



# Der Begriff der „Informationssicherheitsverletzung“ in der Cyberversicherung

10.06.2020

**Cyberrisiken treten immer mehr ins Bewusstsein von Unternehmen. Dazu zählen Cyberattacken krimineller Art wie auch Cyberrisiken durch menschliches oder technisches Versagen, Fehlfunktionen und höhere Gewalt. Insbesondere Cyberattacken stehen auch in Österreich an der Tagesordnung und stellen seit mehreren Jahren eines der größten, schwer bewältigbaren Betriebsrisiken für Unternehmen dar. Die Nachfrage nach Cyberversicherungen nimmt stetig zu.**

Der Cyberversicherungsmarkt der Gegenwart ist hochgradig zersplittert und durch hohe Inkonsistenz sowie Intransparenz geprägt. In den wesentlichen Regelungsbereichen, wie der Wahl der Versicherungsfalldefinition, der Art der Beschreibung versicherter Gefahren, dem Versicherungsumfang, der Bezeichnung und Anzahl wählbarer Risikobausteine, der Risikoausschlüsse und vor allem der gefahrrelevanten Obliegenheiten iSd § 6 Abs 2 VersVG weisen die bestehenden Cyberversicherungen weitreichende Unterschiede auf. Diese gravierenden Unterschiede erschweren schon allein in regelungstechnischer Art einen Vergleich marktgängiger Versicherungsprodukte.<sup>1</sup>

<sup>1</sup> Kath, ZVers 3/2019, Die Cyberversicherung Überblick über ein neues Versicherungsprodukt (2019) S 30f.



**AUTOR**  
**Julia Loisl**  
**Rechtsanwaltsanwärterin**  
**T +43 1 512 03 53**  
[julia.loisl@vhm-law.at](mailto:julia.loisl@vhm-law.at)

Julia Loisl ist  
Rechtsanwaltsanwärterin bei  
VHM Rechtsanwälte.

Ihre Schwerpunkte sind  
Dispute Resolution und  
Versicherungsrecht.

*Schlagworte: Cybergefahren,  
Cyberversicherung,  
Elektronische Daten,  
Informationssicherheits-  
verletzung,  
Informationsverarbeitende  
Systeme.*

**Vavrovsky Heine Marth**  
**Rechtsanwälte GmbH**

Wien – Salzburg

Fleischmarkt 1  
1010 Wien, Österreich  
T +43 1 512 0353  
F +43 1 512 0353 – 40  
[office.wien@vhm-law.at](mailto:office.wien@vhm-law.at)

[www.vhm-law.at](http://www.vhm-law.at)



Allen angebotenen Cyberversicherungs-Produkten ist gemein, dass es sich um gebündelte Versicherungsverträge handelt.

Im Rahmen einer **Haftpflichtversicherung** wird Schutz für Schadenersatzansprüche Dritter gewährt. Als Versicherungsfall kommt hier die Verletzung von Datenschutzgesetzen, von gesetzlichen bzw vertraglichen Geheimhaltungspflichten und von Persönlichkeitsrechten in Frage. Auch die Weiterleitung von Schadsoftware an Dritte und ein vom IT-System des Versicherungsnehmers ausgehender DoS-Angriff sind versichert.

Zum anderen sollen **Eigenschäden** – also finanzielle Schäden des versicherten Unternehmens – abgedeckt werden. Im Bereich der Eigenschäden sind Risiken wie die unrechtmäßige Offenlegung, Beschädigung, Zerstörung, Veränderung, Blockierung oder den Missbrauch der elektronischen Daten und IT-Systeme aufgrund eines Hackerangriffs, einer DoS-Attacke oder der Infektion des IT-Systems durch Schadsoftware bzw auch bereits die Androhung einer der genannten Angriffsszenarien, erfasst. Manche Versicherer beziehen in die Definition des versicherten Risikos auch Datenschutzverletzungen mit ein, unabhängig davon ob eines der angeführten Angriffsszenarien vorliegt.<sup>2</sup>

## Die Definition des Cyberrisikos in den ABC 2018

Unter den Allgemeinen Bedingungen für die Cyberrisiko-Versicherung („**ABC 2018**“) besteht Versicherungsschutz für reine Vermögensschäden, die durch eine sog "**Informationssicherheitsverletzung**" verursacht werden.

