers eingeschleust. Der Schaden wird erst nach drei Tagen festgestellt, das gesamte interne Netz ist zwischenzeitlich befallen. Bis zur vollständigen Entfernung des Virus steht der Betrieb still. Das Unternehmen verklagt den Dienstleister auf Sachschaden und entgangenen Gewinn.

**Datendiebstahl**
Unbekannte Täter hacken sich in die Systeme einer großen Arztpraxis und entwenden sensible Patientendaten. Mit Hilfe der IT-Forensik werden die betroffenen Patienten identifiziert. Ein Anwalt berät über die Aufklärungspflichten bei den Patienten. Eine Kommunikationsagentur informiert die betroffenen Dateninhaber über den Diebstahl. Kosten durch den Datendiebstahl 45.000 EUR.

**Angriff führt zu Serverüberlastung mit mehreren Tagen Stillstand.**
Eine Firma bietet Telekommunikations-Anlagen online an. Über einen Zeitraum von fünf Tagen wird der Firmen-Server über einen DoS-Angriff (absichtlich herbeigeführte Serverüberlastung) zum Absturz gebracht, so dass keine Geschäftsabwicklung mehr möglich ist. Neben dem Ertragsaus-fall entstehen Kosten für die Beendigung des DoS-Angriffs und für die Verhinderung weiterer Angriffe.

**E-Mail mit Trojaner legt Handwerksbetrieb vorübergehend lahm**
Eine nach dem Öffnen einer an einen Handwerker gerichteten E-Mail, aktiviert sich ein Tro-janer und versperrt den Zugang in das IT-System. Ein Angebot die Verschlüsselung gegen Zahlung einer Geldsumme wieder aufzuheben folgt umgehend. Nach Einschätzung des beauftragten IT-Unternehmens kostet die Entschlüsselung einen fünfstelligen Betrag. Die forensische Tätigkeit benötigt 10 Arbeitstage und führt zu einer tw. Betriebsunterbrechung.

**Fehler beim E-Mailing**
E-Mail-Marketing geht schnell. Manchmal zu schnell: Ein Mitarbeiter hat aus Versehen ein internes Dokument mit sensiblen Kundendaten eines Kunden an den gesamten Empfängerkreis geschickt. Der komplette E-Mail-Verteiler sieht so dessen Bestellhistorie und Bankdaten. Ein Schaden, der nicht nur peinlich ist, sondern auch Kosten nach sich zieht – vom Aufwand der erforderlichen Meldung bei der Datenschutzbehörde bis zum Schadenersatzanspruch des geschädigten Kunden.

**Manipulation eines Lesegeräts**
Trinkgeld gibt man gerne noch in bar. Aber die Rechnung wird oft mit der Kreditkarte beglichen. So verarbeitet ein Restaurant in wenigen Tagen viele Hundert Kreditkartendaten. Kriminelle haben den Kartenleser manipuliert und konnten die Daten abgreifen und missbrauchen. Schadenersatz, Kreditkartenüberwachung, Imageverlust.

**Internet-Kriminelle verschaffen sich Zugang zu Bankdaten von Kunden**
Internet-Kriminelle verschaffen sich Zugang zu den Kreditkarten- und Bankdaten aus dem Ticket-Server eines Konzertveranstalters. In den kommenden Wochen buchen Unbekannte mehrfach Beträge von den Kreditkarten-Konten der Musik-Fans ab. Im Folgenden müssen alle Kunden angeschrieben und auf den Diebstahl hingewiesen werden. Der Ticketserver muss neu generiert und gesichert werden und Schadenersatzanforderungen von den Fans stehen auch noch aus.