versicherungs tip
Der unabhängige, exklusive Insider-Report für autonome Makler, kompetente Vermittler und integre Führungskräfte der Assekuranz

Spezial Beratung

Düsseldorf, 23.05.2017 34. Jahrgang Beilage zu Nr. 21/17

Aktuelle Entwicklungen bei Cyber-Versicherungen

– **Norbert Pischke**, Trainer und Produktmanager Sach/HUK der **Deutsche Makler Akademie (DMA)** –

Das **Bundesamt für Sicherheit in der Informationstechnik** (**BSI**) sieht in seinem letzten Lagebericht zur IT-Sicherheit in Deutschland vom Oktober 2016 eine neue Qualität der Gefährdung durch Cyber-Angriffe. Ursächlich hierfür ist die zunehmende Digitalisierung und Vernetzung wie sie durch Entwicklungen, wie z. B. Industrie 4.0 oder das Internet der Dinge, weiter vorangetrieben wird. Informationen auszuspähen sowie Geschäfts- und Verwaltungsprozesse zu sabotieren sind längst nicht mehr das einzige Ziel der Angreifer. Es sind inzwischen Geschäftsmodelle entstanden, mit denen sich Cyberkriminelle auf Kosten Dritter bereichern. So wird sogenannte Ransomsoftware genutzt, um die Daten am Computer zu verschlüsseln und dem Inhaber den Zugriff zu verwehren. Im Anschluss wird ein ‚Lösegeld' gefordert, um die Verschlüsselung aufzuheben.

Der Staat hat auf diese Bedrohungsszenarien inzwischen auch mit gesetzgeberischen Maßnahmen reagiert. Das seit Juli 2015 gültige **Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme** (**IT-Sicherheitsgesetz**) soll insbesondere die kritischen Infrastrukturen schützen. Betroffen sind hiervon Unternehmen u. a. aus den Bereichen Strom- und Wasserversorgung, Informationstechnik, Telekommunikation sowie Ernährung. Ziel ist es, Ausfälle oder Beeinträchtigungen der Versorgungsdienstleistungen zu verhindern oder zu minimieren und die Verfügbarkeit und Sicherheit der IT-Systeme zu erhalten. Betreiber kritischer Infrastrukturen (KRITIS) müssen alle zwei Jahre IT-Sicherheitsmaßnahmen nach dem Stand der Technik nachweisen. Angriffe auf ihre IT sind verpflichtend den Behörden zu melden.

1. IT-Sicherheit ist eine Aufgabe der Unternehmensführung

Die Sicherheit der IT-Systeme ist und bleibt eine dauerhafte Herausforderung. Sie gehört zum Risikomanagement und ist damit eine Führungsaufgabe des Unternehmers. Dies gilt nicht nur für die wichtigen Bereiche des wirtschaftlichen Lebens wie sie das IT-Sicherheitsgesetz benennt. Auch und gerade mittlere und kleinere Unternehmen nutzen verstärkt die Chancen der Digitalisierung und entsprechend das Internet. Sie setzen sich damit gleichzeitig den hiermit verbundenen Risiken aus und sind heute in der Pflicht, entsprechende Vorsorge im Bereich der Cyber-Sicherheit zu leisten. Nach einer repräsentativen **forsa**-Umfrage im Auftrag des **GDV** unter Entscheidern in kleinen und mittleren Unternehmen sehen 75 % der Befragten ein hohes Risiko von Cyber-Kriminalität für mittelständische Unternehmen. Für das eigene Unternehmen nehmen dies jedoch nur 36 % an. Ausreichend gegen Cyber-Kriminalität geschützt sehen sich 80 % der Befragten. Nur 63 % verschlüsseln aber z. B. sensible Daten und nur 64 % wollen in den nächsten zwei Jahren in weiteren Schutz gegen Cyber-Kriminalität investieren.

Wenn Hacker die Playstation von **Sony**, **Microsofts** Xbox oder sogar einen deutschen Hochofen lahm legen, erscheint dies offensichtlich nur kurzzeitig spektakulär. Die Bedrohung durch Cyberkriminelle ist aber längst real. Schon jedes vierte kleine mittelständische Unternehmen ist bereits Opfer eines erfolgreichen Angriffs geworden und hat dadurch einen wirtschaftlichen Schaden erlitten. Es kann schon reichen, wenn bei einem Betrieb Daten von Lieferanten und den besonderen Einkaufskonditionen gehackt werden. Handelt es sich bei den Daten um Kundeninformationen, wird der Schaden wohl ungleich größer sein.

2. Einhaltung von Mindeststandards der IT-Sicherheit sind zwingend

Der Unternehmer muss die Bedrohung durch Cyber wie jedes andere Risiko systematisch angehen und sich entsprechend absichern. Zunächst ist hier die organisatorische Ebene anzusprechen. Grundlage jeder

Impressum
markt intern Verlagsgruppe – **kapital-markt intern** Verlag GmbH, Grafenberger Allee 30, D-40237 Düsseldorf. Tel.: +49 (0)211 6698 199, Fax: +49 (0)211 6912 440. www.kmi-verlag.de. Geschäftsführer: Dipl.-Kfm. Uwe Kremer, Rechtsanwalt Gerrit Weber, Dipl.-Ing. Günter Weber. Gerichtsstand Düsseldorf. Handelsregister HRB 71651. Vervielfältigung nur mit Genehmigung des Verlages.