Versicherer-Wordings knüpfen demgegenüber an den Eintritt eines im jeweiligen Bedingungswerk näher definierten "Cyberangriffs", "Cyberschadens", "Cyberevents" oder einer "Netzwerk-sicherheitsverletzung" an.<sup>3</sup> Eine hinsichtlich ihres Bedeutungsumfangs und ihrer Reichweite führende Terminologie hat sich bislang noch nicht durchgesetzt.<sup>4</sup>

Der Definition der *Informationssicherheitsverletzung* kommt die wichtige Bedeutung zu, dass das im allgemeinen Sprachgebrauch schwer fassbare und ziemlich konturlose Cyberrisiko in rechtlich eindeutige Bahnen zu lenken. Das in den *ABC 2018* mit dem Begriff der Informationssicherheitsverletzung definierte Cyberrisiko beinhaltet nicht bloß Konstellationen der Cyberkriminalität, sondern auch Cyberrisiken nicht krimineller Art. Umgekehrt darf aber auch nicht angenommen werden, dass sämtliche Cybergefahren von diesem Begriff erfasst wären.<sup>5</sup>

<sup>2</sup> Keltner in Berisha/Gisch/Koban (Hrsg), Haftpflicht-, Rechtsschutz- und Cyberversicherung (2018) S 112.

<sup>3</sup> Auch die deutschen AVB Cyber des Gesamtverbandes der Deutschen Versicherungswirtschaft aus 2017 knüpfen an der Terminologie Informationssicherheitsverletzung und seiner darin vorgenommenen Definition an.

<sup>4</sup> Malek/Schütz, Cyberversicherung: Rechtliche und praktische Herausforderungen (2019) S 422.

<sup>5</sup> Kath, ZVers 3/2019, Die Cyberversicherung Überblick über ein neues Versicherungsprodukt (2019) S 13.



Im Folgenden soll auf die in den *ABC 2018* verwendete Definition des Cyberrisikos der sogenannten „*Informationssicherheitsverletzung*“ näher eingegangen werden.

### **Informationssicherheitsverletzung**

Die *ABC 2018* definieren in Art 1.2.1. die Informationssicherheitsverletzung als „*eine Beeinträchtigung der Verfügbarkeit, Integrität, Vertraulichkeit von elektronischen, vom Versicherungsnehmer verarbeiteten Daten oder von informationsverarbeitenden Systemen, die der Versicherungsnehmer zur Ausübung seiner betrieblichen oder beruflichen Tätigkeit nutzt*“.

Der Begriff der „*Datenverarbeitung*“ definiert sich nach Art 4 Z 2 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung). Außerdem wird in Ziff 2.1. *ABC 2018* festgelegt, dass der Begriff „*elektronische Daten*“ auch Software und Programme umfasst.

Man bedient sich damit einer generell abstrakten Definition zur Umschreibung des versicherten Cyberangriffs, während andere Bedingungswerke vorrangig auf abschließend und konkret aufgelistete Angriffsszenarien zurückgreifen.<sup>6</sup>

Als unmittelbare Konsequenz dieser Definition ergibt sich, dass die Beeinträchtigung anderer als elektronischer Daten, ebenso wenig wie jene privat genutzter elektronischer Daten,

geschützt ist. Was bei gemischter Nutzung bestimmter Daten (teils privat, teils betrieblich bzw beruflich) gelten soll, lassen die *ABC 2018* offen. Hier ist anzunehmen, dass dies zulasten des Versicherungsunternehmens ausschlagen wird.

Geschützt ist auch die Beeinträchtigung der Verfügbarkeit, Integrität oder Vertraulichkeit „*informationsverarbeitender Systeme*“, die der Versicherungsnehmer zur Ausübung seiner betrieblichen bzw beruflichen Tätigkeit nutzt. Hierbei kommt es nicht darauf an, ob sich diese Systeme im Eigentum bzw in der unmittelbaren Verfügungsmacht des Versicherungsnehmers oder in dessen Betrieb befinden. Auch Systeme externer Dienstleister, deren sich der Versicherungsnehmer bedient, kommen in Betracht. Freilich wird dieser solcherart weite Versicherungsschutz dann an anderer Stelle wieder eingeschränkt.

Die „*Verfügbarkeit*“ von Daten oder eines informationsverarbeitenden Systems beschreibt das Vorhandensein funktionierender Zugriffs- und Nutzungsoptionen. Bei der „*Integrität*“ geht es dagegen um die Nachvollziehbarkeit von Daten- oder Systemänderungen; es darf nicht möglich sein, Daten unbemerkt zu ändern. Der Grundwert der „*Vertraulichkeit*“ stellt den Fokus auf die Berechtigung. Daten dürfen nur von den dazu berechtigten Personen gelesen und verarbeitet werden.<sup>7</sup> Eine Informationssicherheitsverletzung im Sinne der Bedingungen ist bereits bei der

<sup>6</sup> *Malek/Schütz*, Cyberversicherung: Rechtliche und praktische Herausforderungen (2019) S 422.

