ZKF-Verwaltungsmodernisierung

Absicherung vor finanziellen Schäden durch Cyberrisiken

Elmar *Sittner*, LL.M., Versicherungsberater, Leipzig

Es vergeht keine Woche, in der nicht mindestens eine Veranstaltung zum Thema von Cyberrisiken und/oder Cyberversicherung stattfindet. Die Fülle der Informationen ist selbst für Fachleute kaum noch zu bewältigen. Dennoch hat sich die deutsche Industrie erst zu einem geringen Teil dazu entschlossen, sich gegen derlei Gefahren zu versichern. Die öffentliche Hand hat sich mit diesem Risiko, zumindest aus dem Blickwinkel der Versicherbarkeit, überwiegend noch nicht befasst.

Selbstverständlich beschäftigt sich auch die öffentliche Hand schon seit Langem mit der Sicherheit des eigenen Netzwerkes und auch Städte, Kommunen und Landkreise verfügen in der Regel über EDV-Experten, die für die Netzwerk- und Datensicherheit verantwortlich sind. Ohne solche Maßnahmen wäre man Angriffen aus dem Netz auch schutzlos ausgeliefert und bekäme überhaupt keinen Versicherungsschutz. Der folgende Beitrag soll aber zeigen, dass die Gefahr durchaus real ist und dass es auch bereits Vorkommnisse gegeben hat, die besorgniserregend sind und die Kommunen sehr viel Geld kosten können.

1. Wie ist die Gefährdungslage einzuschätzen?

Alexander Geschonneck und Thomas Fritsche haben im September 2015 festgestellt, dass Deutschland fragwürdiger Spitzenreiter im Verhältnis der Schäden durch E-Crime gemessen an der Wirtschaftsleistung ist.[1)] Den Gesamtschaden veranschlagen die beiden Mitarbeiter der KPMG-Abteilung Forensik mit ca. 54 Mrd. €. Die Versicherer schätzen, dass sich lediglich etwa 10 % der deutschen Unternehmen gegen das Risiko eines Cyberangriff versichert haben. Bei der öffentlichen Hand liegt die Quote bei weniger als einem Prozent. Ob sich diese Situation seit September vergangenen Jahres deutlich geändert hat ist zweifelhaft.

Aus Sicht von Dr. Christopher Lohmann (CEO Zentraleuropa und Osteuropa der Allianz Global Corporate und Specialty SE) rangieren Cyber-Vorfälle im Jahr 2016 erstmals unter den drei größten Unternehmensrisiken weltweit.[2)]

Spektakuläre Vorfälle, wie sie sich z.B. bei Sony, bei TV 5, bei diversen Kreditkartengesellschaften, bei eBay und besonders medienwirksam auch beim Deutschen Bundestag ereignet haben, sind bei deutschen Kommunen und anderen Gebietskörperschaften noch nicht bekannt. Es hat aber schon eine ganze Anzahl von Datendiebstählen und Sabotagen gegeben, die zu erheblichen Schäden und auch zu Lösegeldzahlungen geführt haben.

Besondere Medienwirksamkeit erlangte aber im Februar 2016 das Neusser Lukaskrankenhaus, bei dem sämtliche erreichbaren Daten durch einen besonders resistenten IT-Schädling verschlüsselt worden sind. Dies führte zum weitgehenden Systemausfall, was wiederum zum Ausfall vieler Operationen führte. IT-Experten gehen von einer Gesamtschadenhöhe von mindestens 1 Mio. € aus.

Im Rahmen der aktuellen Diskussion, ausgelöst vom jüngsten spektakulären Ereignis bei Yahoo (Diebstahl von 500 Mio. Datensätzen!) schätzen Experten den jährlichen Gesamtschaden in Deutschland, verursacht durch Cyberkriminalität auf ca. 22 Mrd. €.

2. Risikomanagement als Voraussetzung für den Versicherungsschutz

Nicht der Abschluss einer Versicherung sollte am Anfang der Überlegung stehen, sondern zunächst einmal der Aufbau eines Cyber-Risikomanagementsystems. Dies beginnt regelmäßig damit, die individuellen Gefahrenquellen und Schwachstellen im eigenen Geschäftsbereich zu analysieren. Mitarbeiterdaten hat auch jede Gebietskörperschaft. Kundendaten sind in der Regel nicht vorhanden, aber doch eine große Menge vertraulicher personenbezogener Daten von Bürgerinnen und Bürgern. Daraus ergeben sich zahlreiche Verpflichtungen aus dem Bundesdatenschutzgesetz. Institutionen mit hohen Zahlungs- und Geldströmen sind hier regelmäßig höher gefährdet als geringer exponierte Risiken.

