ACCURISK Risikomanagement Versicherungsmakler GmbH

Verbundpartner der stark vor Ort! Raiffeisen Spar+Kreditbank eG

Schutz vor Cyber-Risiken // Alles auf einen Blick

/1/ Cybercrime, Cyber-Risiken

Cybercrime, also durchs Internet oder Netzwerke begangene Straftaten, sind längst fester, bedauerlicher Bestandteil unserer Gesellschaft im Internet geworden. Das Bundeskriminalamt veröffentlichte in seinem Bericht zur Bundeslage fast 65.000 Fälle im Jahr 2013- und das sind nur die Fälle, die auch zur Anzeige gebracht wurden! Die Spielarten der Cyberkriminalität sind inzwischen sehr vielseitig und reichen vom Datendiebstahl bis hin zur digitalen Erpressung.

Die Medien berichten regelmäßig von Fällen, bei denen große Konzerne gehackt wurden – aber auch kleine und mittelständische Firmen sind beliebte Ziele für Angriffe, da Datenmaterial hier im Regelfall schlechter oder gar nicht geschützt ist. Die finanziellen Folgen eines solchen Angriffs können schnell in die Tausende gehen.

/2/ Cybercrime kann inzwischen jeder!

Geschädigt werden kann auch jeder! Fallen die Begriffe „Hackerangriff“ und „Cybercrime“, denken viele automatisch noch an eher verschrobene Technikfreaks mit laxen Moralvorstellungen, die im Keller sitzen und das Tageslicht scheuen. Mag dieses Bild in den frühen Tagen der Hackerszene vielleicht noch passend gewesen sein, hat sich die Welt seit den 80er Jahren doch gewaltig verändert. Ging es früher in erster Linie darum zu zeigen, was technisch möglich ist und dies evtl. mit einem (zumeist) harmlosen Scherz zu verbinden, steht heute überwiegend die mutwillige Schädigung im Mittelpunkt solcher Aktivitäten.

Es bedarf heute auch keiner besonderen Finesse im Umgang mit dem Computer oder ausgefeilten Programmierkenntnissen, um als Täter aktiv zu werden. Auch Sie selbst könnten theoretisch innerhalb von 24 Stunden eine cyberkriminelle Laufbahn starten. Die nötigen Tools und Anleitungen sind in einschlägigen Foren schnell gefunden und heruntergeladen.

Selbst auf Plattformen wie Youtube finden Sie beispielsweise Anleitungen zum Versand von Mailbomben.

Aufgrund des einfachen Zugangs zu benötigtem Equipment und Informationen ist davon auszugehen, dass die Zahl der Täter von Jahr zu Jahr steigen wird. Es steht dann nicht unbedingt das Ziel im Vordergrund, sich zu bereichern (z. B. direkt über Missbrauch erbeuteter, fremder Kreditkartendaten oder indirekt über den Verkauf erbeuteter Daten). Unlängst berichteten die Medien von einem entlassenen Auszubildenden einer Bank, der als Racheakt eine Mailbombe an seine ehemalige Filiale schickte und damit die Server für mehrere Tage lahmlegte. Auch der Anteil ideologischer Hacker erlebt einen gewaltigen Zulauf und ebenso wächst die Gruppe der „Script Kiddies“, der Heranwachsenden, die aus jugendlicher Dummheit heraus mit ihren Kenntnissen Schaden anrichten. Auf die verschiedenen, gängig gewordenen Formen der Cybercrime möchten wir an gesonderter Stelle noch ausführlicher eingehen.

Wichtig an dieser Stelle: Grundsätzlich könnte jeder zum Täter werden. Und es kann jeder Betrieb betroffen und geschädigt werden UND vor allen Dingen als „unfreiwilliger Helfer“ schadenersatzpflichtig gemacht werden, wenn Dritte dadurch geschädigt werden, weil man vor Ort an deren Daten kommen konnte. Die finanziellen Folgen, die Ihnen aus einer Cyberattacke direkt oder indirekt entstehen können, dürfen Sie keinesfalls unterschätzen.

/3/ Opfer und Mitverursacher

Opfer und Mitverursacher

Ein erfolgreicher Hacker-Angriff auf ein Großunternehmen verursacht einen durchschnittlichen wirtschaftlichen Schaden von 1,8 Mio. €. Bei kleinen und mittelständischen Unternehmen liegt der Durchschnittswert bei 70.000 €. Kann man sich die Schadenhöhe ggf. noch vorstellen, die einem selbst drohen kann, sind die Schadenersatzforderungen, die geschädigte Dritte stellen können, doch immer wieder überraschend. Man hat ja gar nicht aktiv mitgewirkt, weshalb sollte man also zahlen müssen?

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

Möchten Sie Ihr Unternehmen rundherum vor den finanziellen Folgen von Cyber-Risiken schützen, müssen sowohl Eigen- wie auch Fremdschaden abgesichert werden. Die Versicherungswirtschaft hat entsprechend reagiert und passende Tarife entwickelt. Hinsichtlich der Leistungsinhalte möchten wir Ihnen nachfolgend einen grundsätzlichen Überblick verschaffen.