<sup>7</sup> Bei den verwendeten Begrifflichkeiten „*Vertraulichkeit, Verfügbarkeit und Integrität*“ wurde

offensichtlich auf das vom deutschen Bundesamt für Sicherheit in der Informationstechnik herausgegebene „Glossar der Cyber -Sicherheit“ und die darin enthaltenen „Grundwerte der Informationssicherheit“ zurückgegriffen.



Beeinträchtigung eines der drei genannten Schutzziele gegeben. Nicht zwingend erforderlich, um den Versicherungsfall auszulösen, ist ein vollständiger Verlust der Verfügbarkeit, Integrität oder Vertraulichkeit.<sup>8</sup>

Die Reichweite des Versicherungsschutzes hängt dabei unter anderem vom Verständnis des Begriffs des *informationsverarbeitenden Systems* ab. Dieser legt fest, welche (technischen) Gerätschaften des Versicherungsnehmers in den Versicherungsschutz eingeschlossen sind und ist ausschlaggebend dafür, ob beispielsweise auch Produktionsmaschinen bzw Fertigungsroboter oder IoT-Geräte ("smarte Geräte") in den Deckungsumfang einbezogen werden. Was unter einem *informationsverarbeitenden Systemen* zu verstehen ist, wird in den *ABC 2018* nicht ausdrücklich definiert. Lediglich in Art 3.2 und 3.3 *ist* eine Konkretisierung enthalten, wonach jedenfalls alle Server erfasst sind.<sup>9</sup>

Zur Risikoabgrenzung für den Versicherer wird in Art 1.2.2 *ABC 2018* die wohl notwendige Ergänzung der Definition der Informationssicherheitsverletzung durch taxativ-konkrete Einzelanführung jener Gefahren bzw Ereignisse geschaffen, die zwingend erfüllt sein müssen, damit eine Informationssicherheitsverletzung iS der *ABC 2018* vorliegt. Im Grunde stellt dies eine abschließende Aufzählung der in der Cyberversicherung versicherten Cybergefahren dar: Angriffe auf elektronische

Daten oder informationsverarbeitende Systeme des Versicherungsnehmers, unberechtigte Zugriffe auf elektronische Daten des Versicherungsnehmers, unberechtigte Eingriffe in informationsverarbeitende Systeme des Versicherungsnehmers, Handlungen oder Unterlassungen, die zur Verletzung datenschutzrechtlicher Vorschriften durch den Versicherungsnehmer führen, sowie Schadprogramme, die auf elektronische Daten oder informationsverarbeitende Systeme des Versicherungsnehmers wirken. Der letztgenannte Tatbestand soll insbesondere der Klarstellung dienen, dass auch nicht zielgerichtete Angriffe auf eine unbestimmte Vielzahl von Adressaten (zB mittels Malware) – soweit man diese nicht bereits unter "Angriffe auf elektronische Daten oder informationsverarbeitende Systeme" subsumieren kann – vom Versicherungsschutz umfasst sein sollen.<sup>10</sup>

## Fazit

Insgesamt zeigt sich, dass die Cyberversicherung der *ABC 2018* keine umfassende Deckung für sämtliche Cybergefahren gewährt, aber immerhin eine Mehrgefahrendeckung.

<sup>8</sup> Pawig-Sander in Ruffer/Halbach/Schimikowski, *Versicherungsvertragsgesetz*<sup>4</sup> (2020), AVB Cyber A.1-2 Rz 3f.

<sup>9</sup> Fortmann, *Cyberversicherung: ein gutes Produkt mit noch einigen offenen Fragen* (2019) S 431.

<sup>10</sup> Kath, *ZVers 3/2019, Die Cyberversicherung Überblick über ein neues Versicherungsprodukt* (2019) S 14.



**Literatur- und Judikaturverzeichnis:**

1. *Keltner in Berisha/Gisch/Koban (Hrsg), Haftpflicht-, Rechtsschutz- und Cyberversicherung (2018)*
2. *Malek/Schütz, Cyberversicherung: Rechtliche und praktische Herausforderungen (2019)*
3. *Kath, ZVers 3/2019, Die Cyberversicherung Überblick über ein neues Versicherungsprodukt (2019)*
4. *Fortmann, Cyberversicherung: ein gutes Produkt mit noch einigen offenen Fragen (2019)*