Cyberschäden: Das nicht-greifbare Risiko (Intangible Risk)

Hackerangriffe, Schadsoftware und Co. – alle Branchen betroffen

Sandra Dammalacks

Fast täglich verbreiten die Medien neue Hiobsbotschaften über Cyberangriffe in Deutschland und auf der ganzen Welt. Gegen Cyberattacken ist keine Branche, kein Wirtschaftszweig gefeit. Die Schäden sind vielfältig: Die Palette reicht von der gefälschten E-Mail, die zu einer Fehlüberweisung in Millionenhöhe führt, über den illegalen Zugriff auf Daten, der den Online-Handel stört oder fehlerhafte Kreditkarten-Abbuchungen zur Folge hat, bis hin zur gehackten Software, die eine Betriebsunterbrechung im Großlager erzwingt oder die Steuerung von Großgeräten zum Absturz bringt.

In jüngerer Zeit standen beispielsweise deutsche Krankenhäuser im Fokus, die Opfer so genannter Ransomware geworden waren. Durch das Öffnen von E-Mail-Anhängen waren erhebliche Teile des Datenbestandes inklusive ganzer Systemdateien verschlüsselt worden. Die betroffenen Krankenhäuser waren vielfach gezwungen, ihre gesamten IT-Systeme abzuschalten und auf Backups zurückzugreifen. Operationen mussten teilweise verschoben, Patienten konnten nicht aufgenommen werden.

Ein großes Stahlwerk beispielsweise verlor wegen einer mehrstufigen Cyberattacke einen seiner Hochöfen. Der Angriff verhinderte das Ausschalten des Ofens, sodass sich dieser in der Folge sukzessive selbst zerstörte. Dieser Schaden wird auf einen dreistelligen Millionenbetrag geschätzt.

Anders als typische Sachschäden mit klar erkenn- und bewertbaren Folgen, etwa nach einem Feuer, sind Cyberattacken vielfach nicht ad hoc greifbar. Zum Zeitpunkt, zu dem das Unternehmen erstmalig Kenntnis von einer möglichen Attacke erhält, etwa weil plötzlich der Zugriff auf wichtige Dateien gesperrt ist oder weil ein Erpresserschreiben eingeht, ist der Angriff schon voll im Gange, die Daten sind längst gehackt.

Nicht selten ist das Ausmaß des fremden Zugriffs zunächst ganz und gar nicht absehbar. Oft muss die betroffene Firma immense interne Kosten aufwenden und sich zudem die Unterstützung externer Fachleute holen, um die Störung zu ermitteln und zu beheben. Gerade mittelständische Unternehmen, die vielfach nicht über eigene IT-Abteilungen verfügen, sind auf solche Störungen oft nicht ausreichend vorbereitet.

Bedenkt man, dass allein durch den derzeit grassierenden Erpressungstrojaner *Locky* pro Stunde rund 5.000 Neuinfektionen ausgelöst werden, ist das Ausmaß des Gesamtschadens schwer vorstellbar. Eines Trojaners wie *Locky* Herr werden zu wollen, ist nach Einschätzung eines führenden Sicherheitsexperten praktisch aussichtslos, weil, ähnlich einem mutierenden Virus, mittlerweile mindestens 60 verschiedene Formen der Malware existierten.

Der wirtschaftliche Schaden durch Cyberangriffe pro Jahr liegt Schätzungen zufolge im Milliardenbereich. Betroffene Unternehmen sind mit unterschiedlichsten Mehrkosten konfrontiert: Zunächst sind da die Aufwendungen, die dem Eigenschadenbereich zuzurechnen sind. Dazu gehören z.B. Kosten für die Schadenbeseitigung und die Wiederherstellung der Daten sowie der technischen Verfügbarkeit des IT-Systems. Hinzu kommen Kosten, die entstehen, weil die betroffenen Dateninhaber und die Behörden informiert werden müssen.

