Kosten eines Cyber-Schadensfalles

Leitfaden

www.bitkom.org

bitkom

Herausgeber

Bitkom
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin

Ansprechpartner

- Marc Fliehe | Bereichsleiter Sicherheit | Bitkom e.V.
  T 030 27576-242 | m.fliehe@bitkom.org
- Cornelius Kopke | Bereichsleiter öffentliche Sicherheit & Wirtschaftsschutz | Bitkom e. V.
  T 030 27576-203 | c.kopke@bitkom.org

Autoren

- Michael Barth, Genua
- Jürgen Fauth, LKA Baden-Württemberg
- Marc Fliehe, Bitkom e.V.
- Alexander Geschonneck, KPMG
- Marc Heitmann, Marsh
- Prof. Timo Kob, HiSolutions AG
- Cornelius Kopke, Bitkom.e.V.
- Michael Kranawetter, Microsoft Deutschland GmbH
- Gerald Liebe, IABG
- Daniel Mühlenberg, BSI
- Marco Schulz, Marconcert
- Rene Seydel, Secunet
- Frank Stoermer, HP
- Mechthild Stöwer, Fraunhofer SIT

Verantwortliche Bitkom-Gremien

Dialogkreis Informations- und Cybersicherheit

Inhaltsverzeichnis

1 Einleitung

Die Digitalisierung unserer Gesellschaft durchdringt alle Bereiche. Immer neue Trends wie Industrie 4.0, Big Data, Car2Car-Kommunikation bringen neue Risiken und Chancen mit sich. Die damit verbundenen Chancen sind elementar um gesellschaftliche und politische Herausforderungen bewältigen zu können und dabei den Anschluss in einer globalisierten Welt nicht zu verlieren.

Seit wenigen Jahren stehen aber auch die Risiken immer mehr im Vordergrund einer unternehmerischen und politischen Betrachtung (IT-Sicherheitsgesetz). Präventive Ansätze gelten schon lange nicht mehr als ausreichend, um den Gefahren aus dem Cyberraum adäquat zu begegnen. Medial verbreitete Beispiele, wie der Hackerangriff auf den Bundestag, machen deutlich: Auch gut geschützte Infrastrukturen können – wenn auch mit sehr hohem Aufwand – zum Ziel von Kriminellen und Ziel von Wirtschaftsspionage werden.

Doch welche Schäden entstehen eigentlich bei einem erfolgreichen Angriff? Welche Kosten sind mit den jeweiligen Schäden verbunden? Was sind die Folgen einer bestimmten Schadensart? Welche Haftungspflichten wurden vielleicht verletzt, welche bestehen jetzt?

Die Entscheider stehen gegenüber den (Mit-)Eigentümern, der Belegschaft, der Öffentlichkeit und den Behörden nicht nur moralisch in der Verantwortung, sondern zunehmend auch juristisch. Als ein wesentliches Beispiel sei hier nur das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) genannt – dieses soll Unternehmensleitungen u. a. dazu zwingen, ein betriebliches Früherkennungssystem für Risiken einzuführen und zu betreiben.

Mit dem hier vorliegenden Leitfaden möchte der Dialogkreis » Informations- und Cybersicherheit« des Bitkom das skizzierte Thema aufgreifen. Ziel ist es, einen praktischen Mehrwert für die Unternehmensleitung, IT-Verantwortliche und sicherheitsverantwortliche Mitarbeiter in den Unternehmen zu schaffen.

Dabei ist es nicht möglich konkrete Zahlen zu nennen, da die jeweilige Schadenshöhe auch immer vom Angriff und dem konkreten Unternehmen selbst abhängt. Hierbei sind so viele Faktoren zu berücksichtigen, dass nur eine Einzelfallanalyse entsprechende Zahlen zuverlässig schätzbar macht. Dieses Werk soll aber dabei helfen die verschiedenen Schadenspositionen, d. h. die Art des Schadens, aufzuzeigen und sich daran auszurichten. Gleichwohl befindet sich zur besseren Verdeutlichung am Ende dieses Leitfadens eine exemplarische Darstellung der Kostenarten anhand eines fiktiven Fallbeispiels.

Als entscheidendes Gliederungskriterium wird die Unterteilung in Eigenschäden und Fremdschäden vorgenommen. Als Eigenschäden werden wir nachfolgend die Schadensarten kennzeichnen, die vor allem auf das Unternehmen selbst zurückfallen. Beispielhaft seien dafür die Kosten für die Betriebsbeeinträchtigung – oder --unterbrechung genannt. Andere Kosten, wie beispielsweise Haftungskosten gegenüber Dritten, werden wir als Fremdschäden aufgreifen. Sie werden dabei sehr schnell bemerken, dass es bei der Kategorisierung eine große Schnittmenge mit fließenden Grenzen gibt. Die jeweils passendere Kategorie mag von der konkreten

Ausgestaltung des Cyber-Sicherheitsvorfalls abhängen und wird je nach Ausgestaltung des Unternehmens im Einzelfall anders gefasst werden können.

Dabei erheben die Gliederungspunkte nicht den Anspruch in chronologischer Reihenfolge abgearbeitet zu werden. Viele der Phasen und Anforderungen während eines Cybersicherheitsvorfalls greifen ineinander oder sind in unterschiedlichen Momenten wiederkehrend bzw. eigene komplexe Prozesse in einer Krise, wie etwa die Verbesserung der Organisations- und IT-Strukturen. Sie sollte unmittelbar nach Entdeckung des Angriffs geplant werden und später nach den Ad-hoc Maßnahmen fortgesetzt werden und auch nach der Bewältigung der Krise stets verbessert und angepasst werden.

Dieses Werk gibt dabei den nötigen Überblick, um die jeweiligen Schadensarten pragmatisch einordnen zu können. Gleichzeitig ist Ihnen dieses Werk sowohl zur Risiko-Beurteilung, der daraus abzuleitenden Budget-Frage für die IT-Sicherheit Ihres Unternehmens, aber auch für den Notfall ein guter Ratgeber. Ein Ratgeber, den Sie hoffentlich nur präventiv nutzen müssen.

Februar 2016

- Michael Kranawetter, Vorsitzender des Dialogkreises, Microsoft Deutschland GmbH
- Prof. Timo Kob, 1. Stellv. Vorsitzender des Dialogkreises, HiSolutions AG
- Marc Fliehe, Bereichsleiter Sicherheit, Bitkom e.V.
- Cornelius Kopke, Bereichsleiter öffentliche Sicherheit & Wirtschaftsschutz, Bitkom e.V.

1 Eigenschäden

1.1 Betriebsbeeinträchtigung und -unterbrechung

Bei einer **Betriebsbeeinträchtigung** sind die kritischen Prozesse und Anwendungen für die Nutzer der IT-Systeme oder für die auf sie angewiesenen Betriebsabläufe nur noch eingeschränkt verfügbar (Schutzziel Verfügbarkeit) oder laufen nicht mehr integer (Schutzziel Integrität) ab. Ein typisches Beispiel dafür ist ein teilweiser Ausfall kritischer IT-Komponenten

Merke

So ist zum Beispiel ein Hersteller von Spezialfolien auf eine unterbrechungsfreie Zufuhr und Verarbeitung des Rohstoffgranulats bei genau definierten Temperaturen angewiesen. Wenn es in diesem Fall mittelbar zur IT-seitigen Beeinträchtigung wichtiger Prozessparameter kommt, kommt es neben dem Produktionsausfall zu sehr hohen Wiederanlaufkosten in der Fertigung.

(z. B. die Hälfte der vorhandenen Web-Server), sodass Nutzer mit langen Antwortzeiten/ Time-Outs bzw. einem unerwarteten Abbruch einer Nutzertransaktion konfrontiert sind. Eine Betriebsbeeinträchtigung stellt auch der Ausfall von unkritischen IT-Systemen dar.

Beispiel

Ein Beispiel dafür ist der Ausfall des elektronischen Zeiterfassungssystems für die Mitarbeiter. Die Zeiten können bei Wiederverfügbarkeit des Systems nach einigen Tagen manuell nachgetragen werden. Geschäftskritische Anwendungen wie z. B. Web-Anwendungen sind von diesem Ausfall nicht betroffen oder können zumindest mit vermindertem Transaktionsvolumen weiterbetrieben werden.

Darüber hinaus kann eine Integritätsverletzung auch zu Mängeln bei Produktqualität und Produktmerkmalen führen, was zu direkten Schäden (Nachproduktion) oder auch zu indirekten Schäden, wie Reputationsschäden durch Produkte, die dennoch in den Markt gelangen, führen kann. Beispiel: Falsch beschriftete Etiketten, die den Allergiker-Hinweis nicht oder fehlerhaft enthalten; eine Arzneimittel-Charge, die keinen oder nur zu geringe Mengen eines Wirkstoffes enthalten; nicht bestellte, rosafarbene Nähte bei Sitzen in der Automobilfertigung, Kleidungsstücken oder der Möbelfertigung.

Beispiel

Wenn beispielsweise ein Unternehmen als Sofortmaßnahme gegen möglichen Informations- und Know-how-Abfluss bei einem Angriff den Internet-Verkehr einschränkt oder gar völlig unterbrechen lässt, kann ein solch ungeordnetes Vorgehen naheliegender Weise erhebliche Folgeschäden nach sich ziehen. Ähnlich aber vergleichsweise weniger dramatisch wirkt es sich aus, wenn ein Unternehmen sich entschließt eine akut ausgenutzte Software-Schwachstelle außerhalb der dafür vorgesehenen Wartungsfenster zu patchen und dabei die Nicht-Verfügbarkeit von betriebskritischen IT-Systemen in Kauf nimmt.

Bei einer **Betriebsunterbrechung** steht eine Anzahl von kritischen Prozessen und Anwendungen für einen längeren Zeitraum (z. B. zwei Stunden) nicht zur Verfügung. Eine Betriebsunterbrechung tritt zum Beispiel auf, wenn Angriffe auf Produktionssteuerungsanlagen stattfinden, die zur Unterbrechung der Produktionsprozesse führen.

Die Auswirkungen einer Betriebsunterbrechung beschränken sich typischerweise nicht allein auf den reinen IT-Betrieb, sondern richten sich maßgeblich nach den durch die IT-Systeme unterstützten Geschäftsabläufe und deren Verfügbarkeitsanforderungen. Ein Ausfall insbesondere bei IT-Systemen der Fertigungs- und Automatisierungstechnik kann entsprechend zu signifikanten Betriebsschäden führen.

Neben den unmittelbar durch vorsätzliche Handlungen herbeigeführten Schäden kann es bei IT-Sicherheitsvorfällen außerdem zu mittelbaren negativen Auswirkungen durch die Schadensminimierung und Ad-hoc-Präventionsmaßnahmen kommen.

Die Kosten einer Betriebsbeeinträchtigung stellen eine Teilmenge der Kosten einer Betriebsunterbrechung dar. Ein kleines Gedanken-Experiment: Stellen Sie sich Ihre gesamte Organisation vor und vergegenwärtigen Sie sich, bei welchen Prozessen IT-Systeme oder Software jetzt schon beteiligt sind. Beispielsweise funktioniert die Auftragsverarbeitung auch ohne IT-gestützte Systeme, wie steht es mit Produktionsplänen, Kundenkommunikation, Bestellsystemen für Roh- und Hilfsstoffe, Buchhaltungsprozesse, Controlling und Erfolgsbeurteilungssysteme, Mitarbeiterzeiterfassung und Stundenabrechnung, Urlaubsplanung, Lieferprozesse, Marketing und Grafikaufträge, Terminkalender und Telefonlisten, Zugang zum Gebäude und Parkflächen, Alarmanlagen und Gebäudekühlung oder Wärmeversorgung bis hin zur Telefonanlage?

Bei einer Betriebsbeeinträchtigung bzw. -unterbrechung können folgende Kosten auftreten:

- Kosten für Produktivitätsausfall
- Kosten für Qualitätsbeeinträchtigungen bis hin zum Produktionsausfall
- Datensicherung des Fehlerfalls (Festplattendatenbestand inkl. Hauptspeicherzustand) zur Nachstellung in einer Testumgebung;
- Fehlersuche und -behebung;

- Kosten für einen möglicherweise notwendigen/ erzwungenen System-Shutdown und damit verbundenen Ausfallzeiten;
- Gegebenenfalls Neuinstallation des Systems und Aufsetzpunkt der letzten Datensicherung;
- Einleitung eines Notbetriebsverfahren für Ersatzprozesse und Einberufung eines Notfallteams
- Herstellung der Betriebsfähigkeit an einem Ausweichstandort u. a. mit zusätzlichem Personal
- Schwenk der IT-Systeme und Anwendungen auf einen Ausweichstandort u. a. mit zusätzlichem Personal
- Einnahmeausfälle, da kritische Anwendungen und IT-Systeme nicht zur Verfügung stehen
- Ansprüche, Schadensersatzklage und Vertragsstrafen, die wir später im Bereich der Fremdschäden genauer betrachten werden.

