

DATENSCHUTZ

KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Cybercrime

Praxisfall Cyberangriff – hätten Sie ihn erkannt?

Lars D. Preußner

Die Täter sind professioneller geworden

Interview mit Leopold Löschl

Cyber-Versicherung

Thomas Hubinger

Datenmissbrauch: Ernstfall und Vorbereitung

Rainer Knyrim, Clemens Foisner, Paul Prihoda

In Cybercrime verfangene Domains „einfangen“

Rainer Knyrim, Boris Tremel

Checkliste Datensicherheitsmaßnahmen

Hans-Jürgen Pollirer

Mit Standardvertragsklauseln in die Cloud

Rainer Knyrim

Gesetzesbeschwerde

Ernst M. Weiss

Thomas Hubinger
Hubinger & Hubinger KG

Cyber-Versicherung

Das unterschätzte Schutzpotential. Die Themen Datensicherheit aber auch Produktionsverluste durch Angriffe aus dem Cyberbereich sind oder sollten fester Bestandteil jedes Risikomanagements sein. Wobei sich (fast) automatisch die Frage nach der Versicherbarkeit der erkannten und bewerteten Cyber-Risiken stellt.

Mittlerweile gibt es am heimischen Versicherungsmarkt einige Anbieter von Versicherungslösungen aus dem Cyber-Risikobereich. Im Detail unterscheiden sich die einzelnen Angebote natürlich, aber hinsichtlich der angebotenen Deckungsbausteine lässt sich eine gemeinsame Linie erkennen.

Allen angebotenen Produkten ist gemein, dass es sich um gebündelte Versicherungsverträge handelt. Einerseits verspricht der Versicherer im Rahmen einer **Haftpflichtversicherung** Schutz bei Schadenersatzansprüchen Dritter. Andererseits sollen finanzielle Schäden des versicherten Unternehmens, sprich **Eigenschäden**, abgedeckt werden. Neben der vertragsabschließenden Gesellschaft sind deren Tochterunternehmen und alle Betriebsangehörigen versichert.

Nicht zu vergessen ist das Angebot aller Versicherer, eine „forensische Analyse“ der Netzwerkstrukturen durch spezialisierte Firmen durchführen zu lassen. Diese können telefonisch, aber auch Vor Ort erfolgen, münden aber jedenfalls in Vorschlägen für die Versicherungsnehmerin zur Verbesserung

ihrer Sicherheitsvorkehrungen. Bei einem Versicherer wird sogar ein fertiger Cyber-Notfallplan zur Verfügung gestellt.

Cyber-Bedrohung?

Dem Grunde nach geht es bei diesen Versicherungen um die Absicherung von Folgen durch Datenverlust bzw verschuldeten Datenmissbrauch. Zu denken ist hierbei an erfolgreiche **Hackerangriffe**, **Manipulation** von Kartenlesern, erfolgreiches **Phishing** oder Weiterleitung sensibler Daten durch **Fehlverhalten von Mitarbeitern**.

Auch Diebstahl bzw Verlust von Arbeitscomputern oder Zugangsdaten ermöglicht missbräuchliches und schädigendes Verhalten durch Kriminelle.

Neben einem Datenmissbrauch kann es aber auch durch **Denial-of-Service-Angriffe** oder gezielte Attacken auf das In-

tranet zur **Blockade des Unternehmens** kommen. Sei es, indem der Zugang auf die eigenen Daten gesperrt wird oder elektronisch gesteuerte Maschinen lahmgelegt werden. Möglicherweise bieten die Angreifer eine schnelle Aufhebung der Blockade bei Überweisung einer entsprechenden Lösegeldzahlung an. Soweit IT-Spezialisten nicht (schnell) helfen können, kann auch die Bezahlung der **Lösegeldforderung** in Betracht kommen.

Durch Manipulationen können **Fehlüberweisungen** aber auch **Fehllieferungen** aus dem Warensortiment provoziert werden.

Nicht zuletzt kann das EDV-Equipment des Unternehmens zur Schädigung Dritter, indem bspw eine **Virenattacke** gegen andere Unternehmen gestartet wird, missbraucht werden.

