Versicherbarkeit von Cyber Schäden bzw. Auswirkung auf die persönliche Haftung der Geschäftsführung

Graz, 09.05.2017

Member of the GrECo JLT Group

A partner of

ERSTE BANK SPARKASSE

Cyber & Crime – Definitionsversuch

„Cyber“

Summe aller nachteiligen, unerwünschten Störungen und unerlaubten Beeinträchtigungen von persönlichen wie geschäftlichen Daten über sämtliche zur Verfügung stehende Möglichkeiten internetbasierten internen wie externen Datenaustauschs (PCs, Laptops, Smartphones, cloud-solutions, externe Server,….).

„Crime“

Summe aller von Vertrauenspersonen oder außenstehenden Dritten in Schädigungsabsicht vorsätzlich begangenen, illegalen und unerlaubten Handlungen gegen ein Unternehmen, sei es in Bereicherungsabsicht oder sonstigen Motiven (z. B. Geheimnisverrat, Diebstahl, Diskreditierung, etc.).

CYBER-Versicherung – Hintergrund

- Versichert ist das Unternehmen gegen Beeinträchtigungen von persönlichen wie geschäftlichen Daten über sämtliche zur Verfügung stehende Möglichkeiten des Datenaustauschs
- Ursprung: Datenschutz
- Cyberdeckungen sind nicht beschränkt auf eine Absicherung gegen „Cyberkriminalität“, auch wenn diese im Fokus steht
- Ursache der Beeinträchtigung können neben diversen Angriffen auch menschliche Fehler oder technisches Gebrechen sein (z.B. Verlust eines Laptops aber auch Verlust eines Aktenkoffers)
- Cyberdeckungen beinhalten Haftpflicht-, Eigenschaden- und allgemeine Dienstleistungs-komponenten (IT-, Rechts- und PR- Spezialisten)
- „Cyber-Event“ ist Voraussetzung, also eine Datenschutz- oder Netzwerksicherheitsverletzung

Cyber Risiken – Thema Datenschutz

DATENSCHUTZGRUNDVERORDNUNG – NEU AB 2018

Artikel 82 Datenschutz-Grundverordnung (EU)

Haftung und Recht auf Schadenersatz

(1) Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

§ 33 Datenschutzgesetz (DSG)

Schadenersatz

(1) Ein Auftraggeber oder Dienstleister, der Daten schuldhaft entgegen den Bestimmungen dieses Bundesgesetzes verwendet, hat dem Betroffenen den erlittenen Schaden nach den allgemeinen Bestimmungen des bürgerlichen Rechts zu ersetzen. Werden durch die öffentlich zugängliche Verwendung der in § 18 Abs. 2 Z 1 bis 3 genannten Datenarten schutzwürdige Geheimhaltungsinteressen eines Betroffenen in einer Weise verletzt, die einer Eignung zur Bloßstellung gemäß § 7 Abs. 1 des Mediengesetzes, BGBl. Nr. 314/1981, gleichkommt, so gilt diese Bestimmung auch in Fällen, in welchen die öffentlich zugängliche Verwendung nicht in Form der Veröffentlichung in einem Medium geschieht. Der Anspruch auf angemessene Entschädigung für die erlittene Kränkung ist gegen den Auftraggeber der Datenverwendung geltend zu machen.

(2) Der Auftraggeber und der Dienstleister haften auch für das Verschulden ihrer Leute, soweit deren Tätigkeit für den Schaden ursächlich war.

Cyber Risiken – Thema Datenschutz

2. Haftpflichtansprüche von Dritten

„Die gesamte EU-Datenschutz-Gesetzgebung befindet sich gerade in einem Umbruch. Und das Endresultat wird sich wahrscheinlich irgendwo zwischen den Forderungen der Mahner aus der (nicht nur digitalen) Wirtschaft und denen der Datenschützer und Politik einpendeln - **vermutlich in letzter Instanz erst vor Gericht**. Und das dauert. Wir sprechen hier über einen Zeitraum von zwei bis drei - ja, vielleicht sogar fünf Jahren - bis wir wirklich Klarheit haben."