Bei der Umsetzung von Industrie 4.0 müssen die dann größtenteils automatisierten Prozesse gut gekannt und möglichst resilient gestaltet werden. Die Geschwindigkeit in der Sie dort Fehler beheben und im laufenden Prozess idealerweise gegensteuern können, wird von entscheidender Bedeutung für den Geschäftserfolg sein. Ein plakatives Beispiel: Ein Unternehmen wird in wenigen Jahren in der Lage sein, Bestell- und Fertigungsprozesse weitgehend automatisiert ablaufen lassen zu können. So können Kunden über den App-Shop ihr gewünschtes Produkt individualisieren und in wenigen Tagen liefern lassen. Wenn nun bei einem großflächigen Cyberangriff gegen Klimaanlagensteuerungen diese in der Produktionshalle eine Temperatur ausgibt, die die Lackierung des Produktes nicht rechtzeitig trocknen lässt, verschmieren die Oberflächen in den weiteren Veredelungsprozessen. Die Produkte bekommen ungleichmäßige Oberflächen und Lacknasen. Bei der anschließenden Politur verkrusten die Bürsten, Lack gelangt durch die Rotation der Politurbürsten in die Scharniere der entsprechenden Politurarme.
Die Fehlersuche dauert lange und die Scharniere der Politurmaschine müssen von deren Herstellerfirma aufwendig gereinigt werden. Für diese Produktschiene entsteht eine Betriebsunterbrechung von mehreren Tagen. Die Fehlersuche und die Beseitigung der Schadsoftware zu der Klimaanlage erfordert ebenfalls Tage.

Um die Kosten einer Betriebsunterbrechung möglichst gering zu halten, sind im Vorfeld folgende präventive Maßnahmen empfehlenswert:

- Erstellung einer Business-Impact-Analyse (BIA) zur Bewertung der kritischen Anwendungen und IT-Systeme, deren Abhängigkeiten untereinander und deren maximal tolerierbaren Ausfallzeiten. Basierend auf den Ergebnissen der BIA wird bei einer Betriebsunterbrechung durch den Notfallstab festgelegt, welche Anwendungen und IT-Systeme mit höchster Priorität und mit welcher Wiederanlaufreihenfolge wiederhergestellt werden müssen.
- Regelmäßiges Backup von kritischen Anwendungs- und Systemdaten.
- Durchführung von Recovery-Tests.
- Erstellen und Üben von Notfallplänen und Maßnahmen.
- Durchführung von Schwenktests bei redundanten Systemen bzw. Rechenzentren.

Beispiel

Es reicht nicht, ein Satellitentelefon oder Notstromaggregat vorzuhalten, wenn es die Betroffenen nicht unter Stress bedienen können oder wissen wie man Diesel nachtankt.

Indirekte Kosten bei Betriebsunterbrechung:

- Kundenabwanderung bei Nichtverfügbarkeit von kritischen Prozessen und Anwendungen.
- Sicherstellung des Mittelflusses für den laufenden Betrieb (einschließlich Mitarbeiterkosten, z. B. Überweisung der Gehälter) auch wenn dazu notwendige kritische Systeme (z. B. Lohnabrechnungssystem) ausgefallen sind.
- Strafen bei Beeinträchtigung vertraglich zugesicherter Service-Zeiten und –Verfügbarkeiten.

Die Kosten der Betriebsunterbrechung und -beeinträchtigung sind stark einzelfallbezogen und abhängig von Umfang und Kostenintensität des normalen Betriebsablaufs, können jedoch durchaus immensen Umfang annehmen. Eine Bezifferung des Faktors muss im Einzelfall durch den IT-Sicherheitsverantwortlichen ermittelt werden.

Schadenbeispiel (Versicherungsfall):

Denial-of-Service-Attacke im E-Commerce

Ein Online-Shop wurde Opfer einer Denial-of-Service-Attacke. Der Online-Shop war 23 Stunden für Kunden nicht verfügbar.

Schadenbild

- Plötzlicher Anstieg des eingehenden Datenflusses
- Allmähliche Überlastung führt zur Nichtverfügbarkeit der Website
- Eingehender Datenfluss wird mit Hilfe des Internetanbieters analysiert und gefiltert, um böswillige Datenbewegungen von der normalen Geschäftsaktivität abzugrenzen
- Schrittweise Rückkehr zur normalen Geschäftstätigkeit

Finanzielle Auswirkungen

Voller Einsatz des IT-Teams (interne Ressourcen)	13.000 €
Mitwirken eines Spezialistenteams (Internetanbieter + Forensik)	18.500 €
Beeinträchtigung beeinflusst den Umsatz über 48h	135.000 €
Beeinträchtigung des Images und Beeinträchtigung des Ratings in Foren → Verstärkte Marketingaktivität	18.500 €
Versicherte Gesamtkosten	185.000 €

Quelle: Marsh / ACE Versicherung

2.2 Schadensermittlung und IT-Forensik

IT-forensische Untersuchungen dienen der Aufklärung von Cyberangriffen und anderen IT-Vorfällen durch Analyse der in den beteiligten IT-Systemen hinterlassenen Datenspuren. Weil die zu untersuchenden Daten dabei teilweise flüchtig sind, d. h. nur über kurze Zeit im Speicher oder auf Speichermedien vorhanden, sind solche Untersuchungen mitunter sehr zeitkritisch. Unbedachtes Vorgehen kann dazu führen, dass wichtige Datenspuren vernichtet werden, bevor ihre systematische Erhebung möglich ist.

Mit der IT-Forensik können unterschiedliche Ziele verfolgt werden, von der Aufklärung der Ursachen eines Vorfalls (Identifikation ausgenutzter Schwachstellen) über die Bestimmung des Ausmaßes (Ermittlung betroffener Daten und Systeme) bis hin zur Schaffung einer soliden Grundlage für juristische Auseinandersetzungen (arbeitsrechtlicher, zivilrechtlicher oder strafrechtlicher Natur). Neben einem tiefen technischen Verständnis für die internen Arbeitsweisen von IT-Systemen und Netzen erfordert diese Tätigkeit daher eine sehr gut organisierte und dokumentierte Arbeitsweise, damit zentrale Aussagen später nicht von der Gegenpartei in Frage gestellt werden können und gerichtsfest verwertbar belegt werden können. Der Unter-suchungsverlauf und die Ergebnisse münden dazu in einem Untersuchungs-gutachten, in dem Zeitpunkte, Mitwirkende und Methoden der Datenerhebung genau fest-gehalten sind. Soweit möglich, werden Untersuchungen stets so durchgeführt, dass eine Reproduktion der Ergebnisse durch Dritte anhand des Untersuchungsberichts jederzeit möglich ist. Dafür ist z. T. komplexe Spezialhard- und -software erforderlich, z. B. um Datenträger beweissicher zu duplizieren, oder um auf Speicherinhalte mobiler Geräte zuzugreifen.

Weil forensische Untersuchungen oft auch Bereiche umfassen, die durch die Datenschutz-gesetze oder das Betriebsverfassungsgesetz geschützt sind, müssen hier – ggf. unter Einbindung der zuständigen Stellen – Interessenabwägungen getroffen und ebenfalls nachvollziehbar dokumentiert werden.

Merke

Es ist dabei eine besondere Herausforderung, Daten manipulationsfrei so zu kopieren, dass belegt werden kann, dass weder das kopierte Material vor der Kopie verändert wurde noch bei dem Kopiervorgang Daten weggelassen oder verkürzt wurden.

Die Kosten für IT-forensische Untersuchungen sind maßgeblich abhängig von der Zielsetzung der Untersuchung und der Komplexität des betrachteten Vorfalls. Oft ist zu Beginn der Unter-suchung das genaue Ausmaß des Vorfalls unbekannt. Entsprechend lassen sich auch die erfor-derlichen Untersuchungsaufwände erst nach einer ersten Bestandsaufnahme abschätzen. Die Schadenssummen reichen vom kleinen fünfstelligen Bereich, z. B. bei einem kleineren Betrugs-fall, bis hin zu hohen sechsstelligen Beträgen, wie bei der Wirtschaftsspionage.

Merke

Durch die forensische Aufarbeitung eines Vorfalls steht oft ein Teil der Infrastruktur zeitweise nicht zur Verfügung, bis die Spuren des Einbruchs und seine Wege ins Netzwerk gesichert und nachverfolgt werden konnten. Dafür ist neben der Expertise eines IT-Forensikers ab einem bestimmten Ausmaß auch die Unterstützung durch einen Hersteller oder einen Systemintegrators nötig. Ggfs. müssen dann Teile der Infrastruktur erneuert werden.

Wegen der besonderen Anforderungen an die hoch qualifizierten Analysten und des Einsatzes umfangreicher Spezialhard- und -software, vor allem aber durch den meist sehr kurzfristigen Einsatz, liegen die Tagessätze für forensische Untersuchungen in der Regel höher als für andere IT-bezogene Dienstleistungen.

Auch die Polizeien und insbesondere die Zentralen Ansprechstellen Cybercrime bei den Landeskriminalämtern (ZAC) sind ebenfalls in der Lage Cyberforensik adäquat durchzuführen. Allerdings muss hier berücksichtigt werden, dass diese einen anderen Ermittlungsauftrag haben (den Täter zu fassen) und die öffentlichen Mittel nur begrenzt zur Verfügung stehen, wodurch derzeit lange Ermittlungszeiten zu erwarten sind. Auch ist es der öffentlichen Hand verboten eine individuelle Beratung für Unternehmen anzubieten. Gleichwohl kann es immer sinnvoll sein auch die ZACs über die Vorfälle zu informieren und Ermittlungen flankierend zu unterstützen.

Schadenbeispiel in der Gastronomiebranche

Ein von der Ukraine, Weißrussland und Afrika aus operierender Betrüger-Ring drang ins Kassensystem eines renommierten Restaurants in Sachsen ein und spionierte über Monate die Kreditkartendaten von wahrscheinlich bis zu 400 Gästen aus. Für den Wirt selbst, den Polizei und Kreditkartenfirmen über den Angriff informiert hatten, war der Schaden enorm:

Rund 115.000 Euro hat ihn die Cyber-Attacke gekostet, denn er musste einen hoch spezialisierten IT-Forensiker aus London kommen lassen, der eine Woche lang nach dem Virus suchte. Außerdem musste er ein komplett neues Kassensystem anschaffen.[1]

2.3 Management der Schadensbewältigung

Hier sind folgende Aufgaben zu bewältigen: Informationen einholen, Informationen bewerten, kommunizieren, Entscheidungen treffen und koordinieren.

Ereignisse können oft im Vorfeld nicht früh genug detektiert oder erkannt und entsprechend verhindert oder wenigstens eingedämmt werden, sodass sich in der Folge tatsächlich Notfälle,

1 Vgl. Bild.de vom 01.07.2015

Krisen, Großschadensereignisse oder sogar Katastrophen aus einer Organisation heraus ent-wickeln können. Dann bedarf es zwingend definierter und eingeübter Notfall- oder Krisenreaktionsmaßnahmen, mit denen es möglich ist, das Ereignis zu managen und die Schäden zu bewältigen. Dies gilt im gleichen Maße für Cybervorfälle, wie für nur physische Schadensereignisse, wobei sich diese zukünftig immer schweren trennen lassen.

Diese Maßnahmen zum Management der Schadensbewältigung müssen ganz konkret für den Notfall oder den Krisenfall greifen, denn 100-prozentige Sicherheit lässt sich nicht realisieren. Für den Ereignisfall müssen deshalb gut vorbereitete Maßnahmen existieren, mit denen den drohenden oder eingetretenen Schäden entgegengewirkt werden kann. Das Management der Schadensbewältigung kann durch die betroffene Organisation oft nicht allein und aus eigenen Ressourcen geleistet werden. Außerdem muss die möglichst schnelle Überführung in den Normalbetrieb des Unternehmens selbst sowie mithilfe externer Experten durchgeführt werden . Hier bleibt festzuhalten, dass je weniger ein Unternehmen auf einen Cybersicherheitsvorfall vorbereitet ist desto mehr externes Know-how wird es im krisenfall einkaufen müssen (s. u. Krisenberatung).

Je nach Schadensfall oder Angriff und in Abhängigkeit vom betroffenen Unternehmen, ergibt sich mitunter ein erhebliches Medieninteresse, das zur Vermeidung von nach-haltenden Reputationsschäden sensibel und mit Erfahrung gelenkt und begleitet werden muss. Erforderlich ist deshalb vorgelagert ein Krisenmanagementkonzept, welches den Krisenstab beschreibt, festhält wer was mit wem kommuniziert und welche Rolle im Fall der Krise ausgefüllt werden soll und zuletzt diese Abläufe in einem Übungsplan trainiert.