versicherungstip Herausgeber: Dipl.-Ing. Günter Weber. Redaktionsdirektoren: Dipl.-Kfm. Uwe Kremer, Rechtsanwalt Gerrit Weber. Chefredakteur: Dipl.-Ing. Dipl.-Oen. Erwin Hausen. Redaktionsbeirat: Christoph Morisse M.A., Rechtsanwalt Dr. Axel J. Prümm, Christian Prüßing M.A. Druck: Theodor Gruda, www.gruda.de. ISSN 0178-5699

Überlegung und Maßnahme ist der technische Schutz durch die Einhaltung von Mindeststandards bei der IT-Sicherheit. Besonders zu berücksichtigen ist der menschliche Faktor. Die gezielte Sensibilisierung und Qualifizierung der Mitarbeiter ist daher ebenfalls ein wichtiger Bestandteil eines Sicherheitskonzeptes. Schließlich ist für den Fall der Fälle ein Krisenreaktionsplan sinnvoll, der die erforderlichen Maßnahmen einschließlich der Eindämmung des möglichen Reputationsschadens regelt.

Ob man für die Analyse des Betriebes gleich sachverständige Beratung hinzuzieht, muss der Unternehmer selbst entscheiden. Die **VdS Schadenverhütung GmbH** bietet kostenlos und webbasiert einen sogenannten ‚Quick Check' an. Hierbei wird aus der Selbstauskunft auf 39 Fragen zu sicherheitsrelevanten Themen (Organisation, Technik, Prävention und Management) als Ergebnis eine Matrix zur Risikosituation im Unternehmen erstellt. Stimmen diese Grundvoraussetzungen, dann sollten auch kleine und mittlere Unternehmen mit einem zusätzlichen Versicherungsschutz das verbleibende Risiko abdecken.

3. Cyber-Versicherungen

Entsprechende Cyber-Versicherungen gibt es schon seit einiger Zeit. Neben den Deckungen von Erstversicherern sind inzwischen auch Makler mit eigenen Versicherungslösungen am Markt vertreten. Im April dieses Jahres hat der GDV mit den unverbindlichen Musterbedingungen für eine Cyberrisiko-Versicherung ebenfalls ein Deckungskonzept vorgelegt. Als Zielgruppe werden kleine und mittelständische Unternehmen bis zu einem Umsatz von 50 Mio. € und bis zu 249 Mitarbeitern definiert. Es muss sich hierbei um IT-Anwender handeln. Ausdrücklich nicht angesprochen werden Betriebe der kritischen Infrastruktur.

a) Gegenstand der Versicherung

Die Musterbedingungen sind dem Risiko entsprechend spartenübergreifend konzipiert und enthalten daher Elemente der Haftpflicht- und Sachversicherung, der Technischen Versicherung sowie der Vertrauensschadenversicherung. Versichert sind die infolge einer Verletzung der Informationssicherheit verursachten Vermögensschäden und bestimmte Kostenpositionen.

Als Verletzung gilt die Beeinträchtigung ● der Verfügbarkeit z.B. durch Löschen oder Verschlüsseln ● der Integrität z.B. durch Verändern und ● der Vertraulichkeit z. B. durch unrechtmäßige Kenntnisgabe von Daten oder informationsverarbeitenden Systemen.

b) Bausteine der Versicherung

Die unverbindlichen Musterbedingungen gliedern sich in zwei Teile: Teil A, welcher die konkreten Regelungen zur Ausgestaltung des Versicherungsschutzes, den Basisbaustein sowie die Bausteine für Service/Kosten, Drittschaden und Eigenschaden enthält. Teil B umfasst, wie nach der Neustrukturierung der Haftpflichtbedingungen üblich, den Allgemeinen Teil mit den Regelungen über allgemeine Rechte und Pflichten der Vertragsparteien.

In dem Basis-Baustein (A1) werden neben Definitionen der Versicherungsfall sowie Obliegenheiten vor Eintritt des Versicherungsfalls, insbesondere aber auch die generellen Ausschlüsse geregelt.

Der Service-/Kosten-Baustein (A2) regelt die versicherten Kostenpositionen vor und nach Eintritt des Versicherungsfalles. Die Leistung umfasst dabei mehr als bloße Geldzahlungen. Hier geht es insbesondere um Dienstleistungen wie die Analyse zur Ermittlung und Feststellung eines Schadens durch sogenannte IT-Forensiker und die Krisenkommunikation, um einen möglichen Imageschaden für das betroffene Unternehmen möglichst gering zu halten. Im Drittschaden-Baustein (A3) wird Deckung für die klassischen gesetzlichen Haftpflichtansprüche infolge einer Informationssicherheitsverletzung gewährt. Im Rahmen des Freistellungs- und Abwehranspruchs wird also der geschädigte Kunde entschädigt oder unberechtigte Forderungen abgewehrt. Der Eigenschaden-Baustein (A4) deckt zunächst die Kosten für die Betriebsunterbrechung im Rahmen eines vereinbarten Tagessatzes und die vereinbarte Haftzeit. Damit werden Unternehmen quasi für den entgangenen Gewinn entschädigt und können zugleich laufende Kosten begleichen. Weiter sind Kosten der Rekonstruktion und Wiederherstellung der Computersysteme versichert.

Es ist zu erwarten, dass die Veröffentlichung der Musterbedingungen dem Markt für Cyber-Versicherungen zusätzliche Impulse gibt. Weitere Versicherer werden in den Markt eintreten. Dies wird im Rahmen des Wettbewerbs erfahrungsgemäß für die Versicherungsnehmer positive Auswirkungen auf den angebotenen Deckungsumfang wie auch den Prämien haben. (Quelle für weitere Informationen zu Cyberschäden: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks)