Cybercrime

Gefahren begegnen, Risiken minimieren

Das Klima für Unternehmen und deren Leitungsorgane wird rauer. Ein funktionierendes Daten-Sicherheitsmanagement liegt schon heute in der Verantwortung der Unternehmensleiter. Stetig zunehmende Cyberrisiken in Verbindung mit einer weitgehenden Verschärfung der Haftungsrichtlinien durch die für 2015 erwarteten Europäischen Datenschutzverordnung bereiten Kopfzerbrechen. Viele Unternehmen in Deutschland sind hierauf bis heute nicht ausreichend vorbereitet. Was tun? Eine Mischung aus gezieltem Risikomanagement und Versicherung der Restrisiken sorgt für bestmöglichen Schutz.

Die Zahl der Cyberangriffe nimmt rasant zu. Eine Cybercrimestudie der KPMG [1] beschreibt, dass es »nicht mehr die Frage ist, ob, sondern lediglich wann und wie eine Attacke gegen das eigene Unternehmen stattfindet« [1]. Dabei werden die Angriffe zunehmend professioneller und unter Einsatz neuester Technologien durchgeführt. Verschärft werden die Risiken für die IT-Sicherheit durch die zunehmenden internationalen Geschäftsbeziehungen in kritische Länder, sowie neue Technologien oder Trends, wie beispielsweise Cloud Computing oder Bring-Your-Own-Device.

Zwar ist die Sensibilität auf die zunehmenden Gefahren zwischenzeitlich gestiegen, doch haben sehr viele Betriebe hinsichtlich ihres IT-Sicherheitsmanagements noch deutlichen Nachholbedarf. Eine aktuelle Studie der Risk Consultants von Corporate Trust 2014 ist vor allem der Mittelstand im Fokus der Angreifer. »In Deutschland wurden 30,8 % der mittelständischen Unternehmen, 23,5 % der Konzerne und 17,2 % der Kleinunternehmen geschädigt« [2]. Dabei stellen Hacker nach dieser Studie aktuell mit 41,5 % die größte Tätergruppe dar, gefolgt von Kunden und Lieferanten mit 26,8 %. Aber auch Vorsatz oder fahrlässiges Handeln eigener Mitarbeiter sind als erhebliche Schwachstelle zu sehen. »Unternehmen sind sich der finanziellen Auswirkungen von Cyberrisiken noch nicht ausreichend bewusst« [2].

Persönliche Haftung des Managements. Die Implementierung eines funktionierenden Sicherheitsmanagements, zu dem selbstverständlich auch die IT-Sicherheit zählt, liegt voll in der Verantwortung der Leitungsorgane. Erleidet ein Unternehmen aufgrund einer Cyberattacke einen wirtschaftlichen Schaden, kann dies zu einer unbeschränkten und persönlichen Haftung des Leitungsorgans mit dem gesamten Privatvermögen führen. Diese Haftung greift bereits bei leichtester Fahrlässigkeit – gesamtschuldnerisch und bei umgekehrter Beweislast.

Verschärfung der rechtlichen Rahmenbedingungen durch die Europäische Datenschutzverordnung. Durch die 2015 erwartete Inkraftsetzung der EU-Datenschutzrichtlinie wird eine teilweise drastische Verschärfung der Anforderungen an den Datenschutz einhergehen. Erwartet werden, neben dem Wegfall der Begrenzung auf sensible Daten gem. § 42a BDSG und steigende Bußgelder sowie umfangreiche Mitteilungs- und Dokumentationspflichten innerhalb eines Zeitraums von 24 Stunden ab »begründetem Verdacht« auf eine Datenschutzverletzung.

Strategien zur Risikobegrenzung. Rasant wachsende wirtschaftliche Risiken für Unternehmen und Manager bei verschärften rechtlichen Rahmenbedingungen stehen häufig einem unzureichenden IT-Sicherheitsmanagement der Betriebe gegenüber. Dieses sollte neben rein technischen auch organisatorische und personelle Maßnahmen beinhalten. Zudem verfügen laut Studie von Corporate Trust derzeit noch nicht einmal jedes 20ste der Unternehmen über eine entsprechende Cyberversicherung.

Nur ein ganzheitliches Konzept aus regelmäßigen Sicherheitsaudits durch externe Spezialisten und Absicherung der Restrisiken über eine den individuell den Unternehmensbedürfnissen angepassten Cyberversicherung bringen größtmögliche Sicherheit.

Cyberversicherung – ein geeignetes Mittel zum Risikotransfer? Auch eine gut funktionierende Cyber Security bietet keinen hundertprozentigen Schutz vor finanziellen Schäden infolge Cyberschäden.

Knapp fünf Prozent der Betriebe in Deutschland besitzen zurzeit eine adäquate Cyberversicherung, während die große Mehrheit gegen Feuerrisiken versichert ist. Die statistische Wahrscheinlichkeit durch eine Cyberattacke oder durch Fahrlässigkeit einen Datenverlust zu erleiden ist dagegen vielfach höher. Wie ist diese Diskrepanz zu erklären?