Krisenstabsorganisation

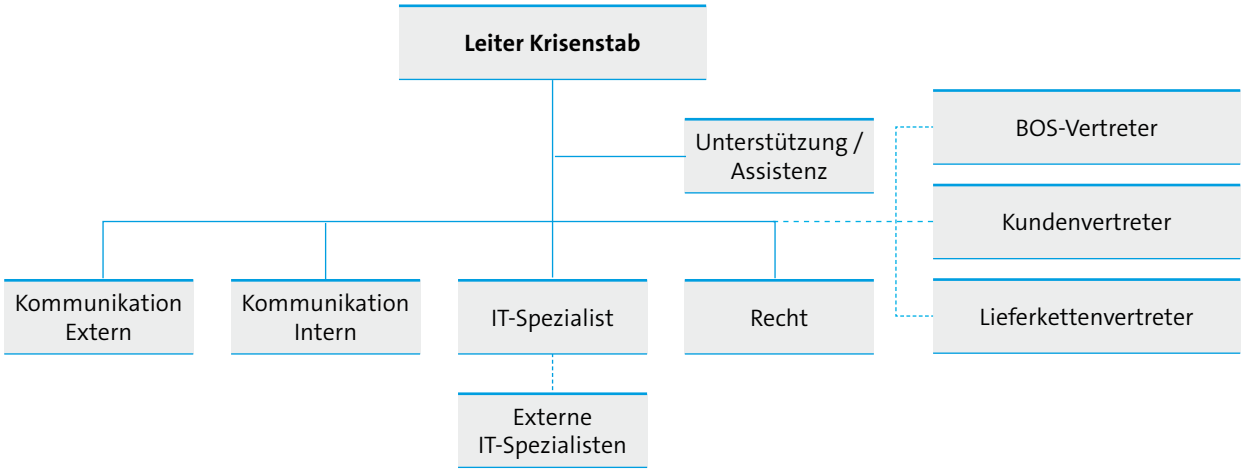

Abbildung 1: Krisenstabsorganisation

- **Leiter Krisenstab:** Der Krisenstabe sollte von einem Mitglied der Geschäftsleitung oder dem Vorstand übernommen werden. Nur wenn die erforderlichen Fähigkeiten fehlen, sollte eine direkt beauftragte und mit vollumfänglicher Entscheidungsbefugnis versehene Person diese wesentliche Aufgabe ausfüllen. Hier sind unter Zeitdruck mitunter langfristig wirkende Entscheidungen zu treffen.

- **Recht**: In Krisen sind oft rechtlichen Fragestellungen schnell zu prüfen, deshalb sollte hier die Rechtsabteilung des Unternehmens im Krisenstab vertreten sein, die wiederum dritte Rechtsanwälte oder Kanzleien koordinieren kann.

- **Kommunikation Intern**: Hier muss eine verantwortliche Stelle die Kommunikation mit den intern betroffenen Unternehmensbereichen und internen Kunden transparent und dauerhaft verfügbar führen. Hier wird mit Mitarbeitern, dem Betriebsrat, Abteilungsleitern usw. kommuniziert.

- **Kommunikation Extern**: Hier muss zwingend ein mit Krisenerfahrung ausgestatteter Kommunikationsprofi für die Kommunikation mit der Außenwelt besetzt sein. Hier wird mit Behörden (BOS, Datenschutz), mit Vertretern der Stakeholder des Unternehmens und vor allem mit den Medien und Dritten kommuniziert.

- **IT-Spezialist:** Ein Mitglied des Krisenstabes muss quasi die operativen Maßnahmen steuern. In Cybersicherheitsvorfällen sollte dies ein IT-Spezialist sein, der auch im Bereich Cybersicherheit notwendige organisatorische und technische Kenntnisse mitbringt.

- **Externe Gruppen:** Je nach Unternehmen und Geschäftsmodell, kann sich ein Cybersicherheitsvorfall im Krisenstadium auch auf Dritte auswirken. Diese sollten frühzeitig in die Krisenorganisation eingebunden werden, um die nötigen Eindämmungsschritte auch bei diesen zu gewährleisten und auch hier transparent zu kommunizieren.

Wesentlicher Bestandteil des Notfall- und Krisenmanagements ist die zielführende und abgestimmte Einbindung der zuständigen Behörden und Organisationen mit Sicherheitsaufgaben (BOS). Hier kann sowohl die Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) als auch den zuständigen ZACs oder der Sicherheitskooperation Cybercrime sinnvoll sein. Krisenkommunikation im engeren Sinne hat zur Aufgabe jegliche offizielle Kommunikation eines Unternehmens während und nach einem sicherheitskritischen Ereignis, unabhängig von Adressat und Form der Kommunikation, im Zusammenhang mit dem Ereignis, seiner Ursachen, Folgen sowie die Schadensbewältigung zu managen. Es werden mit hoher Wahrscheinlichkeit Anfragen der Medien, der Geschäftspartner, interessierter Dritter, der Mitarbeiter und evtl. deren Angehörigen aufkommen. Diese dürfen nicht ignoriert werden, weil dadurch leicht die Botschaft transportiert wird, dass sich das Unternehmen nicht äußert und etwas verheimlichen will. Dies darf aber die eigentliche Arbeit des Notfall- oder Krisenstabes nicht vom Management und der Bewältigung des Ereignisses abhalten. Für diese Aufgabe müssen in der Übungsplanung

sowie dem Notfall- und Krisenkonzept folgende Phasen unterschieden werden, um möglichst effizient zum Normalbetrieb zurückkehren zu können.

- während des Notfalls oder der Krise (Phase 1),
- unmittelbar nach dem Notfall oder der Krise (Phase 2),
- während einer evtl. Phase mit Betriebsunterbrechung oder -einschränkung (Phase 3)
- die Wiederaufnahme des Normalbetriebs (Phase 4).

Phasen eines Notfall- und Krisenkonzepts

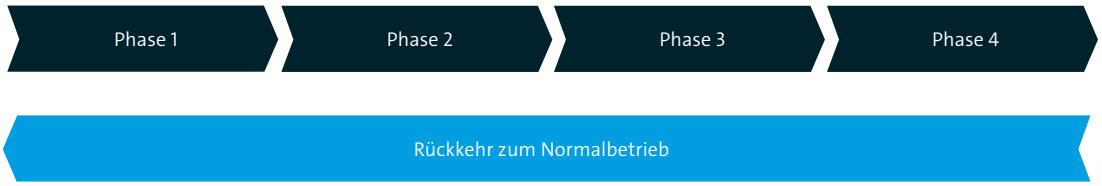

Abbildung 2: Phasen eines Notfall- und Krisenkonzepts

Alle von Menschen geschaffenen organisatorischen und technischen Systeme sind fehleranfällig – von einem Systemversagen ist also grundsätzlich auszugehen. Entscheider sollten also eine Notfall- und Wiederanlaufplanung vorsehen und diese regelmäßig erproben und optimieren.

»Wiederanlauf« meint in diesem Sinne nicht allein eine Wiederherstellung der betrieblichen Abläufe auf Basis einer möglicherweise systemimmanenten Fehleranfälligkeit der Informations- und Kommunikationstechnologie (ITK), sondern auch eine Verbesserung der ITK-Infrastruktur, um erkannte Schwachstellen zu beheben und die Stabilität des Systems zu erhöhen (s. u. Wiederherstellungskosten).

Während all dieser Phasen können folgende Schadenspositionen auf eine Organisation oder Unternehmen zukommen:

- Kosten für Ausstattung des Krisenstabes (Unterbringung, Verpflegung, Anreise usw.)
- Kosten Überstundenausgleich und Krisenbewältigungsprämie
- Kosten externer Krisendienstleister (Krisenstabsleiter, Kommunikationsprofis)
- Kosten externen IT-Dienstleister im 24/7 Notfallmodus
- Kosten externen Rechtsberatung (s. a. dort)
- Kosten für Aufwand externer Krisenstabsmitarbeiter von Zulieferern und Kunden

2.4 Wiederherstellungskosten

Bei einer Beeinträchtigung eines Systems ist das Ziel die Herstellung eines sicheren Zustands des Systems sowie die Wiederherstellung der betroffenen Daten auf einen Systemstand vor dem Ausfall bzw. Angriff.

Dabei fallen folgende Kosten an:

- Personalkosten zur Datenwiederherstellung nach Aufsetzen eines sicheren System sowie eventuell zusätzliche Kosten zur Datenrekonstruktion von nicht gesicherten Daten (z. B. durch externe Dienstleister);
- Kosten für einen eventuell notwendigen Standortwechsels des Rechenzentrums (z. B. Reisekosten der Mitarbeiter für Bahn, Flug, PKW und Hotel) oder durch Inanspruchnahme externer IT-Services und Unterstützungsleistungen;
- Personalkosten für Analyse des Systemausfall (z. B. forensische Untersuchungen) inklusive Empfehlungen für Konfigurationsänderungen zum Aufsetzen des sicheren Systems;
- Kosten für Betriebsmittelschäden (z. B. bei Ausfall der Klimaanlage beschädigte IT-Komponenten durch Überhitzung oder bei Stromausfall/Ausfall unterbrechungsfreie Stromversorgung durch Beschädigung der Festplatten);
- Kosten für zusätzlich nötig gewordene Lieferanten oder gar einen Lieferantenaustausch, z. B. bei nicht behebbaren Sicherheitslücken der verwendeten Systeme und Anwendungen inklusive der Kosten für System- und Architekturanpassungen;
- Aufarbeitung des entstandenen Betriebsstaus durch die Unterbrechung z. B. mit Hilfe von zusätzlichem Personal, respektive angeordneter Mehrarbeit.
- Evtl. Mehrkosten eines Ausschreibungsprozesses inklusive der Begleitung im Auswahlverfahren, die Arbeitszeit und Personal binden, wenn einzelne oben genannte Positionen ausgeschrieben werden müssen.

Zusätzlich fallen folgende indirekte Kosten an, die sich auch mit den Kosten der Forensik überschneiden können:

- Interne Ermittlungskosten, falls bei der Analyse des Systemausfalls Hinweise auf inkorrektes Verhalten von Mitarbeitern festgestellt wurden;
- eventuelle Prozesskosten, falls bei Innentätern arbeitsrechtliche Maßnahmen durchgeführt werden müssen.

Fallbeispiel

Bei einem Mittelständler in NRW ist während einer Internetrecherche ein Trojaner installiert worden, der Dateien verschlüsselt, die auf verbundenen Netzlaufwerken liegen. Experten sprechen von einem sogenannten »Drive-by-Download«. Die vorhandenen Virenscanner haben diesen Trojaner zwar gemeldet, konnten aber nicht verhindern, dass einige Dateien und Verzeichnisse verschlüsselt wurden. Nach einer umfangreichen Analyse der Verzeichnisse, mussten diese aus einem Vollbackup, das mehrere Tage alt war, wiederhergestellt werden. Die Untersuchungen zeigten, dass sowohl die Verzeichnisse der Kostenrechnung als auch der Einkaufsabteilung komplett betroffen waren, sowie Teile der Ergebnisrechnung und der Buchhaltung.

Exkurs

Die Recovery von Backups, die integer / sauber sind ist nicht trivial. Es bedarf der Synchronisation von Produktivdaten, die seit dem letzten Backup entstanden sind und konsistent ins Backupsystem überführt wurden, ohne selbst betroffen zu sein.

Schadenausmaß

In der Summe wurden ca. 9 GB bzw. 1600 Verzeichnisse mit knapp 21.000 Dateien wiederhergestellt. Die Kosten für den internen Personalaufwand und die Unterstützung durch externe IT-Forensiker belief sich auf EUR 150.000.[2]

2.5 Krisenberatung

Krisenmanagement im Zusammenhang mit Cyberangriffen unterscheidet sich in mehreren Dimensionen von klassischem Krisenmanagement, z. B. im Zusammenhang mit personellen oder physischen Angriffen (Entführung, Bombendrohung oder Terroranschlag).

Zunächst ist die Gruppe potenzieller Opfer nicht sinnvoll eingrenzbar. Moderne, vernetzte Technologien und Wertschöpfungsprozesse führen dazu, dass fast jedes Unternehmen überall auf der Welt Opfer oder Werkzeug eines Cyberangriffs werden kann. Viele Unternehmen sind für einen solchen Fall organisatorisch schlecht vorbereitet. Der Aufbau dieser Strukturen – so sinnvoll er auch im Einzelfall sein mag – überfordert viele Unternehmen sowohl technisch als auch finanziell. In diesem Fall ist es sinnvoll, entsprechend spezialisierte IT-Dienstleister beratend und auch zur Unterstützung im Notfall heranzuziehen.