/4/ Für wen ist die Versicherung?

Diese Versicherung ist für alle Gewerbetreibende, Freiberufler und Betriebsinhaber geeignet, die Daten nicht nur in Papierform verwalten.

Was ist versichert und welche Kosten werden übernommen?

Versichert sind – je nach Umfang des Vertrages – die gerechtfertigten Haftpflichtansprüche, die aus dem Missbrauch der Daten entstanden, die in Ihrem Betrieb gespeichert waren. Steht die Verpflichtung zum Schadenersatz fest, leistet die Versicherung Entschädigungszahlungen stets bis zur Höhe des entstandenen Schadens, maximal jedoch bis zur Höhe der vertraglich vereinbarten Deckungssummen. Für einige Risiken gibt es ggf. separat im Vertrag festgelegte Deckungssummen. Auch Eigenschäden sind Teil des Versicherungsschutzes bzw. können mit abgedeckt werden. Die Tarife am deutschen Versicherungsmarkt unterscheiden sich teils sehr deutlich in ihren Leistungen.

Der Leistungsumfang einer „Cyber-Risk-Versicherung“ erstreckt sich primär auf die Kosten, die Ihrem Haus nach einer Attacke entstehen und auf Vermögensschäden, die durch „Ihre Beteiligung“ Dritten zugefügt werden. Ein solcher Vertrag übernimmt je nach Versicherer, Tarif und vereinbartem Umfang:

- Kosten für IT-Forensik
- Rechtsberatung
- Informationskosten
- Kreditüberwachungsdienstleistungen
- Kosten für Krisenmanagement
- Kosten für PR-Beratung
- Betriebsunterbrechungsschäden
- Vertragsstrafen (PCI)
- Lösegeldzahlungen
- Wiederherstellungskosten
- Sicherheitsverbesserungen

Welche Schäden sind oft nicht versichert?

Auch beim Deckungsumfang einer „Cyber-Risk-Versicherung“ kann es Ausnahmen geben. Regelmäßig sind dies z. B.:

- Verletzungen von Kartell- und Wettbewerbsrecht, sowie Patentrecht
- Schäden durch vorsätzliches Handeln
- Auswirkungen von Krieg oder Terror
- Schäden aus einer behördlichen Vollstreckung
- Geldbußen oder Geldstrafen

- Schäden im Binnenverhältnis zwischen Versicherungsnehmer und mitversicherter Person
- Garantiezusagen

Wie lässt sich die Versicherungssumme ermitteln?

Die Höhe der Deckungssummen sollte am speziellen Risiko Ihres Unternehmens ausgerichtet und in entsprechender Höhe vereinbart werden.

Welche zusätzlichen Versicherungen sind zu empfehlen?

Geschäftsführer, Aufsichtsräte oder Vorstände haften bei Beratungs- und Entscheidungsfehlern persönlich und unbeschränkt mit ihrem gesamten Privatvermögen. Für diesen Fall, dass Sie oder eine andere versicherte Person für einen Vermögensschaden (weder Personen- noch Sachschaden) im Zusammenhang mit der jeweiligen versicherten Tätigkeit ersatzpflichtig gemacht werden, kann mit einer D&O-Versicherung (Organ- oder Manager-Haftpflichtversicherung) vorgesorgt werden.

Da der Gesetzgeber seit dem 01.07.2010 für Vorstandsmitglieder von Aktiengesellschaften einen persönlichen Pflicht-Selbstbehalt von 10%, max. 1,5-fach des Jahresbruttobezuges vorsieht, ist eine zusätzliche D&O-Selbstbehaltversicherung zu empfehlen.

Eigenschadenversicherung

Ähnlich wie bei der D & O, schützt die Eigenschadenversicherung eine Firma vor den Vermögensschäden durch Handlungen und Entscheidungen ihrer Mitarbeiter. Der versicherte Personenkreis ist hier jedoch nicht die Führungsetage, sondern der größere Teil der Mitarbeiter, die eher als Erfüllungsgehilfe tätig sind (inkl. Aushilfen und Praktikanten). Auch hier können größere Schäden verursacht werden: falsch weitergegebene Rabatte an Kunden, vergessenes Komma bei einer Bestellung, einer Zeitarbeitsfirma wird vergessen mitzuteilen, dass keine Arbeiter mehr benötigt werden, etc. Die Eigenschadenversicherung ist eine interessante neue Form des Firmenschutzes.

/5/ Schadenbeispiele

Was kann Ihrem Unternehmen zustoßen?

Da sich der Themenkreis „Cyber Risiken“ für viele noch in der Kategorie „böhmisches Dorf“ befindet, möchten wir an dieser Stelle gerne auf die häufigsten Schadensereignisse eingehen. Wir hoffen, dass Ihnen unsere Ausführungen auch Hilfestellung bieten, dieses Gefahrengebiet besser zu verstehen und das konkrete Gefahrenpotenzial für Ihr Unternehmen realistischer einschätzen zu können.

