Versicherbarkeit von Cyber-Risiken

Darstellung der Risikosituation und Absicherung anhand von Praxisbeispielen

Agenda

1. Cyber-Risikolandschaft – Angriffsszenarien und Gefahren im Überblick
2. Cyber-Risiken – Versicherbarkeit in den jeweiligen Sparten
3. Versicherungsumfang der Cyber-Versicherung im Detail
4. Versicherungsschutz anhand von Praxisbeispielen – vereinfachte Darstellung

1. Cyber-Risikolandschaft – Angriffsszenarien und Gefahren im Überblick

Daten, Zahlen und Fakten

- Die Anzahl der **Cyber-Attacken** steigt jährlich an → von 2019 auf 2020 lag der **Anstieg in Österreich bei 26,3%**
  [Quelle: Cybercrime Report 2020 BMI]
- **65%** aller Cyber-Attacken zielen auf die IT-Systeme ab (u.a. Infiltrierung mit Schadsoftware, Datendiebstahl)
  [Quelle: EY-Studie Datendiebstahl in Österreich 2020]
- **17%** der österreichischen Unternehmen wurden bereits Opfer einer **Ransomware-Attacke**
  [Quelle: EY-Studie Datendiebstahl in Österreich 2020]
- Weltweit wurden im Jahr 2020 **Erpressungsgelder** im Wert von **406,3 Mio US Dollar** ausgezahlt
  [Quelle: Chainalysis]
- **86%** aller Angriffe sind **finanziell motiviert**
  [Quelle: Data Breach Investigation Report 2020,Verizon]

Angriffsszenario	Beschreibung	Opfer
Phishing	Herauslocken von Nutzerzugangsdaten und vertraulichen Informationen	• Raiffeisenbank-Phishing-Mails und SMS • FMA-Phishing-Mails
Malware	Attacke der Systeme mit Schadsoftware bspw. Ransomware	• Salzburg Milch • Schwing GmbH • Palfinger
Betrug	Betrug unter Verwendung elektronischer Kommunikation	• Shark Tank • FACC • Leoni AG
Data Breach	Offenlegung von personenbezogenen bzw vertraulichen Daten	• Gesundheitsministerium • Facebook • Marriott
DoS	Überlastung der IT-Systeme durch massenhafte Serveranfragen	• Gesundheitsministerium www.österreich-testet.at • Telekom Austria

Cyber-Risikokategorien im Überblick

Data Risk

- **Fehlende Kenntnis** über geschäftskritische Daten
- **Mangelnde Absicherung** von personenbezogenen Daten
- Verlust oder Beschädigung von **Daten**
- Mangelhafte Umsetzung von **Datenschutz-Vorschriften**

IT-Risk

- Unzureichende **Wartung**
- Veraltete Software
- Mobile Endgeräte und **BYOD**
- Unzureichende **Weiterbildung** von Mitarbeitern
- **Bedienfehler**
- **Auslagerung der IT** (u.a. Cloud-Services)

Operational Risk

- Störungen/Mängel im Fertigungsprozess (**Produktmängel**)

Infrastructure Risk

- Zerstörung, Verlust oder Beschädigung der **Hardware inkl. Software** durch Elementargefahren
- Zerstörung oder Beschädigung von Sachwerten
- **Ausfall der Stromversorgung**

Crime

- **Ransomware, DDoS- und Hackerangriffe**
- Fraud & Faking (**Phishing & Pharming**)
- **Diebstahl** von Hardware und Daten