2 Vgl.Marsh (Detaillierte Quellenangaben einfügen)

Die Fähigkeiten, über die eine Krisenmanagement-Organisation für Cyberangriffe verfügen muss, unterscheiden sich ebenfalls signifikant von denen für traditionelle Krisen infolge intentionaler Risiken. Die Krisenteams sind üblicherweise größer, was wiederum einen hohen Reifegrad der Organisation wie auch hohe und einheitliche Ausbildungsstände der Krisenmanager erfordert. Die Zusammenarbeit mit Behörden stellt weitere personelle Anforderungen, denn die Zahl der involvierten Behörden ist üblicherweise höher als beispielsweise bei einer Erpressung (z. B. in Form des Landes- oder Bundesdatenschützers oder des BSI). Zusätzlich zeichnen sich Cyberkrisen durch ein hohes Maß an Komplexität aus, das Krisenteams vor substanzielle Herausforderungen stellen kann: Wenngleich die Zahl der tangierten Interessengruppen vergleichsweise klein sein kann (Justiz, Datenschutz, Öffentlichkeit, Politik), ist eine herkömmliche Dreipunktprojektion auf den schlechtesten, besten und wahrscheinlichsten Verlauf der Krise häufig nicht sinnvoll möglich, woraus sich weiter erhöhte Anforderungen an die Entscheidungsfindung des Krisenteams ergeben. Das bedeutet: Der Entscheidungsdruck steigt infolge der Menge und zeitlichen Kritikalität der Interessengruppen-Anfragen, während gleichzeitig die Entscheidungsgrundlage wenig bis unbekannt bleibt.

Außerdem zeichnen sich Cyber-Krisen häufig durch besonders hohe Öffentlichkeitswirksamkeit aus. Hieraus ergibt sich die Notwendigkeit, häufig ebenfalls nicht vorhandene Ressourcen in der Krisenkommunikation bereitzuhalten oder im Krisenfall zu engagieren.

Die meisten Unternehmen sind auch nicht auf die Zusammenarbeit zwischen dem strategisch ausgerichteten Krisenmanagement und der operativen Notfallbewältigung im Rahmen des Business Continuity Managements eingerichtet. Auf diese Weise entstehen einerseits hohe Reibungsverluste im Krisenmanagement (das nicht ausreichend schnell mit notwendigen und verständlichen Informationen versorgt wird) und andererseits im Notfallmanagement (das unklare oder unrealistische Vorgaben aus dem Krisenmanagement erhält).

2.6 Verbesserung der Organisations- und IT-Strukturen

Das System muss kurzfristig gehärtet werden,
um nicht sofort wieder verwundbar zu sein.
Die erfolgt idealer Weise in 3 Schritten.

Ein Cyber-Schadensfall in einer Organisation erfordert meist eine direkt anschließende Verbesserung der vorhandenen Infra- und Prozessstrukturen, da Schadensfälle häufig aufgrund von mangelhaften oder veralteten Sicherheitsprodukten und -prozessen auftreten.

Zu berücksichtigen ist hier auch, dass oftmals die Verbesserung der bestehenden Systeme in einem fließenden Prozess erfolgen muss. Eine trennscharfe Neuaufsetzung nach der Bearbeitung eines Krisenfalls lässt sich schwerlich verwirklichen, da die Geschäftsprozesse auch im Krisenfall in der Regel nicht völlig eingefroren werden können. Die Erfahrungen

bei hochprofessionellen APT-Sicherheitsvorfällen, wie beispielsweise diesem aus dem Deutschen Bundestag Anfang 2015 ist, dass man nicht den »Vorfall erst abschließen kann« und alles wieder so herstellt wie zuvor, sich dann die Zeit nimmt und eine neue Systemorganisation strukturiert gestalten kann. Vielmehr muss eine IT-Struktur kurzfristig geändert und gehärtet werden, damit der Angreifer nicht sofort wieder über die »alten« Fehler erneut eindringen kann.

Als Reaktion auf den jeweiligen Schadensfall genügt es oftmals nicht, die betroffenen Sicherheitslösungen in der IT-Infrastruktur auszutauschen. Die Verbesserung der vorhandenen Strukturen muss vielmehr gezielt erfolgen, dabei muss angelehnt beispielsweise an ISO 27001 und den IT-Grundschutz in den PDCA-Zyklus (plan-do-check-act) für das IT-Sicherheitsmanagement einbezogen werden.

Während die Kosten für die eigentliche Schadenerfassung im Bereich der IT-Forensik angesiedelt sind, sind für die Verbesserung der IKT-Infrastruktur in Abhängigkeit des Schadensfalles technische und organisatorische Maßnahmen organisationsweit zu betrachten. Dies betrifft in einem ersten Schritt die Schwachstellenanalyse als Grundlage für den Status quo der Verbesserungsmaßnahmen, geht weiter über die Schwachstellenadressierung und schließt mit der Umsetzung der Lösungsmöglichkeiten ab. Hier konkrete Fixkosten zu benennen gestaltet sich schwierig, da sowohl Prozesse als auch Strukturen und eingesetzte Technologien von Organisation zu Organisation stark unterschiedlich sein können.

Schritt 1: Schwachstellenanalyse:

In diesem Bereich muss sich der IT-Sicherheitsverantwortliche damit auseinandersetzen, wodurch der Cybersicherheitsvorfall möglich wurde. Die Erkenntnisse aus der Schadenerfassung im Rahmen der Wiederherstellung sollten dazu verwendet werden, um zu überprüfen, ob die aufgetretenen Schwachstellen auch in anderen Teilen der Organisation oder der Infrastruktur auftreten können. Dabei genügt nicht nur eine Betrachtung der Sicherheitssysteme, vielmehr muss der Blick hier organisationsweit gehen und die relevanten Prozesse und Infrastrukturelemente einbeziehen.

Wichtige Fragen, die in dieser Phase beantwortet werden sollten sind: Welche Teile der Infrastruktur waren betroffen und eventuell verantwortlich und werden diese Komponenten auch in anderen Bereichen des Unternehmens eingesetzt? Haben organisatorische Mängel den Cyberangriff begünstigt? Waren die Notfallvorsorge und die firmeninterne Kommunikation ausreichend einbezogen? Waren Hardware-Komponenten und/oder genutzte Software mangelhaft? War das Personal nicht ausreichend geschult? Interne und externe Aufwendungen entstehen in dieser Phase hauptsächlich für die Analyse der Infrastruktur und Organisation in Bezug auf die identifizierten Schwachstellen. Ein Ergebnis kann aber auch sein, dass das betroffene Unternehmen neue Ressourcen für das Thema Sicherheit bereitstellen muss. Die daraus resultierenden Personalkosten werden aber nicht als Kosten eines

Sicherheitsvorfalls einzustufen sein. Vielmehr wird es sich so verhalten, dass Kosten eines Angriffs in der Folge dann geringer ausfallen können, da die Auswirkungen von mehr Spezialisten aufgefangen werden können.

Schritt 2: Adressierung und Behebung von Schwachstellen

Der Ergebnisumfang bei der Schwachstellenanalyse bestimmt die Art, wie die gefundenen Sicherheitslücken behoben werden. Für alle identifizierten Elemente und Prozesse sind entsprechende Maßnahmen zu definieren, die zu einer Behebung der Schwachstellen beitragen. Die Verantwortlichen können die Infrastruktur verändern, die komplette Organisation in die Notfallvorsorge einbeziehen, Hardware und Software auf den Stand der Technik anpassen sowie Weiterbildungsmaßnahmen für das Personal in Sachen IT-Sicherheit und Cyberbedrohungen einplanen. Diese Phase sollte eng in Zusammenhang mit der Schwachstellenanalyse erfolgen und zieht auch interne bzw. externe Aufwendungen nach sich – in Abhängigkeit von der Menge der identifizierten Schwachstellen.

Schritt 3: Umsetzung der Lösungsmöglichkeiten

Der letzte Schritt und auch größte Kostenfaktor liegt in der Auswahl und Umsetzung der zuvor festgestellten Maßnahmen.

Nach Abschluss einer oder mehrerer Maßnahmen empfiehlt sich eine Nachbetrachtung deren Wirksamkeit. Diese Nachbetrachtung sollte möglichst durch eine unabhängige Instanz wie z. B. der internen Revision oder einer externen Prüfungsgesellschaft erfolgen.

Allerdings, diese Kosten könnten auch schon aus den konkreten Kosten eine Cyber-Sicherheits-vorfalls herausgenommen werden, weil sie insoweit im Grunde die Kosten der Herstellung eines angemessenen IT-Schutzniveaus darstellen, das vorher offenbar nicht gegeben war. Gleichwohl stellen sich diese Kosten entsprechend höher dar, wenn es zu einem Vorfall gekommen ist, als wenn diese im laufenden Betrieb zu einem Maß an Prävention und Resilienz führen, dass sich Angriffe entweder nicht erfolgreich durchführen lassen oder geringere Ausmaße annehmen. Insofern werden diese hier dennoch als Position genannt und ihre Dynamik sollte berücksichtigt werden.

2.7 Rechtsberatungskosten

Ein weiteres Feld sind die anfallenden Rechtsberatungskosten in Folge eines Cyberangriffs. Hier ergeben sich zwingend Fragestellungen nach Datenschutz, der Haftung für Dritte und gegenüber Mitarbeitern, Kunden usw. Informationspflichten müssen geprüft werden, die sich aus dem AktienG, Produkthaftung, BDSG, oder dem neuen IT-SiG ergeben können sowie nach Compliance-Richtlinien. Zudem können sich aus den Auswirkungen des Angriffs auch Auswirkungen auf die Vertragsbeziehungen ergeben, wie Haftungs- oder Freistellungsfragen. Es müssen aus verschiedenen Perspektiven verschiedene Rechtsbeziehungen und Rechtsfragen

juristisch im Krisenmodus aber auch im Anschluss daran, geprüft werden. Die erforderlichen Kapazitäten kann eine vorgehaltene Rechtsabteilung typischer Weise nicht abdecken.

Eine (externe) Rechtsberatung kann im Umfeld einer Cyberattacke folgende Kostenarten entstehen lassen:

- Kosten für Anwälte zur juristischen Bewertung der Situation, insbesondere die Ermittlung der vertraglichen und gesetzlichen Verpflichtungen (z. B. Melde- oder Informationspflichten, etc.) sowie Beratung hinsichtlich der Handlungsoptionen und Schadenseingrenzung;
- die arbeitsrechtliche Beratung bei internen Ermittlungen;
- Kosten für zivilrechtliche Verfahren;
- Klassische Verteidigerkosten im Straf- oder Bußgeldverfahren;
- Cyberangriffe können durch ihre häufig internationale Natur auch die Rechtsberatungskosten steigern, da auch exterritoriale Anwälte beschäftigt werden müssen.
- Durch die Komplexität der Auswirkung wird es nötig werden mehrere unterschiedlich spezialisierte Kanzleien oder Rechtsanwälte zu beauftragen.

2.8 Informationskosten

Schäden durch Cyberangriffe sind häufig nicht auf die angegriffene Organisation beschränkt, sondern können auch indirekte Auswirkungen auf Dritte zur Folge haben. Je nach Organisation und Typ des Vorfalls ergeben sich unterschiedliche gesetzliche, branchenspezifische oder vertragliche Vorgaben, wer wie, wann und in welchem Umfang über einen Vorfall informiert werden muss. Mögliche Adressaten sind Kunden, Partner, Aufsichts- und Regulierungsbehörden, Mitarbeiter, Anleger oder die Öffentlichkeit.

So kann z. B. der Abfluss von personenbezogenen Kundendaten bei einem Unternehmen in Folge einer Schadsoftwareinfektion oder die Kompromittierung eines Online-Shops eine Informationspflicht nach § 42a BDSG auslösen. Analoge Vorschriften gelten auch nach Telemediengesetz (TMG) bzw. Telekommunikationsgesetz (TKG) für bestimmte Branchen. Nicht zuletzt das im Juli 2015 in Kraft getretene IT-SiG enthält Informationspflichten, die die Unternehmen kritischer Infrastrukturen zu erfüllen haben.