„Wirft man einen Blick auf den aktuellen Stand der Diskussion zum Privacy Shield, die **Anpassung der EU-Datenschutz-Grundverordnung an nationales Recht** oder auch den generellen Umgang mit personenbezogene Daten (PII), dann ist **aktuell nur sicher, dass nichts sicher** ist. Die Meinungen der Rechtsexperten taumeln zwischen „Alles wird schlimm" und „Alles wird gut". Hauptsächlich vermutlich, weil die **Gesetze und Verordnungen dazu neigen, herrlich unkonkret zu bleiben**. Und weil das so ist, werden am Ende Gerichte darüber entscheiden, was in der Praxis erlaubt sein wird und was nicht, wahrscheinlich indem jemand verklagt wird. Begriffe aus der digitalen Praxis wie Cookies, Tags, Opt-In oder Log-In-Daten werden sicherlich keine Verwendung in der Gesetzgebung finden. Wird es also in Zukunft einen klarer umrissenen und in der EU einheitlichen Handlungsspielraum geben? Möglicherweise, aber sicher nicht von jetzt auf gleich

Quelle: Finanznachrichten.de 1.6.2016, Dr. Jochen Schlosser, Senior Vice President Data , Adform

Cyber Risiken – Thema Datenschutz

3. Behördliche Verfahren und Strafen

Artikel 83 Datenschutz-Grundverordnung

Allgemeine Bedingungen für die Verhängung von Geldbußen

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

(5) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von **bis zu 20 000 000 EUR** oder im Fall eines Unternehmens von **bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahrs verhängt, **je nachdem, welcher der Beträge höher ist**.

Artikel 99 Datenschutz-Grundverordnung

Inkrafttreten und Anwendung

(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

(2) Sie gilt ab dem 25. Mai 2018

CYBER-Versicherung – Deckungsüberblick

Eigenschäden (taxativ)	Drittschäden/Haftung wegen	Dienstleistungen
• Forensische Ermittlungskosten (Datenverlust, Datenmanipulation) • Mehraufwand z. B. zur Wiederherstellung von Daten/Systemen • Betriebsunterbrechung/ Ertragsausfall • Erpressung - Lösegeldforderungen • Abwehrkosten bei Datenschutzuntersuchungen / Verfahren (tw. Geldbußen) • Informationskosten an Kunden und Behörden	• Datenschutzverletzungen • fehlender Netzwerksicherheit und Hackerangriffe • nicht erfolgter Information nach DSG • Verletzung geschützter Unternehmensinformationen • Rechtsverletzungen in digitaler Kommunikation	• IT- Dienstleistungen • Rechts- Dienstleistungen • PR- Dienstleistungen • Sofortmaßnahmen (Notfallnummer)

Crime – Vertrauensschaden

Vertrauensschäden

Summe aller von Vertrauenspersonen oder außenstehenden Dritten in Schädigungsabsicht vorsätzlich begangenen unerlaubten Handlungen gegen ein Unternehmen, sei es in Bereicherungsabsicht oder sonstigen Motiven (z. B. Untreue, Unterschlagung, Betrug, Diebstahl etc.)

- Ursprung – Absicherung gegen Wirtschaftskriminalität („white collar crime“)
- Versicherungsschutz für das Unternehmen gegen „Kriminalität am Arbeitsplatz“
- Absicherung von Eigenschäden und Drittschäden, verursacht durch
  - Vertrauenspersonen
  - Dritte (etwas eingeschränkter)

Vertrauensschaden-Versicherung – Überblick

Schäden durch Vertrauenspersonen	Schäden durch Dritte	Zusätzliche Kosten
• Unmittelbare Vermögensschäden des VN • Schäden aus Geheimnisverrat (eigene und fremde Betriebsgeheimnisse) • Drittschäden (bei vorsätzlichen Schädigung eines Dritten durch eine Vertrauensperson)	• Cyber-Schäden durch Dritte • Raub • Tresoreinbruch • Fälschen von Zahlungsanweisungen und Rechnungen • Überweisungsbetrug • Falschgeld, Bank- und Zahlungsanweisungen • Kreditkartenbetrug • Bargeld, Wertpapiere • Betrug (fake president)	• Schadenermittlung • Rechtsverfolgung • PR- Dienstleistungen • Mehrkosten zur Aufrechterhaltung des Geschäftsbetriebes • Datenwiederherstellung • Zinsen • Abwehrkosten • Vertragsstrafen