Versicherbarkeit im Überblick

Cyber-Risiken	Versicherbar	Nicht versicherbar
Data Risk	• **Mangelnde Absicherung** von personenbezogenen Daten • Verlust oder Beschädigung von **Daten und Software**	• **Fehlende Kenntnis** über geschäftskritische Daten • Mangelhafte Umsetzung von **Datenschutz-Vorschriften***
IT-Risk	• Mobile Endgeräte und **BYOD** • **Bedienfehler** • **Auslagerung der IT-Infrastruktur**	• Unzureichende **Wartung*** • Unzureichende **Weiterbildung** von Mitarbeitern*
Operational Risk	• Das operative Risiko ist grds versicherbar	• Unternehmerrisiko (**Gewährleistung**, Nicht- oder Schlechterfüllung)**
Infrastructure Risk	• Zerstörung, Verlust oder Beschädigung der **Hardware** • **Zerstörung von Sachwerten** (Gebäude, Waren &Vorräte)	• Ausfall der Stromversorgung
Crime	• Crime-Risiken sind grds in ihrer Gesamtheit versicherbar	• Handlungen durch **Gesellschafter** mit einer Beteiligung über 25%

*Die Folgen dieser Risiken sind teilweise versicherbar.
** Das Unternehmerrisiko ist lediglich teilweise versicherbar (zB Nachbesserungs-Begleitschäden, Aus- und Einbaukosten etc.)

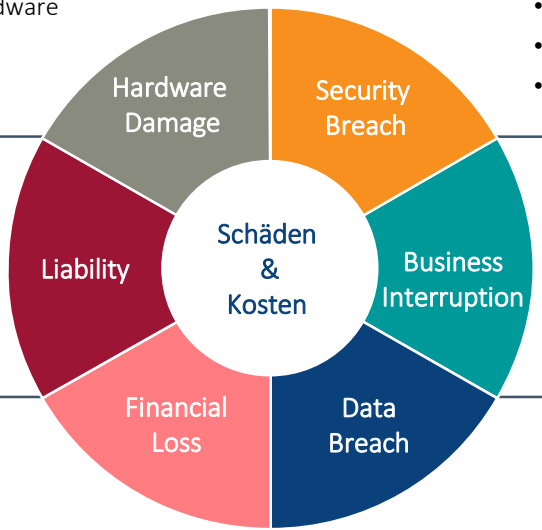
Schäden im Überblick

Hardware Damage

- Kosten für die **Wiederbeschaffung** von Hardware
- **Wiederherstellung** von Daten

Security Breach

- Kosten für IT-Forensik und Krisenberatung
- **Datenwiederherstellungskosten**
- **Lösegelder**



Liability

- **Schadenersatzansprüche** Dritter
- Abwehrkosten
- Unterlassungs- und Widerrufsklagen

Business Interruption

- **Mehrkosten** für die Aufrechterhaltung des Betriebes (zB Anmietung von IT-Infrastruktur)
- **Entgangener Gewinn**

Financial Loss

- Hoher **finanzieller Schaden** (zB Verlust von Geldern, Waren etc.)
- Rechtsverfolgungs- und **Schadenermittlungskosten**

Data Breach

- Kosten für **IT-Forensik**
- Rechts- und PR-Beratung
- **Benachrichtigungskosten**

2. Cyber-Risiken – Versicherbarkeit in den jeweiligen Sparten

Potentieller Versicherungsschutz


Potentieller Versicherungsschutz für Cyber-Gefahren pro Sparte (vereinfachte Darstellung)

Cyber Risiken	Cyber-Versicherung	Vertrauensschaden versicherung	Betriebshaftpflicht-versicherung	Sach-All-Risk- inkl. BU-Versicherung	Technische Versicherung
Data Risk					
IT-Risk					
Operational Risk					
Infrastructure Risk					
Crime					

Cyber-Risiken: Abgrenzung des Deckungsumfanges in den anderen Sparten

Vertrauensschaden-versicherung

- Kein ausreichender Versicherungsschutz **für IT-Forensik und Datenwiederherstellung**
- **Betriebsunterbrechungsschäden** sind nicht versichert
- **Nur zielgerichtete Angriffe** sind vom Versicherungsschutz umfasst

