Schützen Sie sich vor Cyberrisiken!
Denn Sie könnten nicht nur Opfer sein, sondern auch selbst haftbar gemacht werden.

©Gina Sanders, Fotolia #61083417

Die Arten der Cyberkriminaltät sind vielfältig und werden im Laufe der Zeit leider immer umfangreicher. Nie war es so leicht wie heute, im Internet Anleitungen und Tools für eine Cyber-Attacke zu finden. Durch den einfachen Zugang zu den Informationen kann also nicht mehr nur der IT-Freak im Keller, sondern theoretisch auch Ihr Nachbar zum Täter werden. Erwartungsgemäß wird die Internetkriminalität von Jahr zu Jahr noch weiter ansteigen.

So leicht man zum Täter werden kann, so schnell kann man jedoch leider auch zum Opfer werden.

Die Vielfalt der Internetkriminalität

Laut statistischem Bundesamt gab es im Jahr 2018 ca. 87.000 polizeilich erfasste Fälle von Cyberkriminalität in Deutschland, die einen Gesamtschaden von mehr als 40 Millionen Euro verursacht haben.

Unter den Begriff Cyberkriminalität fallen unter anderem die folgenden Punkte:

- **Mailbomben** (organisiertes Verschicken einer Vielzahl von Mails, die zu Serverüberlastungen führen)
- **DoS-Attacke** (Denial of Service: Dienstblockade aufgrund einer Überlastung von Infrastruktursystemen)
- **Datenmissbrauch** (betrügerischer Missbrauch von sensiblen Daten, z.B. Bankverbindung)
- **Datensabotage** (Beschädigung, Veränderung oder Löschen von Daten)
- **digitale Erpressung** (z.B. Blockade eines Rechners, die erst gegen Bezahlung aufgehoben wird oder angedrohte Veröffentlichung sensibler Kundendaten)

Aus einem Opfer wird schnell ein Mitschuldiger

Doch neben den enormen Schadenhöhen, die auf einen selbst zukommen können, gibt es noch weitere Gefahren, die die Internetkriminalität mit sich bringt. Wird man beispielsweise Opfer eines Datendiebstahls und werden hierbei beispielsweise persönliche Kundendaten entwendet, kann man hierfür haftbar gemacht werden. Stellt das Gericht fest, dass man die Daten nicht entsprechend gesichert hat und dem Täter den Zugang ermöglicht hat, werden die Schadenersatzforderungen des geschädigten Dritten nicht lange auf sich warten lassen.

Denn die Rechtsprechung vertritt in dieser Sache einen klaren Standpunkt: wer z. B. durch unzureichende Sicherung seines Datenbestandes eine Schädigung eines Dritten begünstigt, ist Mitschuldiger (siehe u. a. auch IT-Sicherheitsgesetz, EU Datenschutz-Grundverordnung, § 202a ff StGB)!

Möchten Sie Ihr Unternehmen ernsthaft vor den finanziellen Folgen von Cyber-Risiken schützen, müssen sowohl Eigen- und auch Fremdschaden abgesichert werden. Die Versicherungswirtschaft hat entsprechend reagiert und passende Tarife entwickelt. Wir helfen Ihnen gerne, den für Sie passenden Schutz zu finden.


©weerapat1003, Fotolia #65739173

Das Thema interessiert Sie?
Sie wünschen weitere Informationen?
Wir freuen uns auf Ihre Fragen!

First Dresden Finance
Versicherungsmakler GmbH & Co. KG
Königstraße 11 • 01097 Dresden
Tel.: 0351 8951170 • Fax: 0351 8951171
post@firstdresden.com
http://www.firstdresden.com

Rev. 200407

Schadenbeispiele aus der Praxis

Hackerangriff auf die Deutsche Telekom

©designsolman, Fotolia #62397844

Ende 2016 ereignete sich ein Fall von Internetkriminalität, der große Schlagzeilen machte. Denn beim Opfer handelte es sich nicht um ein kleines Unternehmen, bei dem man Sicherheitslücken eventuell eher erwarten würde, als bei einem Großkonzern, sondern um einen sehr großen Telefon- und Internetanbieter - die Deutsche Telekom. Der Fall erregte besondere Aufmerksamkeit, da mehr als eine Million Telekom-Kunden betroffen waren. Konkret hackte sich der Täter in den Router der Telekom ein, sodass für sehr viele Kunden der Internetanschluss zeitweise nicht nutzbar war.