Mitunter enorme Aufwendungen drohen dem Unternehmen zudem durch Ertragsausfall und laufende Kosten. Der Betriebsunterbrechungsschaden ist vielfach der größte Kostenposten nach einem cyberschadenbedingten Ausfall. Eine weitere Position können Lösegeldzahlungen sein, wenn nach Datenverlust Erpressung im Spiel ist.

Aber auch bei Drittschäden, also für die so genannte Haftpflichtkomponente bei Schadenersatzansprüchen und Rechtsverteidigungskosten, kann eine erhebliche Summe zusammenkommen und die Unternehmensbilanz gefährden. Zudem wollen externe Forensiker und Berater, die zwangläufig nach einem schwerwiegenden Cyberfall eingeschaltet werden müssen, bezahlt werden. Ein oft unterschätzter, aber nicht zu vernachlässigender Aspekt ist neben all dem der immaterielle Schaden, etwa bei Verlust der Reputation oder des Markenimages.

Der Zeitpunkt eines Cyberangriffs ist ebenso wenig vorherseh- und einschätzbar wie die Höhe der dadurch entstehenden Folgekosten. Der Vermögensschaden und die bilanziellen Auswirkungen für das betroffene Unternehmen sind, so dramatisch sie sein können, im Vorfeld aufgrund der Vielfältigkeit ihrer Ursachen nicht greifbar.

Sind Unternehmen darauf vorbereitet?

Laut der Umfrage eines führenden Industrieversicherers waren im Jahr 2014 rund 94 % der deutschen Unternehmen nicht gegen Cyberattacken versichert. Was speziell die mittelständischen Unternehmen in Deutschland betrifft, ergab die Studie einer namhaften Wirtschaftprüfungsgesellschaft, dass nur ein kleiner Teil von ihnen derzeit über gute Standards zur Informationssicherheit verfügt.

Nach Einführung des neuen IT-Sicherheitsgesetztes, das formal bis zum 13.Juni 2017 umgesetzt werden muss, ist allerdings zu erwarten, dass nicht nur die im Gesetz explizit erwähnten Betreiber kritischer Infrastrukturen, sondern auch viele andere Unternehmen sich inzwischen ernsthafter mit der Cyberthematik auseinandersetzen.

Das Management jedes Unternehmens muss, das ist unstreitig, sicherstellen, dass die eigene IT dem aktuellen Stand der Sicherheit und Technik entspricht. Dies bedeutet im Zweifelfall erhebliche Investitionen. Um z.B. historisch gewachsene IT-Infrastrukturen zu überprüfen, bieten sich IT-Schwachstellenanalysen und Stresstests an. Mittlerweile hat sich auf diesem Gebiet ein besonders spezialisierter Beratermarkt etabliert.

Die ersten Schritte: Risikoanalyse, Bewertung, Maßnahmenbestimmung

Um sich ein umfassendes Bild über das individuelle Risiko des Unternehmens zu machen, empfiehlt es sich, eine so genannte Risk Landscape-Analyse vorzunehmen. Hier werden alle Unternehmensaktivitäten im Netz und jeder Softwareeinsatz, sowohl für die eigene Produktion als auch für Fremdprodukte, dezidiert zusammengetragen und potenziellen Risikoszenarien wie Betriebsausfallschäden, Haftung gegenüber Dritten, Informationsverpflichtungen etc. gegenübergestellt.

Je nach Branche fällt das Risikopotenzial für Cyberattacken und deren Folgekosten sehr unterschiedlich aus. Das Risiko des Unternehmens, das Onlinehandel betreibt und seinen Produktverkauf über das Internet steuert, ist sicherlich anders zu bewerten als das Risiko des Lageristen, der die Produkte zwar softwaregesteuert, aber „physisch“ zu versenden hat. Bei Schäden ist jedenfalls mit erheblichen finanziellen Belastungen für das jeweilige Unternehmen zu rechnen.