Cyber & Crime – Spartenübergreifende Deckungskomponenten

	Sach-/techn. Versicherung*	Haft-pflicht	Erpressung	Crime	Cyber
Eigenschäden					
Kosten für IT-Forensik	-	-	-	✓	✓
Kosten für PR-Berater	-	-	-	✓/○	✓
Kosten für Rechtsberatung	-	-	-	- /○	✓
Kosten für die Benachrichtigung der Betroffenen nach Datenverlust	-	-	-	-	✓
Kosten für die Wiederherstellung der Daten nach einem Hackerangriff	-	-	-	✓	✓
Sachschadenunabhängiger Betriebsunterbrechungsschaden	-	-	-	- /[○]	✓
Erpressung/ Bedrohung	-	-	✓	-	✓
Vermögenschäden aus nicht cyberspezifischen Events	-	-	✓	✓	-
Drittschäden					
Ansprüche wegen Datenschutzrechtsverletzung	-	○	-	-	✓
Ansprüche wegen Persönlichkeitsrechtsverletzung	-	○	-	-	✓
Ansprüche wegen Verletzung geistiger Eigentumsrechte	-	○	-	-	✓
Ansprüche wegen Übermittlung von Malware auf Drittsysteme	-	○	-	-	✓/○

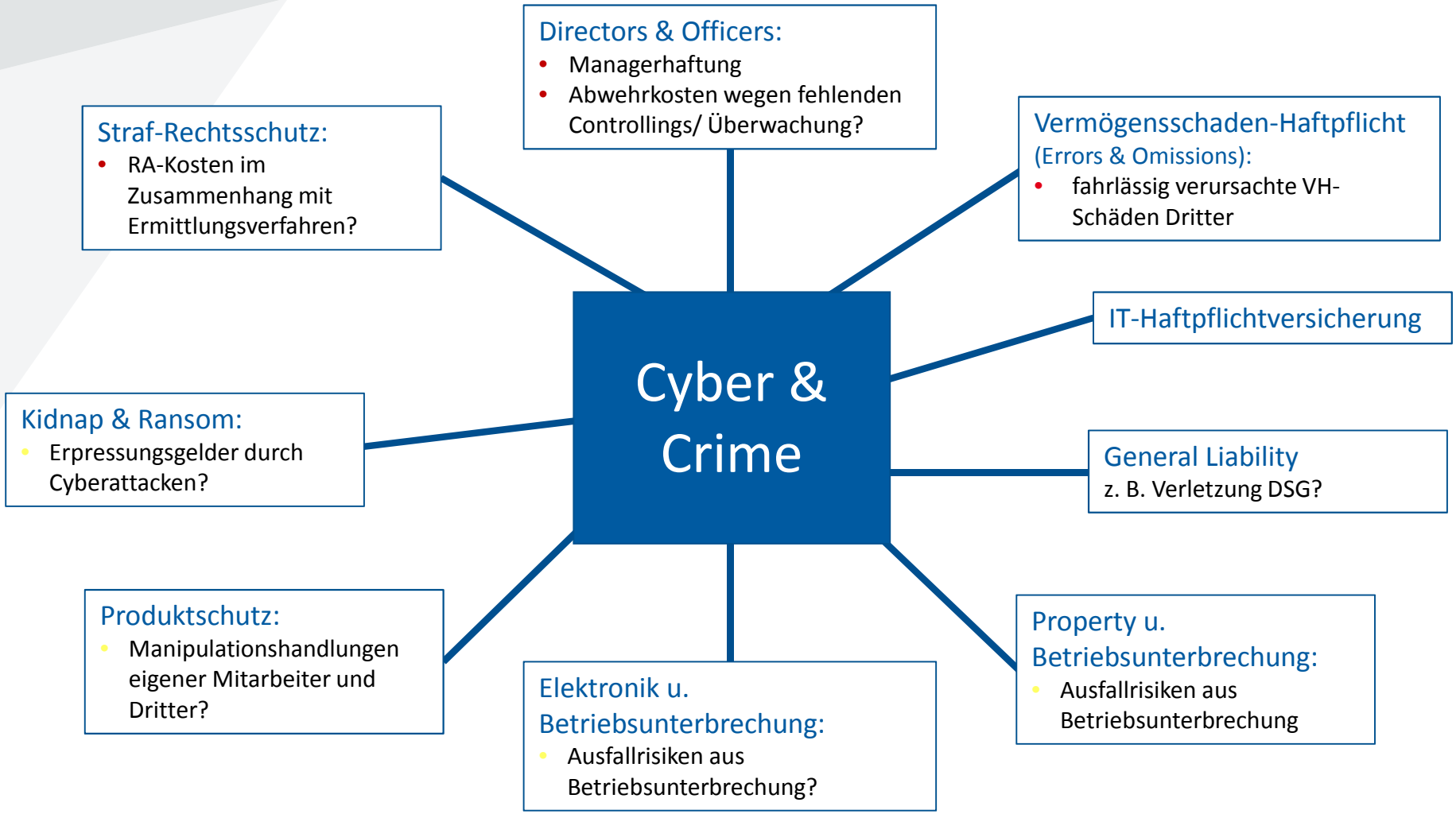
✓ **versichert** - **nicht versichert** ○ **Einschluss möglich/fallweise möglich**