Haftpflichtversicherung

Bereits aus dem Begriff Cyber-Versicherung lässt sich erahnen, dass mit derartigen Verträgen keine Berufs- bzw Betriebshaftpflichtversicherung ersetzt werden kann. Vielmehr

handelt es sich um eine **Ergänzung** der klassischen Versicherungsdeckungen.

Vermögensschaden

Generell gilt, dass ausschließlich Vermögensschäden versichert sind, die weder auf Personenverletzungen noch auf Sachschäden zurückzuführen sind. Ausdrücklich als Vermögensschäden gelten der Verlust oder die Veränderung bzw. Nichtverfügbarkeit von elektronischen Daten Dritter.

- Bspw werden gestohlene Kreditkarteninformationen der Kunden für Einkäufe missbraucht. Betroffene Kreditkartenfirmen werden jedenfalls Schadenersatz fordern.
- Durch eine Sicherheitslücke im eigenen System wird ein „befreundetes“ Unternehmen Opfer einer Virusattacke. Die geschädigte Firma wird die Kosten zur Beseitigung der Schadsoftware zurückfordern.

Der Versicherer erfüllt entweder den Schadenersatzanspruch Geschädigter oder übernimmt die Kosten für die Abwehr bzw. den Abwehrversuch eines bloß vermeintlich bestehenden Anspruchs. Darüber hinaus wird auch die Übernahme von Verteidigungskosten einer etwaigen strafrechtlichen Verfolgung angeboten.

Versicherungsfall – Claims-Made-Prinzip

Als Versicherungsfall gilt die erstmalige Erhebung eines (vermeintlichen) Schadenersatzanspruches infolge einer Datenschutzrechtsverletzung oder anderen (Cyber-) Rechtsverletzung. Versicherungsschutz besteht für alle Rechtsverletzungen während der Laufzeit sowie für alle nicht bekannten Rechtsverletzungen vor Abschluss des Versicherungsvertrags.

Wissentliche Verletzung von Gesetzen oder Anweisungen der Auftraggeber ist nicht versichert.

Allein der **Zeitpunkt der Anspruchserhebung ist relevant**. Versicherungsschutz kann auch noch eine Zeitlang nach Vertragsende bestehen. Diesbezüglich wird von einer **Nachmeldedfrist**, die zwischen 60 Tagen und 5 Jahren angeboten wird, gesprochen.

Grenzen der Versicherbarkeit

Nicht jedes Fehlverhalten kann abgesichert werden. So sehen die Versicherungsbedin-

gungen vor, dass vorsätzliche Schadensverursachungen oder **wissentliche Verletzung von Gesetzen, Vorschriften oder Anweisungen der Auftraggeber** zum Verlust des Versicherungsschutzes führen. Vorteilhaft ist jedoch, dass der Versicherungsschutz erst, aber dann rückwirkend, entfällt, wenn diese Ausschlussstatbestände endgültig feststehen! Bis zur Feststellung trägt der Versicherer, quasi als Vorschuss, die Kosten.

Verletzungen von Kartell-, Wettbewerbs- oder Patentrechten oder Vertragshaftungen sind ebenso ausgeschlossen oder allenfalls nur eingeschränkt versicherbar!

Eigenschäden

Der Versicherungsschutz zur Deckung eigener Schäden beginnt immer mit der **Computer-Forensik**. Manchmal kann erst nach genauer Prüfung festgestellt werden, ob die vermutete Rechtsverletzung oder ein Hackerangriff vorliegen. Soweit die Vermutung begründet ist, die Prüfung allerdings ergibt, dass gar kein Versicherungsfall vorliegt, bieten manche Versicherer trotzdem eine Beteiligung an den entstandenen Kosten an. Diese Beteiligung ist immer der Höhe nach und oftmals quotenmäßig begrenzt.

Versicherungsfall

Als Versicherungsfall gilt der Eintritt eines Eigenschadens durch eine Datenschutzrechtsverletzung, durch einen Denial-of-Service-Angriff oder eine nicht autorisierte Nutzung, Vervielfältigung, Veränderung, Beschädigung, Zerstörung oder Diebstahl von Daten, die das versicherte Unternehmen elektronisch aufbewahrt.