Betriebshaftpflicht

- Bietet keinen Versicherungsschutz für **Eigenschäden**
- IT-Forensik ist nur im Rahmen der Prüfung des Versicherungsfalles gegeben
- Versichert lediglich die **Abwehr und Freistellung** von **Schadenersatzansprüchen** Dritter

Sach- inkl. BU-Versicherung

- **EDV-Anlagen** sind grds **ausgeschlossen**
- Kein Versicherungsschutz wenn kein **Sachschaden** vorliegt
- Teilweise sind Viren und Hackerangriffe bereits explizit ausgeschlossen

Technische Versicherung

- Versichert **ausschließlich Schäden** an den **technischen Anlagen**
- Daten- und Datenträger nur versichert, wenn sie **wiederbeschaffbar** und für den Versicherungsnehmer **erforderlich sind**

3. Versicherungsumfang der Cyber-Versicherung im Detail

Cyber-Versicherung: Deckungsumfang im Überblick

Krisenmanagement

- **24H Beratung** durch IT-Sicherheits- und Krisenberater
- **IT-Forensik**
- Credit **Monitoring**

Haftpflicht

- **Freistellung** und **Abwehr** von **Schadenersatz-ansprüchen**

Betriebs-unterbrechung

- **Mehrkosten** für die Nutzung fremder Anlagen
- **Entgangener Gewinn**

Datenwieder-herstellung

- **Kostenschutz** für die **Wiederherstellung** von Daten, auch bei **manueller Wiedereingabe**

Erpressung

- **Bezahlung von Löse- und Belohnungsgeldern,** auch in Crypto-Währungen

Rechtschutz

- **Vertretung** vor der **Datenschutzbehörde** und **Gerichten**
- **Bezahlung** von Bußgeldern

Crime

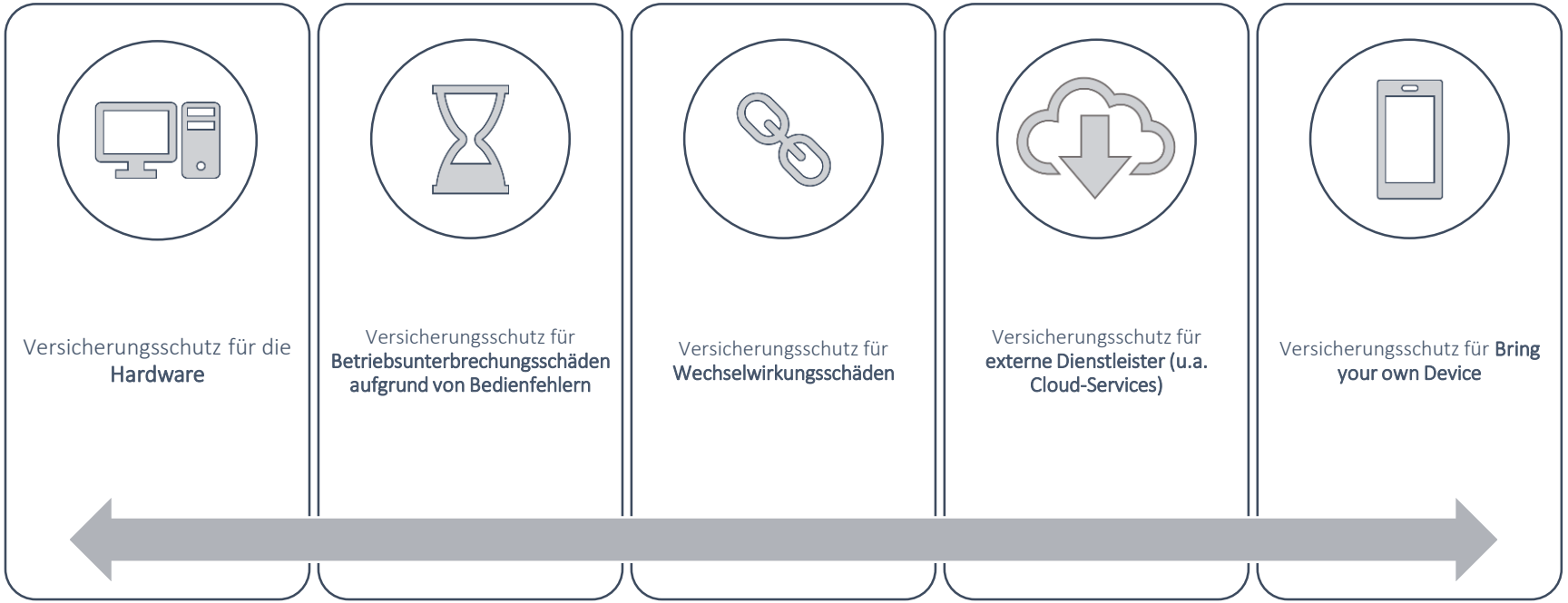
- **Vorsätzliche Schädigung** bspw. durch Cyber-Diebstahl/Fraud [nur eingeschränkter Versicherungsschutz*]

