14. Bonner Dialog für Cybersicherheit (BDCS)

Digitale Selbstverteidigung – Morgen ist es zu spät

Der Transfer von Cyber-Risiken auf Cyber-Versicherungslösungen als Teil der „Digitalen Selbstverteidigung“

Bonn, 05. Mai 2020

Dr. Dominik Bender
Prokurist / Syndikusrechtsanwalt

DR. AXE
AXEKURANZ

Agenda

- Risikoexponierung
- Risikoanalyse & Risikotransfer
- Risikoabsicherung
- Cyber-Trends 2020 & Ausblick

RISIKOEXPONIERUNG

DR. AXE
AXEKURANZ

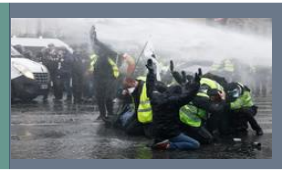
Das Allianz Risk Barometer 2020 - Die 10 wichtigsten globalen Geschäftsrisiken

1 39%

Cybervorfälle
(z.B. Cyberkriminalität, IT-Ausfall, Datenschutzverletzungen durch Mitarbeiter, Geldbußen und Strafen)

2019: 37% (2)

2 37%



Betriebsunterbrechung
inkl. Lieferkettenunterbrechung
(Top-BU-Auslöser: Cyber-Incidents!)

2019: 37% (1)

3 27%

Rechtliche Veränderungen
(z.B. Handelskriege und Zölle, Wirtschaftssanktionen, Protektionismus, Brexit, Zerfall der Euro-Zone)

2019: 27% (4)

4 21%

Naturkatastrophen *
(z.B. Sturm, Überschwemmung, Erdbeben)

2019: 28% (3)

5 21%

Marktentwicklungen
(z.B. Volatilität, verstärkter Wettbewerb/neue Wettbewerber, M&A, stagnierende Märkte, Marktschwankungen)

2019: 23% (5)

6 20%

Feuer, Explosion

2019: 19% (6)

7 17%

Klimawandel/steigende Volatilität des Wetters

2019: 13% (8)

8 15%

Reputationsverlust oder Beeinträchtigung des Markenwerts

2019: 13% (9)

9 13%

Neue Technologien
(z.B. Auswirkung der Vernetzung von Maschinen, Nanotechnologie, AI, 3D-Druck, Blockchain)

2019: 19% (7)

10 11%

Makroökonomische Entwicklungen
(z.B. Sparprogramme, Anstieg der Rohstoffpreise, Deflation, Inflation)

NEU

Source: Allianz Global Corporate & Specialty. Figures represent the number of risks selected as a percentage of all survey responses (2,718). The 2,718 respondents could provide answers for up to three risks. **Photos**: Adobe, iStock, Shutterstock
*Natural catastrophes ranks higher than market developments based on the actual number of responses.

RISIKOEXPONIERUNG

DR. AXE AXEKURANZ

Die Cyber-Risikoexponierung insbesondere von Unternehmen

Ursachen

- Manipulation / Entzug / Verlust von **Unternehmensdaten**;
- Manipulation / Entzug / Fremdnutzung / Verlust von **Kundendaten**;
- Entzug / Manipulation / Verlust / Veröffentlichung von schützenswerten Daten (**Kunden- und Mitarbeiterdaten**)

Geographische Auswirkungen

- Ggfs. weltweit verteilte Niederlassungen / Tochtergesellschaften;
- Ggfs. weltweit ansässige Kunden / Lieferanten.

Mögliche Anspruchsteller / Geschädigte

- **Dritte (Kunden / Lieferanten),** da vertragliche Verpflichtungen nicht eingehalten werden können;
- Dritte **(Kunden), da Erhebung von Kundendaten** (EU-DSGVO!);
- **Konzerngesellschaften** durch interne Wechselwirkungsschäden;
- **Eigener Betriebsunterbrechungsschaden des Unternehmens**;
- **Mitarbeiter**, da Erhebung von personenbezogenen Daten im Anstellungsverhältnis;
- **Behörden**, wenn gesetzl. Datenschutzvorgaben nicht erfüllt.