Die Gründe dafür sind vielschichtig. Diese sind insbesondere...

- Mangelnde Transparenz und Information zu den Produkten
- Geringe Vergleichbarkeit bestehender Konzepte
- Mangelndes Bewusstsein im Umgang mit Cyberrisiken
- Fehlende Erfahrungswerte zu versicherungsrelevanten Szenarien

Gerade eine individuell auf die Bedürfnisse angepasste Cyberpolice kann existenzielle Unternehmensrisiken absichern und zugleich die Leitungsorgane vor persönlicher Inanspruchnahme beispielsweise von Investoren oder Eigentümern schützen. Aus Unternehmersicht ist eine Cyberpolice daher schon deshalb hochinteressant, um im Extremfall nicht auf die D&O-Police zurückgreifen zu müssen.

Schutz vor Cybergefahren

Angreifer identifizieren – Sicherheitslücken erkennen und schließen

Um die virtuellen Bedrohungen durch Cyberangreifer besser verstehen zu können, hilft oft ein Vergleich mit der realen Welt eines Einbrechers, der in ein Haus eindringen will. Alle Teile vom Keller bis zum Dach des Gebäudes stellen dabei die IT eines Unternehmens dar.

Cyberdiebstahl. »So wichtig sind unsere Daten nicht« denken sich manche Unternehmensverantwortlichen in einer ersten Reaktion. Doch ein Cybereinbrecher benötigt nur ein gekipptes Fenster in Ihrem IT-Gebäude oder eine unsichere Webanwendung und er ist im Haus und beginnt Kundendaten zu kopieren und damit zu stehlen. Je nach Zielsetzung wird er diese öffentlich machen oder an einen Mitbewerber verkaufen. Wie werden Sie das Ihren Kunden erklären? Wie werden Sie mit den Datenschutzrechtsverletzungen fertig? Wie beruhigt man die Medien und den sozialen Shitstorm? Was ist zu tun, wenn die geheimen Produktdetails über Ihren zukunftsträchtigsten Umsatzträger zeitnah in China oder den USA verfügbar sind?

Cybersabotage. Ein Cybereinbrecher sucht die Schwachstellen in Ihrem Gebäudeschutz. Daher ist es auch nicht zielführend aus Kostengründen beispielsweise nur die Fenster der Ost- und Südseite des Hauses zu vergittern. Seien Sie sicher, der Cybereinbrecher wird intelligent genug sein, sich eine andere Hauswand für den Einstieg zu suchen. Auch Zäune aus Firewalls halten schon seit vielen Jahren keine professionellen Angreifer mehr vom Grundstück fern, denn sie werden einfach überstiegen. Im Inneren bewegt sich der Cyberangreifer dann verkleidet als Hausbewohner oder als Gebäudemanager. Der Cybereinbrecher hat damit ausreichend Zeit, den Hauptschaltschrank zu suchen und zu finden. Als sogenannter Domain-Admin übernimmt er die Kontrolle über Ihre Organisation. Dann entscheidet er, ob Sie morgen noch Geschäfte abwickeln oder nicht.

Cyber-(ver)fälschung. Manchmal will ein Cybereinbrecher weder Daten stehlen noch das Unternehmen ausschalten. Häufig besteht das Ziel darin, Laborwerte, Messergebnisse oder Steuerungsparameter für Maschinen zu manipulieren. Ergebnis: Entscheidungen werden dann auf Basis falscher Daten getroffen. Qualitativ mangelhafte Produkte werden an Kunden versendet. Maschinen und Anlagen sind aus unerklärlichen Gründen störanfällig und müssen zurückgerufen werden. Das bekannteste Beispiel eines solchen Angriffs ist die Manipulation der Urananreicherungszentrifugen im Iran, das zur Zerstörung der kostspieligen Maschinen geführt hat.

Ursachen für Cyberangriffe. Die Ursachen für Cyberangriffe sind nur auf den ersten Blick die kriminellen Hacker. »Gelegenheit macht Diebe« gilt unverändert auch im Zeitalter der Cybersicherheit. Zu viele eingesetzte IT-Systeme sind nicht oder nur unzureichend auf Sicherheitsschwachstellen getestet worden. Gekippte Fenster, Gips statt Stahlbeton oder Tresorschlüssel, die unter der Fußmatte versteckt werden helfen dem Cyberangreifer effizient und effektiv sein Ziel zu erreichen.

Ohne Sicherheitstests/-audits keine Sicherheit. Die Erfahrungen der SEC Consult seit mehr als 10 Jahren zeigen, dass man durch umfassende Sicherheitsaudits und -tests die Robustheit gegen Cyberangriffe fundamental erhöht. Der Umkehrschluss gilt ebenso. IT-Systeme, die nicht durch Sicherheitsprofis wie beispielsweise SEC Consult getestet wurden, sind praktisch ausnahmslos anfällig und beinhalten in der Regel schwere Sicherheitslücken. Solche Sicherheitstest/-audits sind als Reality Check der Dreh- und Angelpunkt. Sie sind auch durch keine der leider immer zahlreicheren selbsternannten »100-Prozent-Schutzlösungen« ersetzbar.