Neben diesen allgemeinen, bzw. IT-spezifischen gesetzlichen Vorgaben bestehen darüber hinaus eine Vielzahl weiterer branchenspezifischer Informationspflichten, die bei Cyber-Angriffen zu berücksichtigen wären, beispielsweise:

- Meldung erheblicher IT-Sicherheitsvorfälle an das BSI nach §8b BSI-Gesetz (BSIG) für Betreiber Kritischer Infrastrukturen,
- Ad-hoc-Mitteilung von börsennotierten Unternehmen nach § 15 Wertpapierhandelsgesetz (WpHG),
- jährlicher Bericht über tatsächlich vorgefallene (IT)-Störungen an die Bundesnetzagentur aus § 52 EnWG

- Meldungen an die BaFin aus der MaRisk heraus, die die Einhaltung von bestimmten Sicherheitsstandards vorgibt und daraus eine Informationspflicht für sich ableitet
- Meldungen von Produktionsfehlern von Arzneimittel nach § 3 Medizinprodukte-Sicherheitsplanverordnung (MPSV) oder
- Meldungen nach § 6 Atomrechtliche Sicherheitsbeauftragten- und Meldeverordnung (AtSMV).

Organisationen müssen die für sie relevanten branchenspezifischen Vorgaben kennen und die Notwendigkeit einer Informationspflicht infolge eines Cyberangriffs eigenständig einschätzen können.

Eine Mitteilung kann über Webseiten, E-Mails, Anschreiben, persönliche Telefonate, direkte Gespräche oder die Medien und Presse erfolgen.

Im Rahmen der Krisenkommunikation müssen die zu verbreitenden Informationen vorab in der Organisation zusammengestellt, aufbereitet und freigeben werden. Können die dafür notwendigen Ressourcen nicht intern bereitgestellt werden, kann es notwendig sein, externe Experten zu beauftragen. Darüber hinaus sind vorab Informationen für mögliche Presseanfragen vorzubereiten sowie Mitarbeiter zu informieren und mit einer abgestimmten Sprachregelung auszustatten.

Im Hinblick auf die Kosten ist die Bekanntgabe einer Nachricht auf der Webseite des Unternehmens oder ein Informationsschreiben per E-Mail (Verfügbarkeit dieser Dienste vorausgesetzt), deutlich günstiger als eine Benachrichtigung per Brief oder ein direktes Gespräch. Alleine die Portokosten für die Benachrichtigung einer großen Kundenanzahl ergeben hohe Summen.

Zusätzlich müssen den Betroffenen auch Rückmeldekanäle zur Verfügung gestellt werden, über die Rückfragen angenommen und bearbeitet werden. Auch hier können bestehende Strukturen an Grenzen stoßen, wenn ein Großteil der Kunden gleichzeitig Rückfragen an die von einem Cyberangriff betroffene Organisation richten.

2.9 Erpressung und Lösegeld

Bei Cybercrime Vorfällen versuchen die Täter häufig für die Rückgabe erbeuteter Daten oder für ein Abwenden/Abbrechen einer Betriebsstörung, etwa ausgelöst durch einen Distributed Denial of Service-DDOS Angriff (DDoS), auf die Bestellplattform des Opfers, ein Lösegeld zu erhalten. Relativ häufig wurden die Daten gar nicht entwendet, sondern mittels Verschlüsselung unbrauchbar gemacht (z. B. durch Crypto-Locker oder andere Formen sogenannte Ransomware) und das Schlüsselwort gegen Lösegeld versprochen – eine Hoffnung, die sich in der Praxis meist nicht erfüllt.

Im Einzelfall kann es nach Abwägung der drohenden Gefahren für die Geschäftsprozesse und den damit verbundenen Schaden im Verhältnis zu der Resilienz des Systems erforderlich werden

ein Lösegeld zu zahlen, um schlimmeres zu verhindern. Dies zeigt sich immer dann, wenn nach sorgfältiger Abwägung der Schaden – auch für die Kunden und Dritte – eine Zahlung betriebswirtschaftlich sinnvoller erscheinen lässt. Natürlich steht und fällt die Resilienz mit der Vorbereitung und Härtung der Systeme. Je mehr in die Vorsorge gegen derartige Attacken investiert wurde, um so resilienter ist das System und unwahrscheinlicher werden erfolgreiche Angriffe. Und vor allem wird die betriebswirtschaftliche Abwägung zum Erfolg der Erpressung besser ausfallen, weil die Kosten bei resilienten Systemen deutlich geringer ausfallen, wenn der Angreifer seine Drohung wahr macht. Hier zeigt sich besonders die Kostenersparnis auf lange und mittlere Frist bei Vorsorgekosten (siehe Abb. Kosten und Notfall und Vorsorgekosten)

Beispiel

Ein mittelständisches Unternehmen im Online-Vertrieb ist Opfer von Datenklau geworden. Die Versicherung beziffert alleine die Kosten des Vorfalls im Bereich gesetzlicher Informationspflichten auf 2.170.000 Euro. Für Media- und PR-Arbeiten mussten weitere 253.000 Euro aufgewendet werden.

Quelle: MARSH/Hiscox Versicherung

Grundsätzlich empfiehlt der Redaktionskreis, möglichst sofort die Unterstützung des zuständigen Landeskriminalamtes zu suchen und von einer Lösegeldzahlung abzusehen.

2.10 Vertragsstrafen und Bußgelder

Unter Vertragsstrafen summieren sich eine Reihe von Kosten, die in Folge eines Cybervorfalles entstehen können. Inwieweit diese zum Tragen kommen, hängt von der individuellen Situation ab. Nachfolgend einige Beispiele:

- Vertragsstrafen gegenüber Kunden aufgrund nicht eingehaltener Lieferverpflichtungen sowie aus eventuellen Folgekosten beim Kunden, z. B. aufgrund von Betriebsunterbrechungen, Einnahmeverlusten oder anderen Extrakosten;
- Vertragsstrafen für nicht ausgeübte Abnahmeverpflichtungen gegenüber Zulieferern;
- Vertragsstrafen, die aus (nicht eingehaltenen) Service-Level-Agreements, z. B. bei Datenverarbeitung für Dritte, resultieren;
- Zusätzlich kann es aufgrund gesetzlicher Auflagen (wie etwa durch das Bundesdatenschutzgesetz oder das IT-Sicherheitsgesetz) in einigen Branchen (z. B. Telekommunikation, Finanzwesen, usw.) zu Bußgeldern kommen, die sich in Deutschland auf einige 100.000 Euro belaufen können. Bei Mehrfachverstößen können sich Strafzahlungen aufsummieren oder auch jeweils höher ausfallen.

2.11 Reputationskosten

In marktwirtschaftlichen Strukturen stellt die in vielen Jahrzehnten aufgebaute Reputation eines Unternehmens einen immateriellen Vermögenswert dar – teuer errungen, aber leicht verspielt.

Während Vorräte an Roh-, Hilfs- und Betriebsstoffen (RHB) selbstverständlich in die Bilanz als Vermögenswerte einfließen, bewerten Unternehmen ihren guten Ruf (Reputation) und immaterielle Vermögensgegenstände (Patente etc.) unterschiedlich – den kleinen und mittelständischen Unternehmen (KMU) fehlt noch weitgehend die notwendige Sensibilität, die größeren Unternehmen wissen sehr wohl um die Schutzwürdigkeit dieser »Schätze«. Doch mitunter ergreifen sie selbst dann keine geeigneten Schutzmaßnahmen und adressieren das Thema strategisch nicht ausreichend. Die immateriellen Vermögenswerte eines Unternehmens müssen geschützt werden – darunter eben das Image und Know-how, Marken, Patente, Lizenzen und Webdomains sowie Daten, ob nun explizit bilanziert oder nicht.

Vermögensschutz ist immer zuerst eine Aufgabe der Geschäftsführung bzw. des Vorstands, die allenfalls operativ, nie aber strategisch zu delegieren ist.

Im Grunde befindet sich jedes Unternehmen während seiner Existenz in einer Krise, wobei nicht jedes im Betriebsalltag auftretende Problem zu einer Krise aufgebauscht werden sollte – es geht um Nüchternheit und Sachlichkeit, ohne die dramatischen Dimensionen gerade für den Mittelstand zu verharmlosen.

Beispiel

Diskontinuierliche Produktion: Wenn es im Rahmen eines Sicherheitsvorfalls zu einem Produktionsausfall kommt, bringt das eine erzwungene Änderung der Produktionssequenz mit sich. Ein produzierendes Unternehmen ist dann ggfs. nicht in der Lage, die geplanten Aufträge fristgerecht und vollumfänglich abzuarbeiten. Vertragsstrafen können die Folge sein.

Im Folgenden geht es um eine konkrete Gefährdung des Unternehmens (oder auch des Verbandes oder Instituts) durch einen Ausfall bzw. eine schwerwiegende Beeinträchtigung der mit dem Internet verbundenen ITK. In dieser Krise ist das Unternehmen einem erhöhten Risiko ausgesetzt, d. h. es besteht die Gefahr, dass existenzielle Unternehmensziele nicht mehr erreicht werden (z. B. Erzielung eines Mindestgewinns und Erhaltung der erforderlichen Liquidität).

In diesem Sinne wird hier eine akute, aber beherrschbare Unternehmenskrise betrachtet, die mit dem zur Verfügung stehenden Krisenbewältigungspotenzial erfolgreich gemeistert werden kann.

Reputationskosten, die hierbei in Folge des Vorfalls als Schaden entstehen können sind folgende:

- Kosten für Werbung für die Produkte, die in Verruf geraten sein können oder für das Unternehmen und die Marken.
- Wertkorrekturen durch Abfallen des Aktienkurses oder sogar eine dauerhafte Gefährdung der Indizierung in einem Aktienindex.
- Niedrigere Umsatzzahlen durch Kundenrückgang erfordern Kundenbindungsprogramme.
- Kosten für Markforschung.
- Kosten für Imagekampagnen und langfristige Imagestrategien.
- Kapitalvernichtung in der Bilanz (Minderung des Unternehmenswertes).
- Höhere Kreditzinsen durch Reduzierung der Bonität (höhere operationelle Risiken).
- Höhere Versicherungsprämien.
- Mehraufwand für das klassische Marketing.
- Mitarbeiterbindung und Vertrauensgewinnende Maßnahmen

2.12 Krisenkommunikation (nach Schadenseintritt)

Obwohl die Krisenkommunikation erst an dieser Stelle behandelt wird, ist sie gleichwohl unmittelbar nach Eintritt der Krisensituation erforderlich und notwendig. Der Wert guter Krisenkommunikation darf in einer modernen Informationsgesellschaft nicht unterschätzt werden. Krisenkommunikation ist insofern durch Krisenberatung zu unterscheiden, als sie sich auf die Kommunikation des Unternehmens in Krisenzeiten bezieht, während die Krisenberatung weiter gefasst den organisatorischen und strukturellen Umgang mit der Krisensituation umfasst. Gleichwohl kann das Beratungsangebot am Markt fließende Übergänge beinhalten.

Hier muss das in der Präventionsphase Aufgebaute und Trainierte innerhalb kürzester Frist aktiviert werden! Zusätzliche Mittel sind insbesondere für die Kommunikation mit der Öffentlichkeit/Presse vorzuhalten, denn es darf ihnen keine Gelegenheit gegeben werden, sich über die Krisenbewältigung zu beschweren. Trotz aller Aufregung und allen Zeitdrucks sind Takt, Entgegenkommen und Offenheit gefragt – ein Leugnen oder Schönreden der Situation wäre fatal und vernichtet Reputation!

Wichtig ist es, mit vielen Informationen Verantwortungsgefühl zu zeigen und die Diskussion auf eine nüchterne, sachliche Ebene zu bringen. Um die Journalisten vom schadensbehafteten Betrieb zu distanzieren, empfiehlt sich die Nutzung eines »neutralen Ortes« (z. B. Tagungsbereich in einem Hotel) für Pressegespräche und -konferenzen. Umfangreiche Pressemappen mit grundlegenden Informationen (ergänzt um aktuelle Pressemitteilungen) sind anzubieten, wie auch ein angemessenes Catering, welches weder Geiz noch versuchte Einflussnahme suggeriert.

Beispiel

Beispiele für schlechte Krisenkommunikation zeigen immer wieder, dass die negative mediale Aufmerksamkeit und der damit einhergehende Reputationsverlust deutlich länger in den Köpfen der Kunden und Öffentlichkeit nachhalten. So hat die Kommunikation von BP beispielsweise in der Deep-Water-Horizon Katastrophe nachhaltigen Schaden verursacht. Die Aussagen des damaligen BP Chefs Tony Hayward spielten zunächst den Vorfall herunter. In einem frühen Statement sagte er - trotz der 11 durch die Explosion getöteten Arbeiter: Der Golf von Mexiko ist ein sehr großer Ozean und im Vergleich dazu ist die Menge an auslaufendem Öl winzig. In vielen weiteren Interviews findet Hayward nach Meinung der Betroffenen selten den richtigen Ton oder die passenden Worte: »Niemand will mehr als ich, dass diese Sache vorbei ist. Ich hätte gerne mein Leben zurück.« Er beschwichtigt, wo er die unangenehme Wahrheit aussprechen müsste, und ist zu ehrlich, wo er mehr Mitgefühl ausdrücken müsste. Auch kommunizierte BP zunächst, es würden nur etwa 800.000 Liter Rohöl am Tag ausströmen. Einen Monat darauf mussten hochrangige Mitarbeiter von BP vor dem U.S.-Kongress zugeben, dass aus dem Leck täglich bis zu 9,5 Millionen Liter ausströmen würden. BP zahlte in der Folge 65,5 Milliarden Dollar und das Unternehmen brauchte knapp 5 Jahre um wieder auf die Ergebnisse vor der Krise zu kommen. Und bei diesem, zugegebener Weise besonderen Beispiel, war das Business Continuity Management kaum tangiert, weil die Ölförderung weltweit für BP nicht abgeschnitten war.