Auf Basis dieser Analyse wird anschließend eine Sicherheitsstrategie entwickelt. Diese Risikostrategie umfasst nicht nur technische Maßnahmen in der IT-Sicherheit und darf daher auch nicht allein in den Händen der IT-Abteilung liegen. Viele Angriffe werden erst durch die (meistens unbewusste) Beteiligung von Mitarbeitern möglich. Die Behördenleitung muss daher die Gesamtverantwortung übernehmen. Es geht hauptsächlich um die Vorsorge vor solchen Vorfällen, aber auch die Entwicklung einer Schadenminderungsstrategie, wenn der Fall eingetreten ist.

Es stellen sich folgende Fragen:

- Drohen nicht bei einer größeren Panne auch immer erhebliche Reputationsverluste?
- Wie geht man mit der Presse um und welche Maßnahmen zur Schadenminderung sind sofort einzuleiten?

Ein beliebtes Szenario ist z.B. das Verschlüsseln von kritischen Daten bei Cyber-Unternehmen, Versorgern und Behörden. Die Verschlüsselung wird durch die Hacker erst dann wieder aufgehoben, wenn ein entsprechendes Lösegeld gezahlt ist. Der Sicherheitsexperte Claudio Wolf bezeichnet das allgemein anzutreffende Sicherheitsniveau in Bezug auf dieses „Geschäftsmodell" als erschreckend.[3)] Ein Bonmot schon aus dem Jahr 2005 des damaligen FBI-Chefs Ro-

1) Geschonneck/Fritsche, Cyberversicherungen, iX – Magazin für personelle Informationstechnik 09/15, 40 ff.
2) Lohmann, Cyber: Die Feuerversicherung des 21. Jahrhunderts, Versicherungspraxis 4/2016, 8 ff.
3) Stuttgarter Nachrichten v. 30.8.2016. Wolf ist Leiter des Abwehrzentrums von Hewlett-Packard Enterprises.

bert Mueller lautet, dass es nur 2 Arten von Institutionen gebe: „Die Einen, die gehackt wurden und die Anderen die noch gehackt werden".

Wie das eigene Sicherheitsniveau organisatorisch und ggf. technisch verbesserbar ist, muss eine jede Institution für sich selbst (ggf. unter Einschaltung externer Fachleute) entscheiden und die Ergebnisse dann umsetzen.

3. Nur das Restrisiko versichern

Manche Branchenkenner bezeichnen die Cyberversicherung heute schon (möglicherweise etwas vorschnell) als die neue Feuerversicherung. Gleichwohl sollte man seine Risikolage vor einem Abschluss sorgfältig analysieren und zunächst das Sicherheitsniveau entsprechend erhöhen.

Wenn dies geschehen ist, liegen relativ günstige Voraussetzungen dafür vor, dass dann verbleibende Restrisiko mittels einer Cyberversicherung zu transferieren. Der Deutsche Cyberversicherungsmarkt entwickelt sich vielversprechend und die Kapazitäten sind auskömmlich, sodass auch ein deutlicher Wettbewerb entstanden ist.

Dabei ist erfreulicherweise festzustellen, dass der Wettbewerb nicht lediglich über die Prämienhöhe verläuft, sondern dass es auch einen erheblichen Bedingungswettbewerb gibt. Wie in anderen Versicherungsbereichen auch, ist dies mit der Schwierigkeit verbunden, dass aus der Vielzahl der Angebote mit jeweils unterschiedlichen Deckungskonzepten das für sich Günstigste herausgesucht werden muss. Vor diesem Hintergrund überrascht es nicht, dass es mittlerweile Spezialisten gibt, die sich nahezu ausschließlich mit diesem Themengebiet befassen.

4. Was deckt eine Cyberversicherung überhaupt?

Cyberversicherungen zeichnen sich durch einen spartenübergreifenden Ansatz aus, der sachschadenunabhängig ist. Es werden dabei gleichermaßen Eigen- wie auch Drittschäden versichert. Es spielt auch keine Rolle, ob der Täter aus dem eigenen Unternehmen kommt oder ob er sich von außen Zugang zu den Daten verschafft hat. Eigenschäden können z.B. durch Unterbrechung des eigenen Betriebes oder aber durch Mehrkosten z.B. für die Widerbeschaffung und Wiedereingabe von Daten entstehen. Schon Benachrichtigungskosten können, wenn z.B. Bürgerdaten gestohlen worden sind, leicht hohe sechsstellige Beträge erreichen. Zu dieser Benachrichtigung ist der Betroffene gesetzlich verpflichtet. Auch Mehrkosten für einen provisorischen Betrieb können schnell höhere Beträge erreichen. Schließlich kann man je nach Ausgestaltung der Police, auch so genannte Erpressungsgelder, die für die Entschlüsselung durch Schadsoftware verschlüsselter Daten gezahlt werden müssen (sofern man sich zur Zahlung entschlossen hat), versichern.