Cyber Incident Response. Neben den umfassenden Sicherheitstest und den weiterführenden technischen und organisatorischen Maßnahmen muss man davon ausgehen, dass Cybereinbrecher von Zeit zu Zeit im Haus aktiv sind. Um solche Angreifer zu erkennen, empfiehlt es sich entsprechende virtuelle Fallen aufzustellen. Darüber hinaus sind die notwendigen Prozesse vorzubereiten sowie Personalfragen und Verantwortlichkeiten zu klären. SEC Consult bietet mit SEC Defence ein umfassendes Leistungspaket für die Abwehr von akuten Angriffen an – mit Hotline, Bereitschaft und Teams von hochspezialisierten Cyberexperten, die vor Ort die notwendigen Maßnahmen ergreifen. Auch hier gilt: Vorsorge spart sehr viel Geld und Zeit.

Markus Robin

Markus Robin,
General Manager,
SEC Consult

Struktur einer Cyberversicherung. Die Komplexität von Cyberrisiken führt dazu, dass sich auch der Versicherungsschutz diesen Herausforderungen anpassen muss. Dabei kristallisieren sich zunehmend drei grundsätzliche Bausteine der Absicherung heraus:

1. Cyberhaftpflicht.

Die Cyberhaftpflicht greift bei Inanspruchnahme durch Dritte infolge einer Datenschutzverletzung auf Grundlage von »Gesetz« oder »Vertrag«. Gängige Policen bieten mitunter lediglich die Absicherung von »gesetzlichen« Schadensersatzansprüchen. Eine solche Absicherung ist oft unzureichend. Führt eine Datenpanne beispielsweise zu einem Schadensersatzanspruch aus der Verletzung einer Geheimhaltungsvereinbarung oder einem nicht erfüllten Service Level Agreement, ist meist die Absicherung einer »vertraglichen« Haftung erforderlich. Zudem sollten auch verschuldensunabhängige Haftungstatbestände berücksichtigt werden.

Bei Unternehmen der IT-Branche ist zudem zu prüfen, in welchem Umfang die Cyberhaftpflicht bereits im Rahmen der bestehenden Betriebs- und Vermögensschadenhaftpflicht enthalten ist. Moderne IT-Haftpflichtpolicen decken die Haftungsrisiken bereits weitgehend ab, so dass hier die Schnittstellen zwischen den Policen klar zu regeln sind.

2. Cyberkostenschäden – Krisenmanagement mit 24h HOTLINE.

Bei der überwiegenden Zahl der Cyberschadensfälle handelt es sich um reine Kostenschäden. Gerade vor dem Hintergrund der künftig verschärften Melde- und Berichtspflichten kommt es auf schnelles und organisiertes Handeln an, um den gesetzlichen Pflichten zu genügen und Bußgelder zu begrenzen beziehungsweise zu verhindern. Herzstück ist die Kooperation mit einem Krisen-Managementunternehmen, welches über eine 24h-HOTLINE dem Versicherungsnehmer bei »begründetem Verdacht auf eine Datenpanne« zur Verfügung steht.

Die wesentlichen Deckungselemente sind:

- KRISENHOTLINE mit 24/365 Erreichbarkeit
- Kosten für forensische Untersuchungen
- Meldung bei betroffenen Dritten oder Regulierungsbehörden
- Kreditüberwachungskosten
- Honorare externer Anwälte
- Call-Center-Kosten
- Kosten für Krisenmanagement und Public-Relations-Maßnahmen (Reputationskosten)

3. Cybereigenschäden.

Neben den genannten Haftungs- und Kostenszenarien stehen auch eine Fülle möglicher »Eigenschäden« auf der Liste der versicherbaren Risiken. Hierzu gehören insbesondere...

- Wiederherstellung von Daten und Netzwerken
- Ertragsausfallschäden infolge Betriebsunterbrechung
- Ausgaben in Verbindung mit Erpressung und Lösegeldforderungen
- Finanzielle Schäden bei Umleitung von Zahlungs- oder Warenströmen

Sogar Vertragsstrafen in Verbindung mit der Verletzung von vertraglichen Geheimhaltungs- und Datenschutzvereinbarungen sind zwischenzeitlich bei einigen Anbietern kein Tabu mehr.

Resümee. Datensicherheit auf hohem Niveau ist bei regelmäßigen Sicherheitsaudits möglich. Die Absicherung der Restrisiken über eine adäquate Versicherungslösung ebenfalls. Handlungsbedarf ist also gegeben. SCHUNCK als spezialisierter Versicherungsmakler mit seinen Partnern wie die SEC Consult bieten umfassende Beratungskompetenz, die es zu nutzen gilt.

Peter Janson

Peter Janson,
Competence Center IT,
Schunck

www.schunck.de

[1] 2013 KPMG Cybercrimestudie

[2] Studie: Industriespionage 2014 der Corporate Trust