RISIKOANALYSE & RISIKOTRANSFER

DR. AXE AXEKURANZ

Risikoanalyse: Lösungsansatz über das Risikomanagement eines Unternehmens

Erfassung und Umgang mit sämtlichen relevanten Risiken unabhängig von Art & Qualifikation des jeweiligen Risikos

- Identifikation der je nach Geschäftsfeld unterschiedlich bestehenden Cyber-Risiken und Feststellung des Schadenpotentials (Mögliche Schadenhöhe? Höhe der Eintrittswahrscheinlichkeit? Jeweils unter Integration aller maßgeblichen Risikofaktoren!).

- **Erforderliche Selbstreflektion des Unternehmens**:
  - Allgemein gilt: Know your Costumer (KYC) – und wie schaut es mit dem eigenen Unternehmen aus?
  - Ausreichende Analyse & Optimierung der eigenen (ggfs. von der Aufsicht vorgegebenen) IT-Sicherheit?
  - Verbesserungspotential in jeder Hinsicht (bspw. bessere Vertragsgestaltungen mit externen Dienstleistern zur Durchsetzung adäquater Sicherheitsstandards? Schulungen der Mitarbeiter?)
  - Hinreichende Erfassung von Risiken der Schädigung Dritter (durch das Unternehmen) und dadurch etwaig ausgelöster Haftpflichtansprüche?
  - Wichtige Zwischenfrage bei der Risikoanalyse insb. bei Kunden und Lieferanten: In wessen Umfeld bewege ich mich?

- **Berücksichtigung der ständigen (nationalen wie internationalen) Veränderungen des rechtlichen Umfelds im Bereich der IT-Sicherheit** (bspw. IT-Sicherheitsgesetz, EU-DSGVO, BAIT & MA-Risk im Bankenbereich etc.).

RISIKOANALYSE & RISIKOTRANSFER

DR. AXE AXEKURANZ

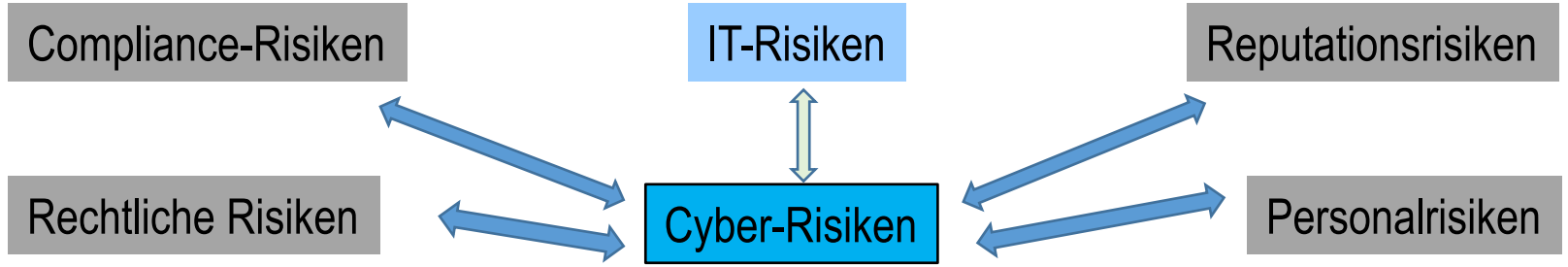
Im Anschluss an die originäre Risikoanalyse:

- Unternehmensinterne Abstimmung zur Vermeidung bzw. Reduktion eigener Kosten und der Frage zur etwaigen Übertragung von Kostenrisiken auf den Risikoträger.
- Erste Feststellung: Cyber-Risiken sind auf der primären Risiko-Ebene überwiegend technischer bzw. organisatorischer Natur.
- **Voraussetzung der Reduktion bzw. Vermeidung von Cyberrisiken:**
  Investitionen in die IT-Infrastruktur & die Unternehmensorganisation (bspw. durch die Schaffung klarer Prozesse u. EU-DSGVO-konformer Datenschutzregelungen für die Mitarbeiter), was eine konsequente Umsetzung & Kontrolle bedingt!
- **Konsequenz:**
  Schaffung eines interdisziplinären Risikomanagements unter Beteiligung aller erforderlichen Kompetenzen.
  Dazu zählen etwa: Risk-Management, IT, Versicherung, Compliance, Controlling, Recht und Datenschutz.
- **Task für das Unternehmen:**
  Bei jedem einzelnen Risiko **gesamtheitliche Bewertung durch alle beteiligten Stellen**, wie welchem Risiko mit welchen Mitteln technisch und wirtschaftlich kompetent zu begegnen ist.
- **Es gilt aber der Grundsatz: Technische und organisatorische Maßnahmen bieten keinen 100%-Schutz gegen Cyber-Gefahren. Es verbleiben Restrisiken.**

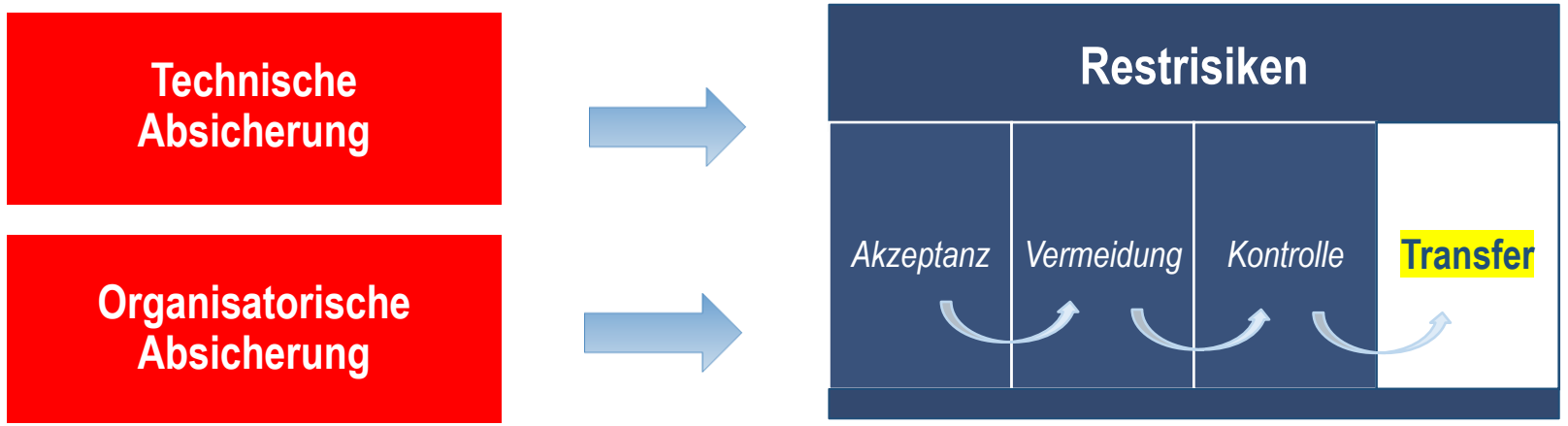
RISIKOANALYSE & RISIKOTRANSFER

DR. AXE AXEKURANZ

Die Cyber-Risikoexponierung insbesondere von Unternehmen



Der Risikotransfer als wichtiger Baustein im ganzheitlichen Cyber-Risikomanagement von Unternehmen



RISIKOABSICHERUNG

DR. AXE
AXEKURANZ

Die Schnittmenge von Cyber-Versicherungen zu „traditionellen“ Versicherungslösungen

Bestehende Versicherungspolicen bieten keinen umfänglichen Versicherungsschutz gegen Cyber-Risiken. Exemplarisch dazu:

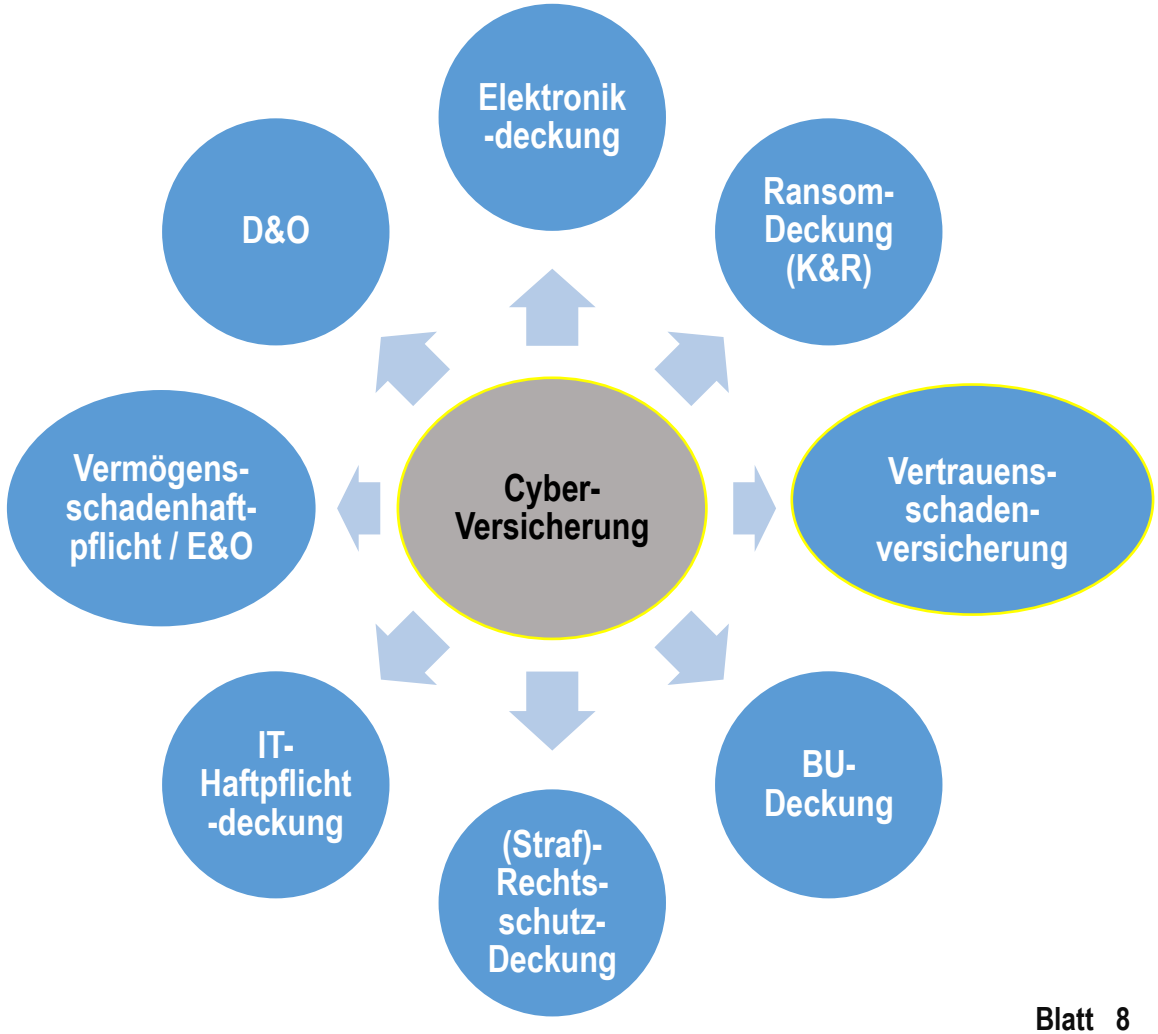
Haftpflichtversicherung: Verschulden des VN erforderlich

BU-Versicherung: Sachschadenereignis notwendig

Sachversicherung: keine Kostenübernahme für Wiederherstellung von Daten, forensischen Dienstleistungen, Informationspflichten ggü. Betroffenen u. Behörden etc.

Versicherungen für Privat (Hausrat, private Haftpflicht, Rechtsschutz u.a.)