Überblick Grenzen maßgeblicher Versicherungssparten

	Sach/Techn. Vers.	Haftpflicht	Erpressung	Crime	Cyber
Eigenschäden	(sachschadenunabhängig)	(i.V.m. vers. Risiko)			(cyberspezifisch)
Kosten für IT-Forensik	x	x	x	✓/O	✓
Kosten für PR-Berater	x	x	x	x/O	✓
Kosten für Rechtsberatung	x	x	x	x/O	✓
Kosten für die Benachrichtigung der Betroffenen nach Datenverlust	x	x	x	x	✓
Kosten für die Wiederherstellung der Daten nach einem Hackerangriff	x	x	x	✓	✓
Sachschadenunabhängiger Betriebsunterbrechungsschäden	x	x	x	x/O	✓
Erpressung/ Bedrohung	x	x	✓	x	✓
Vermögenschäden aus nicht cyberspezifischen Events	x	x	✓	x	x
Drittschäden					
Ansprüche wegen Datenschutzrechtsverletzung	x	O	x	x	✓
Ansprüche wegen Persönlichkeitsrechtsverletzung	x	x/O	x	x	O
Ansprüche wegen Verletzung geistiger Eigentumsrechte	x/O	x	x	✓	x
Ansprüche wegen Übermittlung von Malware auf Drittsysteme	x	O	x	x	✓

✓ versichert **X nicht versichert** **O Einschluss möglich / fallweise möglich**

Cyber & Crime – Schnittstellen zu anderen Versicherungslösungen



D&O Versicherung

Wann kann ein Cyber oder Vertrauensschaden zu einem D&O Schaden werden?

IT – Sicherheit

IT- Sicherheit ist Kernkompetenz eines Unternehmens

- Verantwortung der Geschäftsleitung als Kollegialorgan
- Geschäftsleitung als Kollegialorgan ist verpflichtet einen für das Ressort verantwortlichen GF zu überwachen
- Ressort verantwortlicher GF obliegt die Auswahl, Anleitung und Kontrolle des zuständigen IT Managers

Konkrete Vorwürfe an Geschäftsleitung

- Der Aufbau einer sicheren IT-Infrastruktur und die Durchsetzung notwendiger Prozesse, um eine sichere Zahlungsfreigabe zu gewährleisten, wurden nicht (in ausreichendem Maße) veranlasst.
- Interne Vorschriften (4-Augen-Prinzip, Einholen der Unterschrift zweier Vorstände für Zahlungsanweisungen) wurden zu wenig kommuniziert, es wurden zu wenige Schulungen durchgeführt.
- Keine (ausreichenden) Kontrollabläufe im Bereich Finanzen installiert und durchgesetzt.
- Das Personal war ungeeignet und deren Auswahl sorgfaltswidrig.