Auch eventuelle Schadenersatzansprüche Dritter sind im Rahmen der Cyberversicherung versicherbar (Drittschadendeckung). Bei Unternehmen ist also darauf zu achten, ob Kollisionen mit einer Betriebsunterbrechungsversicherung, mit einer Betriebs- oder Berufshaftpflichtversicherung oder einer Vertrauensschadendeckung entstehen bzw. welche Überschneidungen es vielleicht mit der Elektronikversicherung gibt.

Im Bereich der öffentlichen Verwaltung wird man keine Betriebsunterbrechungsversicherungen vorfinden, lediglich im Rahmen der Sachversicherung eventuelle Mehrkostenversicherungen, die allerdings immer an einen Sachschaden anknüpfen. Auch im Bereich der Elektronikversicherungen mag es an der einen oder anderen Stelle einmal eine Mitversicherung von Daten oder Softwareschäden geben. Auch diese setzt aber immer einen entschädigungspflichtigen Sachschaden voraus.

Ein ganz wichtiger Aspekt ist aber auch die Assistenzdeckung in einer Cyberpolice. Cyberpolicen heben nicht darauf ab, dass der Versicherer lediglich einen vom Kunden nachzuweisenden Schaden bezahlt, sondern die Cyberpolice garantiert eine sofortige Unterstützung des Kunden im Falle eines Cybervorfalles. Diese Unterstützungsleistungen, die als Baustein zur Verfügung stehen, sind auch unbedingt zu empfehlen. Es können dann IT-forensische Experten, Sachverständige, Juristen oder Kommunikations- und Krisenmanager hinzugekauft werden, die das Krisenmanagement gemeinsam mit den eigenen Fachleuten steuern und Schadenminderung betreiben.

5. Bedarf es eines speziellen Cyberversicherungskonzeptes für Kommunen?

Grundsätzlich wird sich die Cyberpolice für die öffentliche Hand, speziell vielleicht einer Kommune, nicht in ganz wesentlichen Bestandteilen von einer Cyberpolice eines Industrieunternehmens unterscheiden müssen. Die Abgrenzung zu vorhandenen Policen wird aber durch die Besonderheiten des kommunalen Versicherungskonzeptes anders aussehen als in einem Industrieunternehmen. Grund hierfür ist die spezielle Haftpflichtversicherung der kommunalen Gebietskörperschaften und die weitverbreitete kommunale Eigenschadenversicherung. Üblicher Haftpflicht-Versicherungsschutz von Unternehmen geht nicht so weit wie die Kommunaldeckung – insofern sind Einschränkungen der Drittschadenkomponente bei kommunalen Cyberpolicen durchaus möglich. Genau anschauen muss sich die Kommune die möglicherweise vorhandene Eigenschadenversicherung. Diese kann (muss aber nicht) eine Komponente zur Mitversicherung von Hacker-Schäden enthalten. Diese ist aber oftmals so gering limitiert (meistens sind noch nicht einmal 100 000 € versichert), dass sie keinen auskömmlichen Schutz vor solchen Schäden bietet.

Auch ist – anders als in einem Industrieunternehmen – nicht davon auszugehen, dass sogleich große Unterbrechungsschäden entstehen können, selbst wenn die kommunale Gebietskörperschaft einmal über einen bestimmten Zeitraum nicht auf ihre Daten zurückgreifen kann. Dies muss sich bei der Berechnung der notwendigen Versicherungsprämie ebenfalls auswirken.

6. Fazit

Als Fazit kann gezogen werden, dass auch Kommunen und andere Institutionen der öffentlichen Hand sich mit diesem Thema verstärkt auseinandersetzen sollten. Die Cyberversicherung kann aber nur das letzte Absicherungsglied in einer Kette von risikomindernden Maßnahmen sein. Wer jetzt schon auf ein gutes Sicherheitsniveau zurückgreifen kann, wird in der Regel auch gute Angebote erhalten. Ein Konzept muss aber auf den Bedarf und die Besonderheiten von Kommunen und anderen Gebietskörperschaften zugeschnitten sein.