Anhand einer Risk Landscape-Analyse erhält das Unternehmen zunächst eine Übersicht der vorhandenen unternehmensspezifischen Risiken sowie möglicher Angriffspunkte für Cyberattacken. Zugleich werden die finanziellen Folgen systematisch erfasst und bewertet. In der Folge kann das Unternehmen einen Maßnahmenkatalog erarbeiten, der z.B. die Modernisierung der eigenen IT, den Einkauf externer Beraterdienstleistungen oder die konkrete Erarbeitung klar definierter Krisen- und Kommunikationspläne beinhaltet.

Warum Cyberversicherungen?

Das Thema Versicherungen ist zwar nur ein kleiner Bestandteil des gesamten Maßnahmenkatalogs, als Schutz für potenzielle Bilanzschäden können passgenaue Absicherungsoptionen jedoch durchaus das i-Tüpfelchen auf dem ganzen Strauß der angedachten Maßnahmen sein.

Die üblichen Versicherungslösungen decken Cyberschäden oft nicht im wünschenswerten Umfang ab. Meist empfiehlt es sich, für Cyberrisiken separaten Schutz abzuschließen. Als erster Schritt ist es sinnvoll, die bereits vorhandenen Versicherungen zu überprüfen (z.B. die Betriebshaftpflicht-, Sach- und Betriebsunterbrechungsversicherung sowie, sofern vorhanden, sonstige Sonderdeckungen, etwa die Vertrauensschadenversicherung oder die Lösegeld- und Erpressungsversicherung).

Oftmals können bereits durch Umstellung der bestehenden Verträge auf neueste Bedingungen und Klauseln einzelne Cyberbausteine integriert werden, um zumindest einen kleinen Grundschutz zu erreichen. Nach Meinung von Experten ist es jedoch nicht damit getan, bereits vorhandene Unternehmensversicherungen um einzelne Cyberbausteine zu ergänzen. Zwar ist dies in der Regel die kostengünstigste Lösung, doch im konkreten Schadenfall erweist sie sich häufig als Flickenteppich, der Lücken lässt – und damit Potenzial für Diskussionen über nicht versicherte Sachverhalte und Kosten. Sehr

zu empfehlen ist ein ganzheitlicher Ansatz zur Absicherung der vielfältigen Risikoszenarien.

Welche Mehrwerte bieten Cyberversicherungen?

Im Vergleich zu den klassischen Sparten wurden Cyberversicherungen als ganzheitliche Erweiterung des Versicherungsschutzes konzipiert mit dem Ziel, maßgeschneiderte Produkte zur Absicherung der neuen Bedrohungslage vorhalten zu können. Grundsätzlich verfolgen diese Deckungen einen spartenübergreifenden und sachschadenunabhängigen Ansatz.

Insofern beinhalten die am Markt erhältlichen Angebote sowohl eine Eigen- als auch Drittschadenkomponente. Auch wird in vielen Bedingungswerken nicht mehr unterschieden, ob die Täter von extern oder von unternehmensintern agiert haben. Einen ganz wesentlichen Mehrwert bieten diese Versicherungen aber vor allem insofern, als die Kosten für externe Sachverständige, für Krisen- und Kommunikationsberater sowie für alle erforderlichen forensischen Untersuchungen automatisch mitversichert sind. Essenziell ist, dass die Deckung im Schadenfall Vorrang hat und dass die Diskussionen über etwaige Subsidiaritäts- oder Kumulklauseln, wie wir sie bei klassischen Verträgen häufig erleben, entfallen.

Im Kleingedruckten liegt der Unterschied

Im Gegensatz zum US-amerikanischen und zum Londoner Markt haben sich die ersten Cyberversicherungen in Deutschland erst sehr spät etabliert. Mittlerweile bieten knapp 15 Versicherer derartige Policen für den deutschen Markt an. Darüber hinaus besteht die Möglichkeit, englische Deckungen und Kapazitäten über den UK-Markt einzukaufen. Inhaltlich sind die angebotenen Bedingungen sehr unterschiedlich.