1. **Inbetriebnahme einer Hotline für Kunden, Lieferanten, Presse und Öffentlichkeit (auch Behörden)**
   - Beantwortung von Anrufen, E-Mails, Faxschreiben und Briefpost

2. **Aktivwerden der PR-Agentur**
   - zielgruppenorientierte Informationsbereitstellung (Presse, Öffentlichkeit, Sicherheitsexperten....)
   - Abfassung/Publikation von Pressmitteilungen und eigenen Berichten

3. **Aktivwerden einer Eventagentur für Informationsveranstaltungen**
   - externer Pressesprecher
   - Sachkosten/Honorare

4. **evtl. Kompensationszahlungen**
   - ggf. freiwillige Leistungen zur Vermeidung von langwierigen juristischen Auseinandersetzungen
   - **Sachkosten**

5. **Nachbearbeitung der Krise und Begleitung der Verbesserungsmaßnahmen**
   - Vermarktung der gelungenen Krisenbewältigung für die Rückgewinnung bzw. Festigung des Vertrauens der Stakeholder. Dokumentation und Wissensmanagementmaßnahmen für die lernende Organisation.

2.13 Litigation-PR

Hierunter wird »Öffentlichkeitsarbeit im Rechtsstreit« bzw. auch »strategische Rechts-kom-munikation« oder »prozessbegleitende Öffentlichkeitsarbeit« verstanden. Es handelt sich um eine Form der Pressearbeit, bei der die Kommunikation nach außen vor, während und nach juristischen Auseinandersetzungen gesteuert wird. Ihr Ziel ist es, die juristische Strategie der beteiligten Anwälte zu unterstützen, das Ergebnis der juristischen Auseinandersetzung mit Hilfe der Öffentlichkeit zu beeinflussen und gleichzeitig Schäden an der Reputation des Mandanten zu vermeiden (sie ist verwandt mit Reputationsmanagement und Krisen-PR).

Beauftragung von Experten für die professionelle, rechtssichere Kommunikation in öffentlichen und medienwirksamen Gerichtsverfahren

- Adressaten sind
  - Öffentlichkeit
  - Medien
  - Rechtsvertretungen
  - Experten
  - Ermittlungsbehörden
  - Gerichte
- Sachkosten/Honorare (Rechtsanwaltskanzlei, ggf. PR-Agentur s.o.)
- Vergleichskosten, die gezahlt werden, um die Anzahl der Fälle auf die kritischen zu reduzieren oder um keine Kleinlichkeit bei persönlich Betroffenen zu zeigen.

2.14 Nachhaltige Beseitigung des Reputationsschadens

Wer einen Schadensfall hinter sich hat, ist gewissermaßen in den Augen der Öffentlichkeit »auf Bewährung«. Analog gilt das oben Aufgeführte, jedoch mit größerem Nachdruck! Zu Präventionskosten kommt ein zusätzlicher Aufwand, um erkannte Schwachstellen in der eigenen Infrastruktur/Technik zu beheben und das eigene vorbildliche Handeln zu kommunizieren, ohne dabei werbend zu wirken, gleichzeitig aber ohne Scham aus der Krise gelernt zu haben. Die Krise sollte am Ende im besten Fall als Chance genutzt werden.

Auch dieser Punkt ist mit Überschneidungen mit den Reputationsschäden zu sehen und hier ergeben sich fließende Übergänge. Hier ist allerdings der Fokus auf diesen Kosten, die nach der Krise wirken sollen. Ein Cyber-Sicherheitsvorfall kann die Reputation nachhaltig stören.Die Kosten dadurch sind oben beschrieben. Wenn das Unternehmen die verlorene Reputation nachhaltig wieder aufbauen will und zudem eine Sicherheitskultur verwirklichen, fallen die nachfolgenden Kostenpositionen an:

Organisatorische und technische Maßnahmen, um sich als sicherheitsbewusstes Unternehmen in der Öffentlichkeit zu präsentieren und Wiederholungen zu vermeiden

- ggf. Einstellung hochqualifizierter Sicherheitsexperten
- Personalkosten für nachgeordnete Spezialisten
- Konferenzbeiträge, Artikel (Anzeigen) in Fachzeitschriften, Organisation von Veranstaltungen für Experten und die interessierte Öffentlichkeit zur Diskussion von Sicherheitsthemen und Darstellung eigener Best-Practice-Lösungen
- Investitionen in verbesserte Infrastruktur/Technik
- Sachkosten

3 Fremdschäden

Während sich Eigenschäden noch relativ gut abschätzen lassen, sind Fremdschäden, die durch einen Cybersicherheitsvorfall entstehen können, sehr viel schwerer vorherzusehen.

Denn bei derartigen Vorfällen ist nicht nur fraglich, welche Schäden in tatsächlicher Hinsicht auf einen Cybersicherheitsvorfall zurückzuführen sind, sondern zu klären bleibt auch, inwiefern diese rechtlich dem Vorfall zugeordnet werden müssen und ob eine Haftung für sie besteht.

Die Haftungsrisiken gegenüber Dritten können in diesem Zusammenhang jedoch eine beachtliche, ggf. sogar existenzbedrohende Höhe aufweisen, sodass eine umfassende Bewertung unumgänglich ist. Deshalb wurde zur leichteren Einschätzung der Fremdschäden ein Fragenkatalog genutzt. Mit dessen Hilfe können die Schadenspositionen für das eigene Unternehmen in der Selbstanalyse besser erfasst werden, während die Analyse der Eigenschäden oben im Abschnitt Eigenschäden weitest möglich bearbeitet wurde.

Bei der Durchführung der Bewertung sollte zunächst einmal evaluiert werden, an welchen Stellen es überhaupt zu Schäden durch einen erlittenen Cybersicherheitsvorfall kommen kann. Es empfiehlt sich folglich, eine Supply-Chain-Analyse durchzuführen sowie eine Betrachtung darüber vorzunehmen, inwieweit die Qualität der Endprodukte durch einen Cybersicherheitsvorfall beeinflusst werden könnte.

Hieraus können nun mögliche Schäden abgeleitet werden, die es hinsichtlich der für sie bestehenden Haftungsrisiken zu bewerten gilt. In diesem Zusammenhang sollte ein spezialisierter Anwalt oder die Rechtsabteilung hinzugezogen werden, da nur so eine verlässliche rechtliche Einschätzung gewährleistet werden kann.

Grundsätzlich kann eine Verpflichtung zur Haftung aufgrund unterschiedlicher materiellrechtlicher Anspruchsgrundlagen bestehen.

Eine Haftung kann sich zunächst aus einer vertraglichen Abrede ergeben. So ist es beispielsweise möglich, dass im Rahmen einer Vertraulichkeitsvereinbarung Haftungspauschalen für Cyber-sicherheitsvorfälle vereinbart werden, bei denen es zu einem Datenabfluss kommt.

Während derartige Vereinbarungen in diesem Fall noch recht klar beziffert werden können, ist dies in anderen Fällen des vertraglichen Schadensersatzes schon deutlich schwerer zu bewerkstelligen.

Werden beispielsweise Zugangsdaten eines Online-Auktionshauses durch Hacker entwendet, ergibt sich in der Regel ein Schadensersatzanspruch der betroffenen Kunden gegen das Auktionshaus hinsichtlich der erlittenen Schäden.

Neben den vertraglichen Schadensersatzansprüchen gibt es auch besonders geschützte Vertrauenstatbestände, die ebenfalls eine Haftung für Schäden, die andere aufgrund von Cybersicherheitsvorfällen erlitten haben, begründen können.

Werden zum Beispiel im Rahmen von Vertragsverhandlungen Produktspezifikationen einem Zulieferer zur Verfügung gestellt, die dann durch einen Cybersicherheitsvorfall offengelegt werden, kann sich daraus eine Haftungspflicht von erheblicher Höhe für den Zulieferer ergeben.

Gerade bei langen Supply-Chains gewinnen die Fälle gesetzlicher Haftung an Bedeutung, da eine gesetzliche Pflicht zur Haftung auch dann begründet sein kann, wenn zwischen dem Geschädigten und dem Unternehmen, bei dem ein Cybersicherheitsvorfall aufgetreten ist, kein Vertragsverhältnis besteht oder bestand. Gerade in Zeiten von weit gestreckten Produktionsprozessen können sich hier Haftungskaskaden ergeben, die schnell existenzbedrohliche Ausmaße annehmen.

Zur Illustration der weitreichenden Folgen von Cybersicherheitsvorfällen können folgende Beispielfälle herangezogen werden:

Wurm in der Finanzbranche

Der Servicemitarbeiter eines IT-Zulieferers in der Finanzbranche infiziert seinen Dienstlaptop in einem Flughafen-WLAN aufgrund eines veralteten Virenscanners mit einem sich selbst verbreitenden Schadprogramm. Durch dieses infiziert nun beim Kunden angelangt dessen Netzwerk, was wiederum zur Folge hat, dass das Netz eines Finanzdienstleisters ausgebremst wird und die Trader ihre Aufträge nicht mehr rechtzeitig an die Börse senden können. Es können Schäden in Millionenhöhe entstehen.

Manipulierter Temperaturfühler

Durch die Verwendung unsicherer Komponenten werden die Steuerungsrechner der Produktionsanlagen in der chemischen Industrie angegriffen. Durch einen manipulierten Temperaturfühler kommt es zu einer Explosion in einem chemischen Fertigungsprozess. Eine Kleinstadt muss evakuiert werden.

Angriff auf die Automobilindustrie

Durch eine veraltete Softwarekomponente im Steuerungssystem eines Produktionsroboters gelingt es, die Fertigung von Fahrzeugen zu manipulieren. Es werden minderwertige Schweißnähte produziert, in der Folge muss eine weitreichende Rückrufaktion gestartet werden, um betroffene Fahrzeuge, deren Crash-Sicherheit nicht mehr gewährleistet werden könnte, auszutauschen.

Missbrauch von Zahlungssystemen

Ein Handelsunternehmen wickelt die Zahlungen des Online-Shops über einen zertifizierten Payment Provider ab. Bei diesem kommt es zu einer Cyberattacke. Im Prinzip haftet der Payment Provider, aber der Shop-Betreiber:

- muss seine Kunden informieren;
- hat Umsatzausfälle;
- hat Reputationsschäden und dadurch erhöhte Werbeausgaben in der Zukunft;
- muss eventuell sein Shopsystem aufwändigen Sicherheitsüberprüfungen unterziehen und den Beweis erbringen, dass das Shopsystem nicht die Ursache war;
- muss zusammen mit dem Payment Provider die Datenschutzaufsichtsbehörden informieren (Meldepflicht);
- muss ein anlassbezogenes Audit bei dem Auftragnehmer durchführen.;
- muss sicherstellen, dass angemessene Maßnahmen getroffen wurden.

Dieser Prozess kann leicht Mittel und Ressourcen für bis zu zwei Jahre binden. Wie sich aus den dargestellten Fällen erkennen lässt, dürfen die bestehenden Haftungsrisiken nicht unterschätzt werden, gleichwohl sie auch deutlich schwerer zu beziffern sind, als die möglichen Eigenschäden. Eine umfassende Analyse der bestehenden Risiken im Hinblick auf eine Schadensverursachung bei Dritten ist mithin unumgänglich.

Fragenkatalog

Zur besseren Einschätzung der eigenen Risiken im Hinblick auf Fremdschäden durch Cybersicherheitsvorfälle kann der folgende Fragenkatalog dienen.

Was kann passieren (Generelle Fremdschäden)?

- Können Qualitätsabweichungen in meinen Produkten zu unmittelbaren Gefahren für Leib und Leben führen? (Bsp.: Medikamentenherstellung, Bremsbeläge von Fahrzeugen)
- Können Qualitätsabweichungen meiner Produkte die Qualität der Produkte anderer beeinflussen? (Bsp.: Fehlerhafte Bolzen im Flugzeugbau)
- Welche Auswirkungen kann ein von meinem Vorprodukt verursachter Schaden beim ' Endprodukt für den Endanwender haben? Stürzt letzten Endes das Flugzeug ab oder blättert nur der Lack früher ab?
- Können Fehler meiner IT-Infrastruktur, die IT-Systeme anderer bedrohen (Bsp: Ausfall meiner IT stoppt Produktionsprozesse anderer)?
- Hinsichtlich welcher Datenbestände bestehen besondere gesetzliche (Bsp.: Datenschutz) oder vertragliche (Bsp.: Geheimhaltungsvereinbarungen) Schutzpflichten gegenüber Dritten?
- Wie hoch sind die zu erwartenden Gesamtschäden für die jeweiligen Schadensszenarien?