Unternehmensdeckungen (nicht abschließend)



RISIKOABSICHERUNG

DR. AXE AXEKURANZ

Schwerpunkte einer (guten) Cyber-Versicherung

Haftpflicht-komponente	Übernahme von cyberspezifischen Eigenschäden	Rechtsschutz	Assistance / Netzwerk mit hochspezialisierten Partnern

Praxisrelevante Cyber-Szenarien und (möglicher) Cyber-Versicherungsschutz

Zielgerichteter Cyber-Angriff

Allgemeine Virenwelle

Verrat, Spionage und Publikation von Daten durch Dritte

Datenschutzverfahren (Rechtsschutz)

Fahrlässig verursachte Datenpannen (inkl. bei Verlust von Mobile Devices)

Cyber-Erpressung

Präventiven Assistance-Dienstleistungen durch Spezialisten

Betriebsunterbrechung (aufgrund einer Cyber-Attacke oder diversen anderen Cyber-Vorfällen; fahrlässige IT-Fehlbedienung durch Mitarbeiter oder sonstige unvorhergesehene technische IT-Probleme)

Sabotage der Versorgung / Verbindung der Unternehmens-IT an Netze (Strom, Internet, Telefon) **durch Dritte**

RISIKOABSICHERUNG

DR. AXE AXEKURANZ

Cyber-Risikoexponierung von Unternehmen und Leistungsportfolien von Cyber-Versicherungen

Drittschäden (Haftung)

Rechtsschutzfunktion (Anspruchsabwehr) / Befriedigung berechtigter Ansprüche:

- Verletzung von Netzwerksicherheit, Datenschutzrecht bzw. von Daten-vertraulichkeit
- Verletzung von Persönlichkeitsrechten (nach Datenverlust)
- Verletzung gewerblicher Schutzrechte / Verletzung der Rechte des geistigen Eigentums
- Verletzung von Vertragspflichten
- (PCI-)Vertragsstrafen

Eigenschäden / Rechtsschutz / Assistance-Bedarf

- Sachschäden (insb. IT-Hardware)
- Betriebsunterbrechungsschäden (insb. entgehender Betriebsgewinn und fortlaufende Kosten)
- Daten- u. Systemwiederherstellungs-aufwand (inkl. Systemverbesserungs-kosten)
- Kosten IT-forensischer Ermittlungen
- „Cyber-Diebstahl“ (missbräuchliche Abverfügungen von Geldbeträgen)
- Erpressungsschäden (inkl. Lösegeld)
- Kosten für Reputations- u. allg. Cyberkrisenmanagement
- Kosten für die Information von Kunden / Behörden nach Datenschutz-verletzungen
- Kosten für die Vertretung in datenschutz- bzw. aufsichtsrechtlichen Verfahren
- Rechtsberatungskosten zu IT- u. Datenschutz
- Kosten für E-Discovery
- Bußgelder (?)
- Präventive Assistance

Cyber-Verdachtsfälle *(Assistance-Bedarf bei potentiellen Cyber-Incidents mit entsprechendem Risiko- und Kostenfaktor)*

RISIKOABSICHERUNG

DR. AXE
AXEKURANZ

Wichtige Assistance-Leistungen im Krisenmanagement als Teil einer ganzheitlichen Cyber-Abwehrstrategie

- **Implementierung bzw. Optimierung von Cyber-Krisenmanagementplänen (auf bestimmte Bereiche wie Cyber-Erpressung bezogen oder übergreifend ausgestaltet):** z.B. etwa Hilfestellungen für relevante Sofortmaßnahmen, Fachinformationen und Anleitungen zu (möglichst von den Akteuren auch gelebten) Rollen und Aufgaben in der Cyber-Krisenbewältigung, Grundlagen zur Cyber-Krisenkommunikation u.v.m.
- **Durchführung von (Onboarding-)Cyber-Workshops zur IT- und/oder Datensicherheit mit dem Versicherer und/oder spezialisierten Kooperationspartnern**
- **Cyber-Krisenstabsübungen angepasst an das Unternehmen zur weiteren Erhöhung der eigenen Widerstands-fähigkeit gegen Cyber-Krisen**

Unmittelbare und mittelbare Stärkung des allgemeinen Cyber-Risikomanagements des Unternehmens

