

- aus assekuranz und allfinanz
- informationen montags und donnerstags

Konzepte und Kriterien

Cybercrime – reichen die Haftpflicht-Konzepte aus?

27. Januar 2014 - „Cybercrime, das unterschätzte Emerging Risk“ - treffender konnte das Thema für Experten und Besucher der 16. Euroforum-Jahrestagung Haftpflicht nicht sein. Ein Diskussionspunkt: Sind neue Lösungen für Produkthaftpflicht und Cyber-Risiken nötig und möglich?

Cyber-Sicherheit gehört mittlerweile zu einem der wichtigsten Themen überhaupt. Fast täglich eine Hiobsbotschaft für die nicht mehr zu überschauende Menge der Computerbesitzer und User des World-Wide-Web. So ist es noch gar nicht lange her, dass hierzulande rund 20.000 Nutzer der Website „Redtube.com“ eine Abmahnung bekamen, weil sie vermeintlich urheberrechtlich geschützte Sexfilme auf der amerikanischen Website Redtube.com abgerufen haben sollen. Und der Abhörskandal rund um den amerikanischen Geheimdienst NSA ist auch noch längst nicht ausgestanden. Seit dem Wochenende soll nämlich feststehen, dass die NSA durch das Abhören des Handys der Bundeskanzlerin offenbar eine zwischenstaatliche Vereinbarung zwischen den USA und Deutschland gebrochen haben soll. Wie sehr die Cyber-Kriminalität zugenommen hat, zeigen erste jetzt verfügbare Statistiken der aus dem Jahr 2012. Die Polizei musste da insgesamt mehr als 64.000 Cyber-Straftaten ahnden. Der Diplomphysiker **Dietrich Winter (Foto: E. Bocquel)**, der als ausgewiesener Fachmann für IT-Themen sowie Umwelt/USV und Emerging Risks gilt, stellte die alle bewegende Frage: „IT-Dienstleister - sind neue Lösungen für Produkthaftpflicht und Cyber-Risiken nötig und möglich?



Seit August 2013 gehört er dem Experten-Team der Allcura Versicherungs-Aktiengesellschaft (www.allcura-versicherung.de) und der angeschlossenen Allcura Fachakademie an. In seinem Vortrag bei der 16. Euroforum-Jahrestagung Haftpflicht (www.euroforum.de) ließ Winter kurz die kommenden Entwicklungen im technischen Umfeld, das so stark durch die IT geprägt wird, Revue passieren. Konzepte gebe es viele. Die rasante Entwicklung in der Vergangenheit zeichne die Schnelligkeit auf, in der Künftiges real werde.

Flächendeckender Einzug der Informations- und Kommunikationstechnik

Winter sprach von der „Industrie 4.0“, was so viel bedeutet wie „Internet der Dinge, Dienste und Daten = Internet of Everything“. Die Verknüpfung „aller“ Dinge mit dem Menschen. „Es erwartet uns ein flächendeckender Einzug von Informations- und Kommunikationstechnik sowie deren Vernetzung“, sagte der Spezialist, der unter anderem in verschiedenen Arbeitsgruppen des GDV Gesamtverband der Versicherer (www.gdv.de) an der Entwicklung der GDV-Musterempfehlung für IT-Softwarehäuser, IT-Dienstleister und IT-Nutzer sowie an einem GDV-Grundsatzpapier zu rechtlichen und technischen Aspekten von IT-Schäden mitgearbeitet hat.

Das **Internet der Dinge, Dienste und Daten** ermögliche sicherlich bald, das im Haushalt von Jedermann bald ein Kühlschrank steht, der „wie von selbst“ ermittelt, wenn bestimmte, von vornherein ausgewählte Produkte nicht mehr verfügbar sind und dann das Fehlende „selbständig“ bestellt. Im Gesundheitsbereich werden demnach auch dauerhafte Messung von Parametern (Blutdruck,-zucker, Herzfrequenz) mit automatischer Information an Arzt und Betreuung per Telefon/Internet bei Abweichungen möglich, die im Ernstfall „automatisch“ den Rettungsdienst alarmieren. Im Rettungswagen könnten dann so viele spezielle Daten durch Sensortechnik erhoben werden, dass die Fahrt im am besten geeigneten Krankenhaus endet, in dem zeitnah schon spezielle medizinische Vorbereitungen für diesen Patienten getroffen werden können.