Was kann dabei durch Cybersicherheitsvorfälle verursacht werden? (Cybersicherheitsfremdschäden)

- Können Cybersicherheitsvorfälle die physische Beschaffenheit von meinen Produkten unmittelbar (Bsp.: Produktionsroboter erhält falsche Anweisungen) oder mittelbar (Bsp.: Werker erhält falsche Produktionspläne) beeinflussen?
- Können Cybersicherheitsvorfälle die digitale Beschaffenheit von meinen Produkten beeinflussen (Bsp.: Internetrouter wird mit einem fehlerhaften und verwundbaren Softwareimage versehen)?
- Können Cybersicherheitsvorfälle auf meinen Systemen auch zu Fehlern der IT-Infrastrukturen anderer führen (Bsp.: Ein Hacker, der in meine Infrastruktur eingedrungen ist, erhält dadurch Zugriff auf die IT-Netzwerke meiner Kunden und kann sich dort weiter ausbreiten.)?
- Können durch Cybersicherheitsvorfälle Daten offengelegt werden, für die besondere gesetzliche oder vertragliche Vorgaben bestehen?

Mögliche Zurechnung und Haftung

- Welche Haftungsmaßstäbe gelten für die entsprechenden Schadensszenarien?
  - Für was hafte ich vertraglich?
  - Für was hafte ich gesetzlich?
  - Ist die Haftung verschuldensabhängig?
  - Hafte ich nur für Vorsatz und grobe Fahrlässigkeit oder auch für leichte Fahrlässigkeit?
  - Ist die Haftungssumme begrenzt?

- Was sind die Voraussetzungen für das Bestehen des Versicherungsschutzes?
  - Klassische Betriebs- und Vermögensschadenhaftpflichtversicherungen bieten in der Regel keinen ausreichenden Schutz vor den Ansprüchen aus Datenverlusten
  - Liegt kein Verschulden des Versicherungsnehmers vor, so haftet er auch nicht im Sinne der Versicherung
  - In der Regel leistet der Versicherer nur für gesetzliche Haftpflichtansprüche, jedoch nicht für vertragliche
  - Neuartige Cyber-Versicherungen bieten nun auch Schutz vor vertraglichen und verschuldensunabhängigen Schadensersatzansprüchen, haben aber bestimmte Voraussetzungen und Obliegenheiten.

- Wo bestehen Prüfungspflichten für Produkte?
  - Überprüft der Kunde selbst die Eingangsprodukte?
  - Wer haftet für die Sicherheit bestehender Netzwerkverbindungen?

Rechtliche Haftungsbegrenzung

- Rechtliche Schutzmaßnahmen
  - Wo sind Haftungsausschlüsse vereinbart?
  - Wo sind Haftungssummen vertraglich begrenzt?
  - Welche zwingenden rechtlichen Vorgaben bestehen für technische und organisatorische Schutzmechanismen, sodass diese ohnehin erfüllt sein müssen?

Technisch-organisatorische Haftungsbegrenzung

- Organisatorische Schutzmaßnahmen
  - Welche Haftungsrisiken werden durch den Einsatz von welchen geeigneten organisatorischen Gegenmaßnahmen vermieden (Bsp.: Ein eingerichtetes ISMS kann dazu führen, dass keine Sorgfaltswidrigkeit besteht)?
  - Inwiefern bestehen Zertifizierungen für meine Infrastruktur?
  - Welche zusätzlichen Maßnahmen könnte ich noch ergreifen, sodass im Schadensfall ein Mehr kommuniziert werden könnte?
  - Wie hoch sind die Kosten für die jeweiligen Maßnahmen?

- Technische Schutzmaßnahmen
  - Welche Haftungsrisiken begrenze ich durch den Einsatz von geeigneten technischen Gegenmaßnahmen?
  - Welche zusätzlichen Maßnahmen könnte ich noch ergreifen?
  - Wie hoch sind die Kosten für die jeweiligen Maßnahmen?

Wirtschaftliche Haftungsabwälzung

- Gegen welche Haftungsrisiken bin ich versichert?
- Wie verhalten sich die Versicherungskosten im Hinblick auf das Bestehen von organisatorischen und technischen Gegenmaßnahmen? Ist es sinnvoll, sich nur zu versichern, nur technisch-organisatorische Schutzmaßnahmen zu ergreifen, oder auf eine Kombination aus beidem zu setzen?

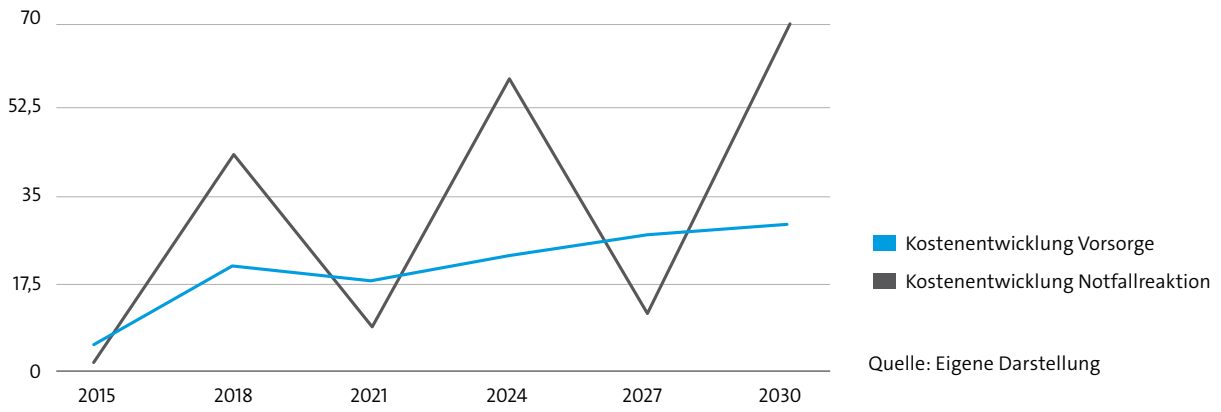

Abbildung 3: Kostenentwicklung Vorsorge vs. Notfallreaktion

4 Präventionskosten

In dem Leitfaden wurde nun ausführlich dargestellt welche Kosten auf eine nicht vorbereitete Organisation zukommen können, wenn es zu einem Cybersicherheitsvorfall kommt. Es soll nun aber auch auf die Kosten eingegangen werden, die auf eine Organisation zukommen, die sich auf dieses Ereignis vorbereiten will.

Die Vorbereitung auf einen Krisenfall kostet Geld, ist aber dennoch ein betriebswirtschaftliches Muss. Denn eine Gegenüberstellung von Krisenbewältigungsstrategien zeigt, dass die Kosten kontinuierlicher Vorsorge, die von lediglich reaktiven Notfallmaßnahmen ohne Vorsorge, auf mittlere und lange Frist überwiegen.

Konkret bedeutet das die Verletzung der Verfügbarkeit, Integrität und Vertraulichkeit betrieb-licher Daten und der betrieblichen ITK durch einen externen Angriff. Die rechtzeitige Zusammenstellung eines Kriseninterventions-Teams mit internen und externen Kräften/Dienstleistern, das Entwickeln von Notfall- und Wiederanlaufplänen und deren regelmäßige Erprobung können aber auch helfen, die betriebliche Aufbau- und Ablauforganisation zu optimieren sowie das Schadenspotenzial und damit Kosten zu senken.

Sichere IT-Infrastrukturen aufbauen und betreiben

- Redundanzen herstellen
- Business-Continuity-Management etablieren
- Robustheit der Sicherheitskonzepte prüfen
- IT-Trainings zur sicheren Bedienung der Anwendungen
- Krisenmanagement etablieren

Aufbau einer IT-sicherheitsaffinen Unternehmenskommunikation/-kultur

- Awareness schaffen
- Unterweisungen und Trainings,
- Einrichtung eines Backoffices für den internen Krisenmanager
- **ggf. zusätzliche Sach- und Personalkosten**

Beauftragung einer PR-Agentur zur Steuerung der Kommunikationswerkzeuge und -kanäle (Schaffung eines positiven Images lange vor Eintritt einer Krise)

- Soziale Netzwerke / Social Media (Facebook, Twitter, YouTube, Blogs, Web-Presseportale etc.)
- Presse (Printmedien)
- Sachkosten/Honorare

Abschluss Dienstleistungsvertrag z. B. mit einem Ausweichrechenzentrum

- Vorhaltung einer »gespiegelten IKT« zur Wahrung der betrieblichen Kontinuität
- Sachkosten

5 Fiktives Fallbeispiel: Die möglichen Kostenpositionen eines Cybervorfalls

Fallstudie:

APT Angriff mit CEO Fraud oder Susi Sorglos und der Scherbenhaufen.

Das deutsche Unternehmen xy produziert Pumpen, die in Spezialumgebungen arbeiten können und hat zum Ausbau der Markposition die Verbindung der Pumpen mit besonderer Sensorsteuerung forciert. Chinesische Pumpenhersteller können inzwischen vergleichbar belastbare Pumpensysteme zu günstigeren Preisen insbesondere in Schwellenländer liefern. Die Sensorsteuerung ist hingegen eine Weiterentwicklung und ermöglicht es die Wettbewerbsposition zu halten. Dadurch können die Pumpen über das Serviceportal der xy kommunizieren und Fernwartungen weltweit durchgeführt werden. Außerdem können Softwareupdates eingespielt werden. Dadurch sind die Pumpen in der Lage ihre Haltbarkeit zu erkennen und den anstehenden Austausch vor einem Ausfall durch Beschädigung anzukündigen. Sie können energiesparend auf die jeweiligen Anforderungen im Betrieb gesteuert werden und Spezial-betriebe können sich über die Plattform der xy zur Wartung der Geräte qualifizieren und direkt Wartungsaufträge annehmen. Die Sensorsteuerung erlaubt auch die Verbindung mit anderen Geräten der xy und die abgestimmte Smart-Steuerung eines Hydrauliksystems. Es ist so möglich im Pumpvorgang Schwellenwerte zu messen und durch die Systeme zu steuern, was die Qualitätskontrollen verbilligt.

Im Rahmen des Geschäftsabschlusses zu einem geförderten Entwicklungsprojektes in Tansania und der Modernisierung einer Schiffbetankungsanlage reist der Geschäftsführer mit einem Ingenieursteam nach Daressalam. Dies postet einer der Ingenieure auf der Facebook-Seite einer Bekannten, die ebenfalls nach Tansania fliegt.

Am ersten Tag der Abwesenheit bekommt das Office-Management der xy eine E-Mail, die eine Reisewarnung und Visabestimmungen zu Reisen für Geschäftsleute enthält und scheinbar von der tansanischen Botschaft in Deutschland und den Betreff der Geschäftsreise enthält. Diese wird an das Geschäftsführerbüro weitergeleitet und von Susi Soglos geöffnet. Darin ist ein Link enthalten, der eine Info-Seite mit den Gebieten enthalten soll, die für Reisen, aufgrund akuter Malariagefahr, gesperrt sein sollen. Susi Sorglos öffnet die Seite worauf hin sich eine Schadsoftware installiert. Die APT Attacke nimmt ihren Lauf und breitet sich im System aus. Innerhalb von zwei Tagen konnten die Pläne für die Geschäftsreise ausgelesen werden und auch andere Systeme infiziert werden.

Am dritten Tag erhält Susi Sorglos zunächst eine gefälschte E-Mail von einem der Entwicklungsingenieure, der ankündigt, dass ein Geschäftsabschluss in Aussicht steht und schon mal die Verträge vorbereitet werden sollten, weil eine tansanische Tochtergesellschaft gegründet werden soll, die das Projekt in Tansania durchführen muss. Am nächsten Tag kommt ein Anruf in schlechter Sprachqualität von der Mobilfunknummer des Geschäftsführers. Die Telefonnum-

mer wurde gefälscht (spoofing). Der vermeintliche Geschäftsführer verlangt die dringende Überweisung des Betrages von 500.000 Euro, um die Tochtergesellschaft gründen zu können. Es wird außerdem Druck ausgeübt und mit einem Verweis auf eine Abmahnung in der Personalakte gedroht. Susi leitet die Überweisung über die Buchhaltung ein.