Benachrichtigungs-kosten

- **Meldung an Betroffene** und die **Datenschutzbehörde**
- **PR-Beratung**

* Für KMU's gibt es Produkte am Markt die auch das Crime-Risiko umfassend versichern

Cyber-Versicherung: Deckungserweiterungen



Potentieller Versicherungsschutz

Versicherungsumfang nach Angriffsszenarien (vereinfachte Darstellung)

Cyber-Risiken	Cyber-Versicherung
Phishing	
Malware	
Fraud	
Data Breach	
DoS	

ACHTUNG!

- Cyber-Versicherung bietet **keinen ausreichenden Schutz** für die **Sachwerte**
- Das operative Risiko (Störungen und Fehler im Fertigungsprozess) ist **nicht versichert**
- **Datenverlust** durch **Elementargefahren** ist nicht versichert
- **Cyber-Betrug** ist meist **gar nicht** oder nur mit einem **Sublimit versichert**

- **Cyber-Versicherung** ist **ein unabdingbarer Bestandteil** eines **gesamtheitlichen Versicherungsschutzes**
- Cyber-Versicherung stellt aber lediglich einen Bestandteil dar und **muss in ein Gesamtkonzept integriert werden**
- **Konzeption eines angemessenen Versicherungsschutzes** bedarf **einer individuellen Analyse**

4. Versicherungsschutz* anhand von Praxisbeispielen – vereinfachte Darstellung

* Der in Folge dargestellte Versicherungsschutz orientiert sich an Standard-Bedingungswerken, besondere – am Markt vorhandene – Deckungserweiterungen wurden nicht berücksichtigt

Versicherungsschutz anhand von Praxisbeispielen – Teil 1

Ein Hackerangriff führt dazu, dass die Klimaanlage des Serverraums ausgeschaltet wird, der Server überhitzt und fängt infolge dessen Feuer. Das Betriebsgebäude wird durch den Brand beschädigt, die Daten zerstört und das Unternehmen erleidet eine Betriebsunterbrechung.

Cyber-Versicherung

- ➢ **Kein Versicherungsschutz für den Sachschaden am Gebäude**
- ✓ Versicherungsschutz für die Beseitigung der Schadsoftware und **Datenwiederherstellung**
- ✓ Eingeschränkter Versicherungsschutz für den **Betriebsunterbrechungsschaden*** und den Ersatz der **Hardware**

Sach- und BU-Versicherung

- ➢ **Kein Versicherungsschutz** für die **Beseitigung der Schadsoftware**, **Datenwiederherstellung und Hardware**
- ✓ Versicherungsschutz für die **Gebäudeschäden** und den **Betriebsunterbrechungsschaden**

Technische Versicherung [! Nur wenn Feuerrisiko mitversichert ist]