Geplant hatte der Angreifer jedoch noch viel Größeres: durch die sogenannten DoS-Attacken wollte er mittels massenhafter Datenanfragen mehrere Webseiten und Router lahmlegen. Hierbei scheiterte er zwar glücklicherweise, die Internet- und Telefonzugänge der Kunden waren aber dennoch blockiert. Da sich die Router nicht mehr neu starten ließen, war die Telekom dazu gezwungen, eine neue Software auf den betroffenen Geräten zu installieren. Neben dem finanziell nicht zu beziffernden Vertrauensverlust der Kunden, kamen also auch noch hohe Kosten für die Wiederherstellung der Funktionalität auf die Telekom zu.

Datenklau bei Yahoo!

©ChaotiC Photography, Fotolia #44739963

Bereits im Jahr 2013 hatte das Internetunternehmen Yahoo! zugegeben, dass Cyber-Kriminelle persönliche Daten von mehr als einer Milliarde Nutzer gestohlen hatten. Die Hacker verschafften sich unter anderem Zugriff auf Passwörter, verschlüsselte Sicherheitsfragen samt Antworten, Adressen und Geburtsdaten. Gemessen an der Zahl der betroffenen Nutzer handelte sich um den bis dahin größen bekannten Datenklau eines einzelnen Unternehmens. Yahoo! musste daraufhin alle betroffenen Kunden anweisen, die Passwörter zu ändern und neue Sicherheitsfragen einzustellen, um unerlaubte Zugriffe zu verhindern. Zudem wurde ein weiterer Datenklau aus dem Jahr 2014 bekannt, bei dem es die Hacker auf die gleiche Art von Daten abgezielt hatten. Die Zahl der betroffenen Nutzer wurde auf mindestens 500 Millionen geschätzt. Hier zeigt sich also ganz deutlich, dass Internetkriminelle nicht nur einen Versuch starten, an Daten zu gelangen, sondern bei Erfolg auch gerne ein zweites Mal zuschlagen.

Sabotage beim Friseur

©jorgenmac 100, Fotolia #70674287

Man könnte meinen, dass nur große Firmen Ziel einer Cyber-Attacke werden, da sie mehr im Fokus der Täter stehen und sich ein größerer Schaden anrichten lässt. Aber auch kleine Firmen und Unternehmen sind nicht davor gefeit, ebenfalls zum Opfer zu werden. Anfang des Jahres 2017 kam ein Fall vor Gericht, bei dem einer Angestellten eines Friseur-Salons vorgeworfen wurde, die firmeneigene Homepage gelöscht zu haben. Vermutlich war es der Angestellten durch eine unzureichende Sicherung der Zugangsdaten möglich, die gesamte Webseite zu löschen. Sind die Kosten für einen Aufbau einer neuen Internetpräsenz zwar noch überschaubar, ist es dennoch erschreckend zu sehen, dass ein Täter auch schnell aus „den eigenen Reihen“ kommen kann. Sind Datenmaterial und Kennwörter nicht ausreichend geschützt, kann aus einem unzufriedenen Mitabeiter leider auch schnell ein Internetkrimineller werden.

Die verschiedenen Beispiele zeigen ganz deutlich, dass sich kein Unternehmen in Sicherheit wiegen und darauf vertrauen sollte, dass schon nichts passiert. Da die Schadenhöhe je nach Unternehmensgröße enorm hoch ausfallen und die finanzielle Existenz bedrohen kann, ist eine Absicherung gegen Cyber-Risiken für jede Firma unerlässlich.