Gedekte Kosten

Im Versicherungsfall können sehr unterschiedliche Kosten auf das versicherte Unternehmen zukommen:

- Kosten zur Wiederherstellung und Absicherung des eigenen EDV-Systems.
- Dazu gehören die Reparatur von Websites, Intranet, Netzwerkstrukturen sowie Programmen und Daten des betroffenen Unternehmens.
- Informationspflichten an betroffene Kunden oder Kreditüberwachungskosten zur Verhinderung eines zukünftigen Missbrauchs von Kundendaten.
- Etwaig besteht die Pflicht Behörden einzuschalten.
- Einem drohenden Imageschaden ist durch entsprechende Public-Relations Maßnahmen entgegenzuwirken.

Wichtig ist jedenfalls rasch professionelle Hilfe zu erhalten. Die Versicherer stellen daher den Kontakt über Notfallnummern zur Verfügung. Grundsätzlich werden alle mit dem Versicherer abgestimmten Kosten notwendiger Leistungen durch IT-Spezialisten sowie Rechts-, Krisenmanagement- und Public-Relations-Dienstleistungen gedeckt.

Darüber hinaus werden als Zusatzdeckungen noch weitere Kostenübernahmen angeboten.

- Ersatz von Ertragseinbußen bei erfolgreicher Betriebsstilllegung durch Blockierung der EDV samt Steuerungssystemen maschineller Anlagen können und sollten mitversichert werden.
- Die Bezahlung von Lösegeld – **nach Rücksprache mit dem Versicherer!** – kann (möglichst diskret, um kein Motiv zu schaffen) mitversichert werden.
- Die Kosten zur Aufklärung und Feststellung eines Spionageangriffs können abgedeckt werden. Ertragseinbußen durch den verlorenen Wettbewerbsvorteil werden aber nicht abgedeckt!
- Durch Passwortdiebstahl werden falsche Kontonummern hinterlegt. Die Manipulation wird meist erst Wochen später festgestellt. Die bis dahin fehlgeleiteten Geldbeträge sind dann bereits spurlos verschwunden. Bei entsprechender Vereinbarung tritt der Versicherer in den Schaden ein.

Versicherungssumme: besser großzügig bemessen!

Versicherungssumme

Grundsätzlich werden bei Cyber Versicherungen sowohl für den Haftpflicht- als auch Eigenschadenbereich Pauschalsummen vereinbart. Es gilt, dass der eingetretene Schaden maximal jedoch die vereinbarte Versicherungssumme vom Versicherer ersetzt wird.

Zu beachten ist jedoch, dass die vereinbarten Versicherungssummen für alle Schäden **pro Versicherungsfall oder Versicherungsjahr nur einmal zur Verfügung** stehen. Serienschäden werden nur als ein Versicherungsfall behandelt. Nicht zuletzt gibt es für die versicherten Personen keine Haftungsobergrenzen. Die Einschätzung der „richtigen“ Versicherungssumme sollte daher eher zu großzügig als zu restriktiv erfolgen.

PRAXISTIPP

Die angebotenen Lösungen stellen eine gute Möglichkeit zur Risikobegrenzung durch Versicherungsschutz dar. Den „besten“ Anbieter gibt es je-

doch nicht. Einerseits hängen die Angebote von Größe und Tätigkeit des zu versichernden Unternehmens ab. Andererseits hat jeder Versicherer seinen speziell „guten“ Baustein. Womit

das beste Preis-Leistungs-Verhältnis auch von der Risikobewertung des CEO abhängt.

Dako 2016/19

Zum Thema

Über den Autor

Thomas Hubinger ist Versicherungsmakler und Geschäftsführer der Hubinger & Hubinger KG.
E-Mail: Thomas.Hubinger@versicherungsmakler-hubinger.at, Internet: www.hubinger.at

Versicherungsbedingungen

- AIG – American International Group, Inc: Cyber Edge 2.0 Vermögensschadenversicherung (2014)
- Allianz Global Corporate & Specialty AG: Cyber Protect Versicherungsbedingungen (VB) zur Versicherung von Datenschutzverletzungen und Risiken der Informationstechnologie (2015)
- HDI Versicherung AG: Cyber+ Bedingungen zur Cyber Versicherung (2013)
- Hiscox Insurance Company Ltd: Cyber Risk Management by Hiscox – Bedingungen 2/2015 für Österreich (2015)