D&O auf einen Blick

Vermögensschadenhaftpflichtversicherung für Unternehmensleiter

- Haftpflichtversicherung (Versicherung der Haftung)
- Unternehmensleiter (nicht des versicherten Unternehmens)
- Vermögensschäden (keine Personen- und Sachschäden)

Was ist versichert?

- Der Versicherer gewährt den versicherten Personen Versicherungsschutz, wenn sie während der Dauer des Versicherungsvertrages erstmals wegen einer bei Ausübung der versicherten Tätigkeit begangenen Pflichtverletzung von einem Dritten, einer versicherten Person oder von einem versicherten Unternehmen für einen Vermögensschaden in Anspruch genommen werden (claims-made Prinzip, der Versicherungsfall ist die Inanspruchnahme).

- Abwehr unbegründeter und Befriedigung begründeter Schadenersatzansprüche (Abwehr- und Leistungsfunktion)

D&O ist keine Eigenschadendeckung des VN

Bilanzschutz?

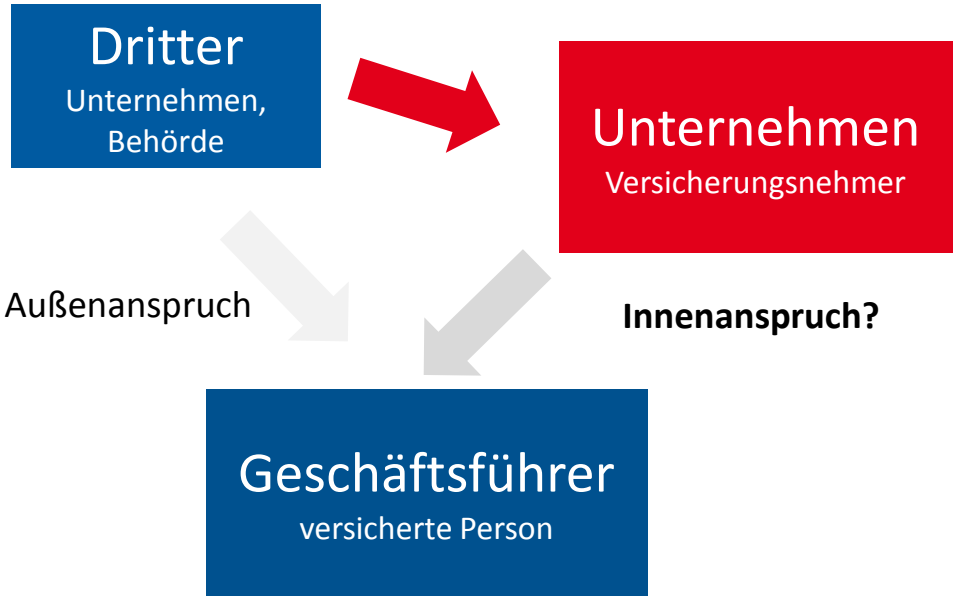
Vermögensschäden die gegen den VN geltend gemacht werden sind nur in Ausnahmefällen versichert (Entity-Deckungen wie z.B. die Wertpapierhandelsdeckung)

Vermögensschäden, die der VN entstehen werden nicht „automatisch“ vom Versicherer übernommen.

Die versicherte Person muss ernsthaft in Anspruch genommen werden. Es muss mit einem Haftpflichtprozess gerechnet werden.

Nur wenn eine Haftung der versicherten Person vorliegt, wird der Vermögens-schaden vom Versicherer übernommen.

nicht versichert, aber u.U. Inanspruchnahme im Rahmen von Innenansprüchen



D&O und Cyber Versicherung

D&O ist kein vollwertiger Ersatz für Cyber – Versicherung

- Kernvoraussetzung für das Greifen einer D&O ist immer eine Pflichtverletzung
- D&O setzt immer eine ernsthafte Inanspruchnahme (Innenanspruch) voraus
- Kein Versicherungsschutz bei wissentlicher Pflichtverletzung

D&O kann aus Sicht des Unternehmens (nur) als eventuelle „Auffangdeckung“
bei Cyber- und Crimeschäden dienen (Kernfunktion: Absicherung der versicherten Personen)

Danke für Ihre Aufmerksamkeit!

Member of the GrECo JLT Group

A partner of

ERSTE BANK SPARKASSE