RISIKOABSICHERUNG

DR. AXE AXEKURANZ

Cyber-Versicherungen als wichtiges Element der ganzheitlichen Cyberabwehr-Strategie von Unternehmen

- Risikodialog mit Kunden, um Bedrohungsszenarien zu identifizieren
- Abgestimmtes Verständnis von Geschäftsmodell und Wertschöpfungskette
- Identifikation der „IT-Kronjuwelen“

Risikobewertung

Assess

Respond

Public Relations

- Forensische Dienstleistungen zur Schadenermittlung
- Krisenmanagement und Regulierung im Schadenfall
- Schadenanalyse zur Vermeidung ähnlicher Fälle in der Zukunft

- Empfehlung von techn. Lösungen und Produkten
- Versicherungskonzepte zur Absicherung des Restrisikos
- Individuelle Krisenpräventionsmaßnahmen

Prevent
Protect

Krisenprävention

Detect

IT-Forensik-Partner

- Kontinuierliche Anomalie-Erkennung
- Einsatz von Frühwarnsystemen
- Austausch über aktuelle Bedrohungslagen

CYBER-TRENDS IN 2020

DR. AXE
AXEKURANZ

Unternehmen

- Übergreifendes Cyber-Risikomanagement? Oftmals (leider noch) Fehlanzeige! Aber es wird besser, der Beratungsbedarf steigt stetig.
- Management zunehmend involviert in IT-Security
- IT-Personalentwicklung: ja! Aber wo?
- Check der Lieferketten und bezogenen Services

Angreifer

- Stark verbesserte Angriffstools (teils auf Geheimdienstniveau) und Crime-as-a-Service („*crime to go*“)
- Spezialisierung und Arbeitsteilung der Angreifer („*we are one family*“)
- Unternehmen im (lukrativen) Fokus der Angreifer

Cyber

Öffentlichkeit

- Weitere Etablierung des Lebens in der Kultur des Internets der Dinge (IoT): Anstieg von Networking und (benötigten) Cloud-Computing-Ressourcen
- Wöchentlich neue Pressemeldungen ./. Reputation !
- COVID19: Das neue 360-Grad-Homeoffice – die neue Gefährdungslage für Privat und Firmen

Schäden

- Cyber Erpressung nach zielgerichteten Angriffen gegen Unternehmen ist der neue Trend; der „TrendTrend“: Gesamtpackages mit Bestandteilen von Phishing, Ransomware und Cryptojacking!
- Kosten für Assistance-Dienstleistungen steigen
- Datenschutzverstöße / Geldbußen

Cyber-Versicherung - quo vadis?

- Eigene Schadenerfahrungen der Unternehmen und der steigende Bedarf an präventiven wie reaktiven Assistance-(Service-)Leistungen wichtigste **Gründe der Implementierung von Cyber-Versicherungen**.

- Erforderlichkeit der konstanten **Weiterentwicklung** der **CyberRisk-Versicherungskonzepte** infolge der sich ständig verändernden neuen Cyber-Bedrohungslagen und weiterer Ausbau der (teils bereits guten) Dienstleistungsportfolien durch die Cyber-Versicherer notwendig und geboten.

- **Cyber-Versicherungen** sind zunehmend **Element der gesamtheitlichen** (**Cyber-)abwehr-Strategie** eines Unternehmens und können als **Multiplikator und Treiber der Cyber-Resilienz von Unternehmen** (ggfs. auch für Privatpersonen) zur allgemeinen Stärkung der weltweiten Cyber-Sicherheit (u.a. in Deutschland) beitragen.

- „***Cyber-Blackboxing***“: Risikoadäquate Beratungspraxis Beratung & Absicherung der Unternehmen im Cyber-Bereich ist ***die*** **Herausforderung der Zukunft**.

Vielen Dank für Ihre Aufmerksamkeit !

Dr. Dominik Bender

Prokurist / Syndikusrechtsanwalt

Dr. Hans Günther Axe Assekuranz Versicherungsmakler GmbH

Adenauerallee 133, 53113 Bonn

Tel. +49 (0)228 21 60 65

e-mail dr.axe@axekuranz.de

www.axekuranz.de