- ➢ **Kein Versicherungsschutz für den Sachschaden am Gebäude**
- ✓ Versicherungsschutz für den Ersatz der Hardware und Kosten der **Datenwiederherstellung**

* nur die cyberbedingte BU ist versichert, nicht die BU durch den Gebäudeschaden

Versicherungsschutz anhand von Praxisbeispielen – Teil 2

Durch einen Hackerangriff werden die Daten der Etikettendruckmaschine manipuliert und es wird ein falsches Ablaufdatum auf die Verpackung gedruckt. Ein Konsument verzehrt das bereits abgelaufene, aber laut Angabe des Ablaufdatums noch zum Verzehr geeignete, Produkt und erkrankt. Die Produkte des Herstellers müssen zurückgerufen werden.

Cyber-Versicherung

- ➢ **Kein Versicherungsschutz für Personenschäden und die Rückrufkosten**
- ✓ Versicherungsschutz für die Beseitigung und die Feststellung des Ausmaßes der Attacke, sowie für die **Datenwiederherstellung**

Betriebshaftpflicht-Versicherung

- ➢ **Kein Versicherungsschutz** für die Beseitigung und Datenwiederherstellung
- ✓ Versicherungsschutz für Schäden aufgrund der **mangelhaften Produkte,** sofern versichert auch für Kosten verursacht durch den **Rückruf der Produkte**

Versicherungsschutz anhand von Praxisbeispielen – Teil 3

Ein Hackerangriff führt dazu, dass die elektronischen Daten des Unternehmens verschlüsselt werden. Die Datenwiederherstellung gelingt nicht vollständig und die Bereinigung ist ohne den Entschlüsselungscode nicht möglich, hierfür verlangen die Täter ein Lösegeld. Das Unternehmen steht über eine Woche still.

Cyber-Versicherung

- ➢ **Kein Versicherungsschutz für Rechtsverfolgungskosten** zur Erhebung von Ansprüchen gegen die Täter
- ✓ Versicherungsschutz für die Beseitigung der Schadsoftware, die Kosten eines Krisenberaters, die **Bezahlung des Lösegeldes, Datenwiederherstellung und für die Schäden aufgrund der Betriebsunterbrechung** (Mehrkosten und entgangener Gewinn)

Vertrauensschaden-Versicherung

- ➢ **Kein Versicherungsschutz** für die Bezahlung von Lösegeldern und den Betriebsunterbrechungsschaden
- ✓ **Eingeschränkter Versicherungsschutz** für die Datenwiederherstellung, Beseitigung der Schadsoftware und Mehrkosten
- ✓ **Rechtsverfolgungskosten** zur Erhebung von Ansprüchen gegen die Täter sind voll versichert

Versicherungsschutz anhand von Praxisbeispielen – Teil 4

Ein Mitarbeiter führt auf Verlangen des Geschäftsführers eine Zahlungsanweisung durch. Nach Tagen stellt sich heraus, dass der Mitarbeiter (und das Unternehmen) Opfer eines Cyber-Betrugs wurden. Das Geld kann nicht mehr zurückgeholt werden.

<u>Cyber-Versicherung</u>

➢ **Kein Versicherungsschutz für Rechtsverfolgungskosten** zur Erhebung von Ansprüchen gegen die Täter

✓ Eingeschränkter Versicherungsschutz **für den finanziellen Schaden**[#]

<u>Vertrauensschadenversicherung</u>

✓ Bietet **umfassenden Versicherungsschutz** für Betrugsschäden, auch für Lieferanten- und Rechnungsbetrug

[#] Manche KMU-Produkte am Markt bieten bereits umfassenden Schutz für den finanziellen Schaden

… vielen Dank für Ihre Aufmerksamkeit!

Mag. Kerstin Keltner

KOBAN SÜDVERS GROUP GmbH
Tel.: +43 50871 2217
Mobil: +43 664 357 64 20
E-Mail: kerstin.keltner@kobangroup.at