Großes Potenzial für und durch IT-Störungen

So angenehm diese Gedanken seien, so groß sei das Potenzial für IT-Störungen, die größtenteils auf den Hersteller zurückfallen. Das habe die Industrie bereits verstanden, sagte Winter. Einer Umfrage zufolge will demnach jedes dritte Unternehmen hierzulande die Sicherheit seiner IT-Systeme überprüfen. Danach würden 15 Prozent auch mit dem Gedanken einer Umstellung

auf einen europäischen IT-Dienstleister spielen, um sich vor dem Zugriff amerikanischer und britischer Dienste zu schützen.

Skeptisch beurteilen die Manager, die Auslagerung von Firmendaten im Internet, so Winter. Denn 54 Prozent würden im sogenannten Cloud Computing ein erhöhtes Sicherheitsrisiko für ihre Daten sehen. „Vor den NSA-Enthüllungen hatten nur ein Drittel der Befragten diese Bedenken“, ließ Dietrich Winter einfließen.

Bei der Bestandsaufnahme, welche Risiken bisher Internet-Dienstleister absichern, nannte Dietrich Winter die „traditionelle“ Haftpflicht-Versicherung die entsprechend greife bei:

- **Störungsrisiko:** Störung des Zugangs zu Netzwerken, Servern, Diensten;
- **Sicherheitsrisiko:** mangelhafte Sicherheit von erstellter, implementierter Soft- und Hardware insbes. hinsichtlich Hackerangriff und Virenbefall;
- **Medien-Risiko:** Verbreitung falscher oder rechtswidriger Inhalte.

Kommen die Hauptrisiken der Informationsverarbeitung hinzu, wobei der Referent die Inhalte des Begriffs SECURITY und ihre Angriffe wie folgt auf den Punkt brachte:

- **(Distributed) - Denial Of Service - Attacks**
- **Datenmanipulierung** (Hacking)
- **Datendiebstahl** (Data-Highjacking)
- **Social Engineering** - auch automatisch durch Scareware/Rogueware (Vorspiegelung von Schadprogrammen mit vermeintlicher Säuberungssoftware gegen Geld)
- **Datenspionage** (Sniffing)
- **Vortäuschen falscher Identität** (Spoofing, Faking).

Der Allcura-Versicherungs-Manager Winter hinterfragte dann unter anderem, was hat sich unlängst in Sachen Meldepflichten diesbezüglich verändert habe. Er sprach von der Verschärfung der **Selbstanzeigepflicht** innerhalb von 24 Stunden. Bei Verstößen gegen den Datenschutz ist seinen Angaben zufolge seit dem 25. August 2013 eine neue EU-Vorschrift (Verordnung 611/2013) zur Meldefrist bei „Datenlecks“ in Kraft getreten. Bisher verpflichtete das BDSG Bundes-Datenschutz-Gesetz alle Diensteanbieter nach einer „Datenpanne“ unverzüglich die Betroffenen und die Behörden zu informieren. Im Paragraphen (§) 42 a BDSG gilt dies bußgeldbewehrt bis zu 300.000 Euro.

Jetzt fordere die Vorschrift von Telekombetreibern und Internet-Providern eine Meldepflicht bei Datenpannen und „Datendiebstahl“ innerhalb einer 24-stündigen Frist an die zuständige Behörde. Insgesamt bedeutet das den Angaben zufolge, dass Unternehmen Diebstahl, Verlust oder unbefugten Zugriff auf persönliche Daten ihrer Kunden melden müssen. Dies beinhaltet unter anderem Finanzdaten, Standortdaten, E-Mail-Dateien, Verbindungsdaten und IP-Adressen.

Dietrich Winter nannte die bekannten Konzepte, die auf GDV-Ebene für die deutsche Versicherungswirtschaft und die Haftungs-Risiken der Internet-Kommunikation erarbeitet wurden (*er hatte an Vielem selbst mitgearbeitet*).