Um das passende Produkt für ein Unternehmen oder für eine bestimmte Branche aus dem Marktangebot herauszufiltern, ist es erforderlich, die Unterschiede zu erkennen – und zu bewerten. Dafür braucht es Expertise und Augenmaß. Eine individuelle Beratung und Anpassung der Bedingungen an das spezifische Unternehmensrisiko ist in der Regel geboten.

Nicht nur hinsichtlich der Definition des Versicherungsumfangs unterscheiden sich die Bedingungswerke oft erheblich, sondern auch im Kleingedruckten, z.B. wenn es um Nachmeldefristen bei Vertragsbeendigung geht (verfallbar/unverfallbar, 60 Tage/bis zu fünf Jahre).

Unterschiede, die bei Vertragsschluss zu beachten sind, gibt es des Weiteren bezüglich der Dauer der Rückwärtsversicherung. Auch die angebotenen Sublimite für einzelne Kostenbausteine oder die Höhe und Ausgestaltung der Selbstbehalte ist von Anbieter zu Anbieter verschieden. Manche Versicherer arbeiten neben einem festen bzw. prozentualen Selbstbehalt in Euro zusätzlich mit einem zeitlichen Selbstbehalt. Gerade in Standardangeboten ist der dafür angesetzte Zeitraum oft von so langer Dauer, dass eine Versicherungsleistung im Schadenfall kaum mehr zum Tragen kommt.

Auch bei den einzelnen Ausgestaltungen der Klauseln und den Ausschlusstatbeständen heißt es Obacht geben und gilt es zu prüfen, ob diese zum Problemfall werden können. In den Wordings finden sich z.B. oft erhebliche Unterschiede bei der Definition, ob es sich um einen zielgerichteten oder einen nicht zielgerichteten Angriff handelt. Dasselbe gilt für Schäden durch interne Täter oder durch Löschung bzw. Manipulation von Daten; ebenso bei Schäden durch Bedienungsfehler oder durch vorsätzliche Programm- oder Datenänderungen (z.B. durch Hacker). Hier gilt es u.a. zu prüfen, ob nur der veränderte Zustand der Daten versichert ist oder auch die daraus resultierenden Auswirkungen und Folgekosten.

Nicht zuletzt gibt es auch bei der Prämienhöhe erhebliche Abweichungen zwischen den einzelnen Anbietern. Preisunterschiede von bis zu 200 % sind möglich.

Wahl des richtigen Versicherers

In Anbetracht der großen Anzahl der Versicherer, die sich in jüngerer Zeit als Anbieter auf dem deutschen Markt für Cyberversicherungen etablieren wollten und wollen, ist es nicht einfach, die richtige Empfehlung abzugeben. Inhaltlich sollten dabei neben einem Vergleich der so genannten *hard facts* wie Prämien, Bedingungsunterschiede, Versicherungssummen und Selbstbehalte auch die *soft facts* Beachtung finden. Dabei sollten Aspekte eine Rolle spielen wie die Expertise des Versicherers bei der Schadenregulierung, das Vorhalten eigener Berater und Ingenieure, die Zusammenarbeit mit externen Beratern und Krisenmanagern oder auch die Internationalität.

Gerade bei schweren Risiken verlangen viele Versicherer nicht nur einen ausgefüllten Fragebogen, sondern zusätzlich einen persönlichen Risikodialog beim Kunden vor Ort. Einige stellen dafür hauseigene Experten, andere externe Dienstleister zur Verfügung.

Wie man sieht, differieren die Bedingungen und das Underwriting bei Cyberversicherungen bislang sehr stark, nicht zuletzt, weil es sich um ein noch sehr junges Versicherungsprodukt auf dem deutschen Markt handelt. Vor Abschluss einer Cyberversicherung sollte daher eine individuelle Beratung in Anspruch genommen und eine maßgeschneiderte Lösung gesucht werden. Wie diese im Einzelnen aussieht, ist u.a. abhängig vom spezifischen Unternehmensrisiko (Risk Landscape), von der Branche sowie von der Ausstattung der vorhandenen IT-Systeme.