Mailbombe

Unter einer Mailbombe versteht man das organisierte Verschicken einer Unzahl von E-Mails (mit oder ohne Anhängen), um die E-Mail-Kommunikation des Empfängers zu blockieren. Inzwischen bietet das Internet eine Vielzahl frei downloadbarer Tools, über die es möglich

ist, tausende von Mails gleichzeitig an einen Empfänger zu versenden. Dies führt – abhängig von Stückzahl und Mailgröße – zu immensen Verzögerungen im Arbeitsalltag. Nicht selten dauert es mehrere Stunden, bis alle Mails empfangen wurden und man sich wieder z. B. der Kommunikation mit Kunden zuwenden kann. Es ist zudem möglich, dass der Mailserver durch die Bombe überlastet wird und gar keine Mails mehr verarbeitet werden können.

Schadenbeispiel:
Ein Callcenter wickelt u. a. für eine Direktbank die Kunden-, Telefon- und Mail-Hotline ab (First-Level). Ein *falsch beratener* Kunde der Bank startet aus Ärger über eine Anlageempfehlung eine Mailbombe, die aber natürlich beim Callcenter „einschlägt" und die Mailkommunikation dort lahmlegt. Es vergehen zwei Tage, in denen keinerlei Mails beantwortet werden können. Es entstehen Kosten für die Untersuchung und Überstunden der Belegschaft zur Aufarbeitung des Rückstands.

DoS-Attacke (Denial of Service)

Denial of Service (kurz DoS; engl. für „Dienstverweigerung") bezeichnet in der Informationstechnik die Nichtverfügbarkeit eines Dienstes, der eigentlich verfügbar sein sollte. Obwohl es verschiedene Gründe für die Nichtverfügbarkeit geben kann, spricht man bei DoS in der Regel als der Folge einer Überlastung von Infrastruktursystemen. Dies kann durch einen mutwilligen Angriff auf einen Server, einen Rechner oder sonstige Komponenten in einem Datennetz verursacht werden. Wird die Überlastung von einer größeren Anzahl anderer Systeme verursacht, so wird von einer verbreiteten Dienstblockade oder Distributed Denial of Service (DDoS) gesprochen.

Schadenbeispiel:
Ein mittelständischer Versand für Outdoor- und Military-Zubehör betreibt auch einen erfolgreichen Onlineshop, dessen Anteil am Gesamtumsatz über die Jahre auf 70% anstieg. Aufgrund des Sortiments machen ein paar studentische Aktivisten aus „dem linken Lager" das Unternehmen als „Naziversand" aus und starten über ein Botnet eine DDoS-Attacke, bei der der Shop mehrere tausend Mal immer und immer wieder angefragt wird, bis der Server kapituliert. Da die Attacke eine komplette Woche fortgesetzt wird, ist der Shop erst nach einigen technischen Änderungen wieder erreichbar. Die entstandenen Kosten: Fehlersuche, technische Optimierung, entgangener Umsatz für eine Woche, Imageschaden wegen Nichterreichbarkeit, etc.

Datenmissbrauch

Datenmissbrauch hat ebenfalls viele Gesichter. Am häufigsten ist hier der betrügerische Missbrauch von Bank- und Kreditkartendaten der Kunden eines Unternehmens, weil so 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.

Datensabotage

Bei einem Datensabotageakt werden Daten beschädigt, verändert oder gelöscht. Dies kann über ein Schadprogramm erfolgen oder gezielt durch einen Eindringling vorgenommen werden.

Schadenbeispiel:
Ein Auszubildender einer Werbeagentur nutzt seine Mittagspause dazu, im Betrieb einen Film herunterzuladen. Diesen legt er auf dem Firmenserver ab, wo ihn sich auch zwei Kollegen kopieren. Die Datei war mit einem Virus versehen, der beim Aufruf des Films die Computer befällt und sich über das Firmennetzwerk verbreitet. Der Virus löscht eine ganze Reihe von Dateien unwiederbringlich. Die Arbeit, die in diese Kundenaufträge investiert wurde, ist verloren – trotz angeordneter Überstunden können nicht alle Abgabetermine eingehalten werden. Es entstehen Kosten für die Forensik, technische Optimierung, Schadenersatzforderungen der Kunden, Kunden wandern ab und das Image der Firma hat schweren Schaden genommen.

Digitale Erpressung

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.

Schadenbeispiel:
Hackern gelingt es, Zugriff auf die Patientenakten eines Allgemeinmediziners zu erlangen. Nachdem die Datenbank erfolgreich kopiert wurde, schreiben Sie den Praxisinhaber per Mail an und drohen mit der Veröffentlichung der Anamnesen – natürlich mit dem Vermerk, woher die Daten stammen. Gegen Zahlung einer gewissen Geldsumme via Western Union könne er die Veröffentlichung verhindern.

ACCURISK Risikomanagement
Versicherungsmakler GmbH
Eichendorffstr. 134
D-90491 Nürnberg
Telefon: 0911 / 5 80 70 99
Telefax: 0911 / 5 80 70 61
Internet: www.accurisk.de
E-Mail: info@accurisk.de
Öffnungszeiten:
Mo - Do: 9 - 12 / 13 - 17 Uhr
Fr: 9 - 12 / 13 - 15 Uhr