- **2001:** unverbindliche Musterbedingungen des GDV für Softwarehäuser;
- **2002:** unverbindliche Musterbedingungen für IT- Dienstleister (+ Provider + ASP) und erstmals Schutz für Personen-, Sach- und unbegrenzte „offene“ reine Vermögensschäden in einem Haftpflichtkonzept;
- **2004/5:** unverbindliche Musterbedingungen für Nutzer der Informationstechnologie und erstmals Schutz für Schäden infolge von Datenlöschung, Betriebsunterbrechung, Sach- und Personenschäden durch Übertragung von Schadprogrammen sowie Persönlichkeits- und Namensrechts-Verletzungen per Internet.

„Ist eine Trennung zwischen Vermögensschäden und Sachschäden noch opportun?“ fragte Dietrich Winter auch das Plenum während der Euroforum-Veranstaltung. Als Eckpunkte der Struktur der IT-Dienstleister Markt Konzepte nannte er IT-Dienstleister-Konzepte, bei denen überwiegend in die allgemeine Haftpflicht mit Versicherungsfall beim Schadenereignis zum Tragen komme. Des weiteren gibt es laut Dietrich Winter vereinzelt Konzepte in der Vermögensschaden-Haftpflicht, wo der Versicherungsfall „Verstoß“ abgedeckt ist. Schließlich gebe es mehrere Varianten, wie Datenlöschschäden der Daten behandelt werde: zum einen wie Sachschäden (Sublimit für Tätigkeitsschäden?); zum anderen wie Vermögensschäden; und dann bleibe ein Rest, bei dem man unsicher, wie das versicherungstechnisch gehandhabt werden solle.



Abschließend verwies Dietrich Winter auf die neue Police „IT-Schutzschirm Plus“, die von der Allcura Versicherungs-AG im September 2013 auf den Markt gebracht wurde (["Neuer IT-Schutzschirm mit besonders vielen Facetten"](#)). Dabei handelt es sich Winters Aussagen zufolge um eine kombinierte Berufs-, Betriebs-, Produkt- und Umwelthaftpflicht-Versicherung für Unternehmen sowie Freelancer der IT- und Telekommunikations-Branche.

Nach Sachlage der Dinge stelle sich weiter die Frage, ob die offene Vermögensschadendeckung für IT-Dienstleister Elemente der Cyberrisk-

Deckung beinhalte, oder ob erweiterte Lösungen nötig seien? Ein Beispiel dazu: Durch eine Pflichtverletzung eines IT-Dienstleisters verlieren gesammelte Kunden-Daten eines Auftraggebers ihre Vertraulichkeit („Datenklau“).

Alle Haftpflichtansprüche, die

- gegen seinen Auftraggeber von den „Daten-Eigentümern“ erhoben werden und die
- der Auftraggeber gegen den IT-Dienstleister erhebt,

sind laut Winter beim IT-Dienstleister versichert, bis hin zur „Forensischen Detailanalyse“, wenn damit seine Pflichtverletzung aufgeklärt werden kann. Mit der Police „IT-Schutzschirm Plus“ der Allcura, die in dieser Form bisher hierzulande noch von keinen weiteren Anbieter entwickelt wurde, sei man breit aufgestellt. Man arbeitete an weiteren Lösungen. (-el / www.bocquel-news.de)

[zurück](#)

Achtung Copyright: Die Inhalte von bocquel-news.de sind nach dem Urheberrecht für journalistische Texte geschützt. Die Artikel sind ausschließlich zur persönlichen Lektüre und Information bestimmt. Abdrucke und Weiterverwendung - beispielsweise zum kommerziellen Gebrauch auf einer anderen Homepage/Website oder Druckstücken - sind nur nach persönlicher Rücksprache mit der Redaktion (info@bocquel-news.de) gestattet.

[Artikel drucken](#) | [Artikel weiterempfehlen](#)

weitere Alternative:
IT- Schutzschirm Plus Allcura Versicherungs AG

eigene VSU für Schäden, ohne Unterscheidung in •Vermögens-, •Datenlösch-, •Sach- oder •Personenschäden aus IT-spezifischen Tätigkeiten / Risiken	+	eine pauschale VSU für sonstige Risiken = BHV + Umwelthaftpflicht- + Umweltschadensversicherung (öffentlich-rechtl. Ansprüche) für P+S mindestens 3 Mio. EUR
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------