Nach der Rückkehr der Reisenden fällt der Schwindel erst auf, als Susi Sorglos ihre Wut über den Geschäftsführer überwunden hatte und ihn auf das Geschäft anspricht. Daraufhin werden interne Ermittlungen eingeleitet. Schnell fällt auf, dass die Informationen nur durch eine Cyberattacke abgeflossen sein können. Es wird sich daraufhin die Frage gestellt, ob die Angreifer auch Zugang zum Plattformportal hatten oder sogar ein Softwareupdate der Pumpensteuerung beeinflussen konnten. Die Pumpensysteme sind sowohl in Wasserwerken als auch in Rettungsfahrzeugsystemen, Kühlhäusern und Großklimaanlagen verbaut.

Beispiele Geschätzter Kosten und Kostenpositionen aus der Fallstudie

Die Kostenschätzungen belaufen sich auf den Zeitraum von 2 Jahren, weil dies der Monitoring-Zeitraum der Bitkom Studie Wirtschaftsschutz: Datenklau, Spionage und Sabotage ist, in dem von betroffenen Unternehmen Zahlen angegeben wurden. Nach zwei Jahren lassen sich außerdem Kosten nicht mehr sinnvoll einem Cybersicherheitsvorfall zuordnen, sondern können als Vorsorgemaßnahmen betrachtet werden. Die Kosten sind bloße Schätzungen ohne Anspruch auf Richtigkeit und beruhen auf Studienangaben und Schätzungen von IT-Sicherheitsunternehmen, IT-Beratungsunternehmen und Versicherungsexperten, die mit der Bearbeitung derartiger Cybersicherheitsvorfälle ständig betraut sind. Die Reihenfolge der Kostenpositionen ist thematisch gewählt und besitzt keine Aussagekraft in Bezug auf Bedeutung, Wichtigkeit oder Chronologie eines Cybersicherheitsvorfalls.

Kostenposition	Beschreibung	Fiktive Kosten
Schaden für die Überweisung	Der Betrag, der überwiesen wurde, ist nur in seltenen Fällen vollständig zurückzuholen. Er wird in diesem Fall zunächst als Schaden zu beziffern sein. Der höchste so erbeutete Betrag belief sich bisher auf 12. Mio. €	500.000 €
Kosten für Produktivitätsausfall	Wenn die Produktionsplattform und die Software der Produkte betroffen sind, fällt bis zur Klärung die Lieferung neuer Produkte aus. Für geschätzte 2 Wochen sind dies bei 20 Mio. Jahresumsatz:	830.000 €
Kosten für Qualitätsbeeinträchtigungen bis hin zum Produktionsausfall	Für ausgelieferte Produkte, die durch ein Softwareupdate betroffen sein können, muss eventuell eine Rückruf- oder Patch-Kampagne gefahren werden.	200.000 €
Datensicherung des Fehlerfalls (Festplattendatenbestand inkl. Hauptspeicherzustand) zur Nachstellung in einer Testumgebung;	Hier müssen sämtliche Systeme des Unternehmens, die befallen sein können, berücksichtigt werden.	50.000 €
Fehlersuche und -behebung;	Die Malware muss identifiziert und beseitigt werden.	40.000 €
Externe IT-Forensik	Die Ermittlung eines komplexen Angriffs erfordert in der Regel externes Forensik Know-how, dass eingekauft werden muss. Dazu laufen Beraterhonorare auf.	100.000 €

Gegebenenfalls Neuinstallation des System und Aufsetzpunkt der letzten Datensicherung;	Hier müssen die betroffenen Systeme neu aufgesetzt werden, nachdem diese identifiziert wurden.	40.000 €
Einleitung eines Notbetriebsverfahren für Ersatzprozesse und Einberufung eines Notfallteams	In den betroffenen Bereichen muss das Unternehmen Mehrarbeit leisten und die Überstunden abgegolten werden.	50.000 €
Schwenk der IT-Systeme und Anwendungen auf einen Ausweichstandort u. a. mit zusätzlichem Personal	Auch während der Notfallphase muss sicher kommuniziert und müssen IT-Systeme benutzt werden. Diese müssen häufig angemietet werden.	20.000 €
Einnahmeausfälle, da kritische Anwendungen und IT-Systeme nicht zur Verfügung stehen sowie Kundenabwanderung bei Nichtverfügbarkeit von kritischen Prozessen und Anwendungen.	Durch den Angriff können nicht nur bestehende Verpflichtungen nicht mehr erfüllt werden, sondern auch Anfragen zurückgewiesen oder sogar ganz abgesagt werden, da die Lieferzeiten den Kunden zu lange dauern.	100.000 €
Sicherstellung des Mittelflusses für den laufenden Betrieb (einschließlich Mitarbeiterkosten, z. B. Überweisung der Gehälter) auch wenn dazu notwendige kritische Systeme (z. B. Lohnabrechnungssystem) ausgefallen sind.	Zusätzlich zur Miete der Drittsysteme müssen bestimmte Unterstützungsleistungen des Unternehmens zugekauft werden, weil intern Kapazitäten gebunden sind, sodass vermutlich Zeitarbeiter eingestellt werden müssen.	40.000 €
Strafen bei Beeinträchtigung vertraglich zugesicherter Service-Zeiten und -Verfügbarkeiten.	Für die Nichtlieferung oder den Ausfall der Pumpen können Vertragstrafen anfallen.	200.000 €
Externe Berater - Krisenstab	Durch die Unternehmenskrise fallen über einen langen Zeitraum Krisenberaterhonorare für die Kommunikationsprofis und Krisenstabsleiter oder Assistenten an.	100.000 €
Rechtsberatungskosten	Hier fallen für die Abschätzung der Vertragsbeziehungen, der Handlungspflichten und Haftungsrisiken, sowie Abwicklung der Prozesse Kosten für externe Anwälte und die Überstunden der eigenen Rechtsabteilung an.	630.000 €
Informationskosten	Das Unternehmen muss eventuell die Nutzer der Plattform über die Datenschutzrechtsverletzung informieren (§ 42a Satz 1 BDSG) und auch die Anleger über die Gewinnwarnungen (§ 15 WpHG).	40.000 €
Bußgelder	Durch die Verletzung von Datenschutzvorschriften in Bezug auf die Nutzerplattform können Bußgelder anfallen.	20.000 €
Verbesserung der IT-Strukturen	Im Nachgang und zur Krisenbewältigung gehört die Verbesserung der IT-Struktur. Dafür müssen externe Unternehmen beauftragt werden die IT-Sicherheitskonzepte erstellen, umsetzen und auditieren.	250.000 €
Schwachstellenanalyse und Schwachstellenbehebung	Nicht nur die IT-Sicherheit muss erhöht werden auch die Sicherheitsprozesse und Schulung im Unternehmen müssen verstärkt werden, damit ein Social-Engineering Angriff wie hier nicht erneut vorkommt.	100.000 €
Personalkosten für Sicherheitsexperten	Das Unternehmen muss qualifiziertes Personal auf dem Markt einkaufen und aufstocken. Auf 2 Jahre gesehen würden hier Kosten auflaufen.	250.000 €
Kosten für Werbung für die Produkte, die in Verruf geraten sein können oder für das Unternehmen und die Marken.	Im Rahmen der Reputationskosten sind erhöhte Kosten für Marketing angefallen, die das Unternehmen zuvor gar nicht hatte, weil es von seiner Reputation lebte.	120.000 €

Wertkorrekturen durch abfallen des Aktienkurses oder sogar eine dauerhafte Gefährdung der Indizierung in einem Aktienindex.	Als die Krise bekannt wird, verkaufen Anteilseigner ihre Anteile, weil sie befürchten, dass die Kosten der Krise sich auf den Wert niederschlagen	1.000.000 €
Niedrigere Umsatzzahlen durch Kundenrückgang erfordern Kundenbindungsprogramme.	Der Kundenrückgang, der bereits beziffert wurde, muss durch Bindungsprogramme, die die bestehenden Kunden halten sollen abgefedert werden.	100.000 €
Kosten für Markforschung.	Marketingkosten entstehen, um eine Aufarbeitung der Krise und Neuausrichtung der Marketingstrategie zu beziffern.	30.000 €
Kosten für Imagekampagnen und langfristige Imagestrategien.	Die Imagekampagne erfordert die Beratung einer spezialisierten Marketingagentur.	300.000 €
Notfall und Krisenkommunikation	Abgesehen von den obigen Kosten der Kommunikationsprofis entstehen im Krisen und Notfallmanagement weitere Kosten, wie eine Callcenter-Hotline, Hotel- und Verpflegungskosten.	90.000 €
Litigation und Vergleichskosten	Einige der Gerichtsverfahren müssen durch Vergleichsangebote abgeschlossen werden.	300.000 €
Rückstellungen für weitere Prozesskostenrisiken	Die Möglichkeit einer Verurteilung zu Schadensersatz muss durch Prozesskostenrückstellungen gedeckt werden.	1.000.000€
Preissteigerung in der Versicherungsprämie	Sofern das Risiko versichert ist, entfällt eine Summe auf die Zahlung der Versicherung. Diese führt aber zu langfristigen Preissteigerungen der Prämie.	200.000 €
Mitarbeiterbindungsprogramme	Nach Abschluss der Krise muss das Management den Beschäftigten für die Durchhaltephase danken und sie außerdem im Vertrauen auf die Zukunft stäken, um eine Abwanderung zu verhindern.	50.000 €
Mögliche Gesamtsumme		**6.625.000 €**

6 Ausblick

Die hier vorgestellten Schadensarten machen deutlich, wie unterschiedlich die Auswirkungen eines Cybersicherheitsvorfalls für Unternehmen sein können. Die tatsächlich bestehenden Risiken sind jedoch individuell und können im Rahmen dieses Leitfadens nicht oder nur unpräzise geschätzt werden. Dazu gehören unter anderem:

- Kosten für Know-how-Abfluss (Verlust von Alleinstellungsmerkmalen)
- Kundenverluste
- Auftragsstornierungen
- Aktienkurs
- Auswirkungen auf Leib und Leben
- Mitarbeiterfluktuation

Vor dem Hintergrund der in diesem Leitfaden skizzierten Herausforderungen, und im Sinne eines Risikomanagements, kann es für ein Unternehmen eine sinnvolle Entscheidung sein, bestehende Restrisiken abzusichern. Angebote mit entsprechender Versicherungspolice sind am Markt zwischenzeitlich verfügbar und runden das Konzept eines ganzheitlichen Sicherheitsmanagements ab.

Obwohl fast drei Viertel aller deutschen Unternehmen Angriffe auf ihre Computer und Datennetze durch Cyberkriminelle oder ausländische Geheimdienste als reale Gefahr sehen, haben sich bisher nur wenige Firmen gegen Cyber-Risiken versichert. Gut die Hälfte aller Unternehmen in Deutschland ist in den vergangenen zwei Jahren Opfer von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden (aktuellste Bitkom Studie). Die Unkenntnis über die vorhandenen Versicherungskonzepte oder die Sorge vor vermeintlich hohen Prämien können ein Gründe dafür sein.

Es gibt bereits mehr als ein Dutzend deutsche Versicherungsgesellschaften, die Absicherungslösungen gegen Schäden durch Cyberangriffe anbieten. Selbst der physische Datenverlust durch einfaches Liegenlassen oder durch den Klau einer Festplatte mit Firmendaten gilt dabei ebenso versichert wie das gehackte Firmenkonto oder die Betriebsunterbrechung durch Virenbefall. Zusätzlich bieten viele Versicherer Präventionsmaßnahmen und Krisenübungen an, damit ihre Kunden im Fall der Fälle vorbereitet sind.

Aber selbst wenn sich ein Unternehmen nicht gegen die aufgezeigten finanziellen Schäden absichern möchte, kann die vor Versicherungsvertragsschluss durchgeführte Prüfung einer Versicherungsgesellschaft über die Versicherbarkeit der Risiken durchaus Aufschluss über die Gefährdungslage bieten.

Cyber-Risk-Versicherungen bieten Schutz vor Risiken wie Hacking, Virenattacken, operative Fehler, Datenrechtsverletzungen sowie das Risiko, Dritte durch die Nutzung elektronischer Medien zu schädigen. Aber jede unternehmerische Tätigkeit muss sich auch bewusst machen. Kein Risiko lässt sich 100-prozentig ausschließen und nicht jedes Szenario versichern. Es lassen sich aber Lücken identifizieren und durch Methoden der Prävention, Detektion, Reaktion und Schadensminderung durch Versicherungen ein gutes Maß an Sicherheit verwirklichen.

Bitkom vertritt mehr als 2.300 Unternehmen der digitalen Wirtschaft, davon gut 1.500 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, 300 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 78 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 9 Prozent kommen aus Europa, 9 Prozent aus den USA und 4 Prozent aus anderen Regionen. Bitkom setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom