RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Cyber-Risiken und Cyber-Versicherungen

WKO NÖ, 12.02.2025
13:00-15:00

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

RA Mag. Stephan Novotny

Rechtsanwalt in Wien

akademischer Versicherungskaufmann

Tätigkeitsbereiche:

- Versicherungsrecht
- Versicherungsvermittlerrecht
- Datenschutzrecht
- Handelsvertreterrecht

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Inhalt

1. Einführung Cyber-Angriffe
2. Überblick Europäische Sicherheitsstrategie
3. Überblick Cyber-Versicherung
4. Musterbedingungen Cyber-Versicherung (ABC 2018)
5. Versicherbare Bausteine

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Inhalt

6. Obliegenheiten des Versicherungsnehmers

7. Abgrenzung zur Vertrauensschadenversicherung

8. Streitfrage Lösegeldversicherung

9. DSGVO und Cyber-Versicherung

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

1. Einführung Cyber-Angriffe

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Cyber-Angriffe

- Zunehmende Abhängigkeit von Technologien durch fortschreitende Digitalisierung
- Aufgrund Vernetzung von IT-Systemen zunehmend auch internationales/geopolitisches Problem
- Cybercrime gilt bereits als größeres Business als globaler Drogenhandel -> Cybercrime als „Kokainhandel des 21. Jahrhunderts“

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Beispiele

- Bis dato weltweit größter IT-Ausfall im Juli 2024
  - Schätzungsweise 8,5 Mio. Windows-Geräte lahmgelegt
  - Lahmlegung von Flugzeugen, Krankenhäusern etc.
  - Befürchtung ähnlicher Vorfälle im Jahr 2025
- Angriff auf Bank in Hong Kong im Februar 2024
  - Mitarbeiter wurde durch KI-generierte Personen aus dem Konzern (Deepfakes) zu Überweisung in Millionenhöhe veranlasst

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Beispiele

- Hackerangriff auf Kärntner Landesverwaltung im Mai 2022
  -> Mutmaßlicher Verkauf von Daten
- Lahmlegung von Websites österreichischer Ministerien und politischer Parteien vor der Nationalratswahl 2024
- Angriffe auf Unternehmen, Krankenhäuser, Banken, FMA, Häfen, Flughäfen, Universitäten, Kulturinstitutionen etc.
- Angriffe gegen Lieferanten -> Verzögerung in Lieferkette

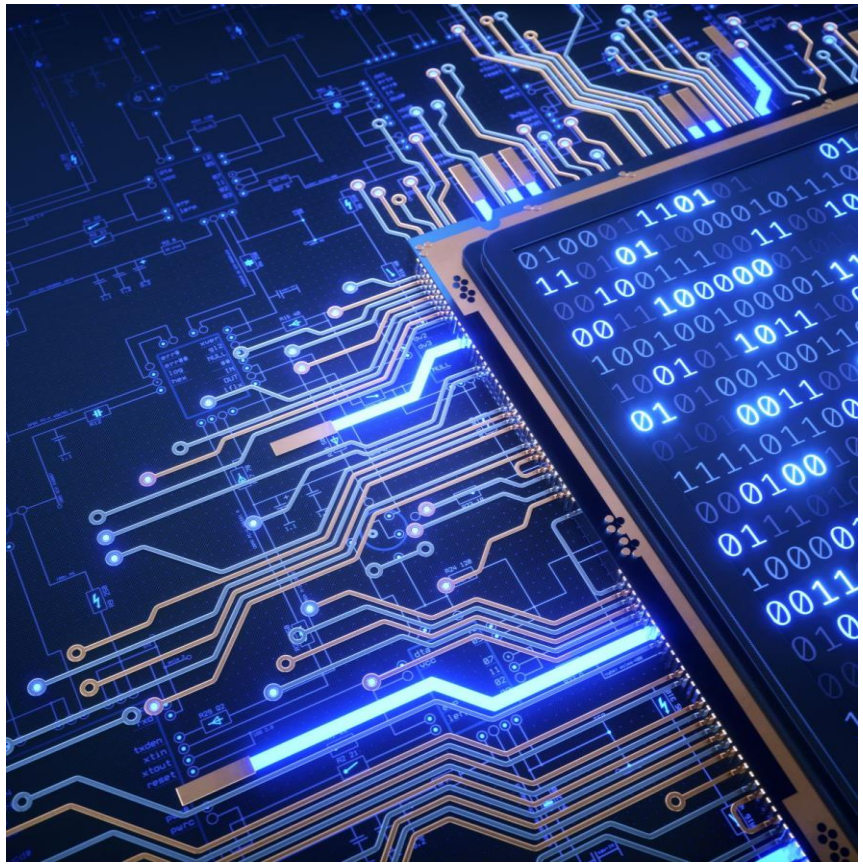
RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Ransomware

- Ransomware = Form von Schadsoftware, die Computer und IT-Systeme kompromittiert, indem sie wichtige Daten verschlüsselt und anschließend an die Benutzer eine Lösegeldforderung stellt, um den Zugang wiederherzustellen
- Aktueller Trend: „Doppelte Erpressung“ -> Verschlüsselung von Daten und gleichzeitig Drohen mit weiteren Maßnahmen wie Datenveröffentlichung, Sperren von Websites etc.
- Für Unternehmen wohl gefährlichste/teuerste Bedrohung -> neben finanziellen Verlusten auch Image- und Vertrauensschaden -> potentiell existenzbedrohend

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

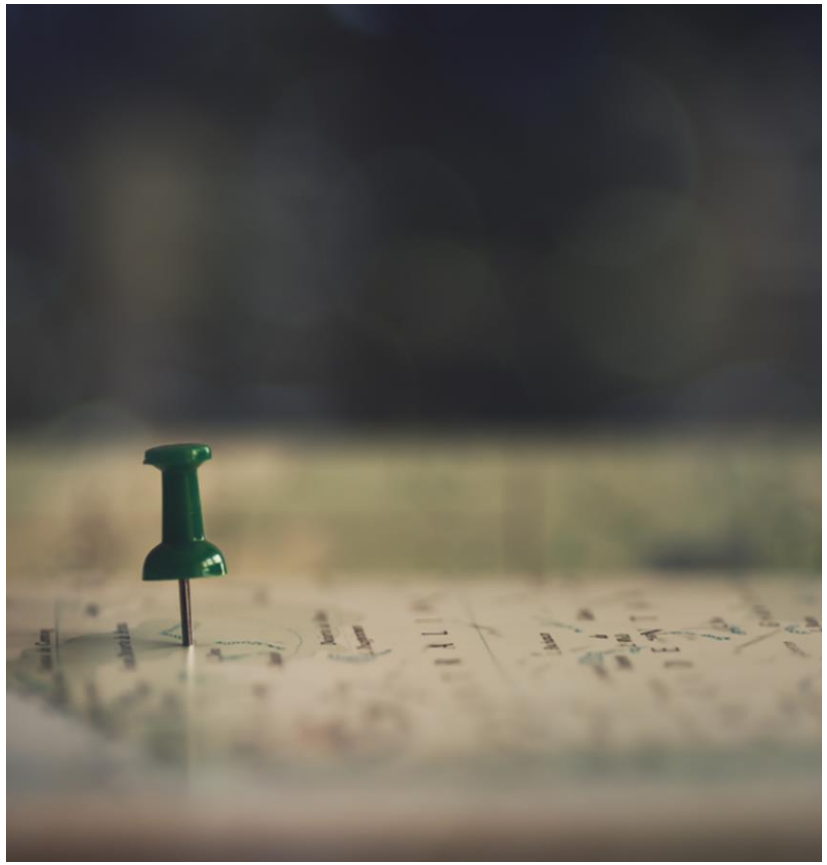
Cybercrime und KI



- Generative KI als Werkzeug für Cyberkriminelle
- Zunehmende Verwendung von Deepfakes
  - Bsp.: Angriff auf Bank in Hong Kong -> Überweisung in Millionenhöhe durch von Deepfakes getäuschten Mitarbeiter
- Large Language Models als zunehmende Sicherheitslücke
  - Potentielle Nutzung von ChatGPT in Cyberangriffen, z.B. um an vertrauliche Informationen zu gelangen
- Weitere Befürchtung: KI-initiierter Börsencrash

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Cyber-Kriegsführung



- Szenario hybride Kriegsführung
- Bsp. Ukraine-Krieg: Sowohl staatsnahe Akteure als auch politisch motivierte „Hacktivisten“ beider Kriegsparteien
- Einsatz von Wiper-Malware auf ukrainischen Computersystemen durch Russland -> Verschlüsselung ähnlich Ransomware, aber ohne die Möglichkeit, Daten nach Zahlung von Lösegeld wiederherzustellen
- Ziele: Blackouts, Funktionstauglichkeit kritischer Einrichtungen, Desinformationskampagne etc.

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Cyber-Security in Österreich

- Österreich: ca. 20.000 Anzeigen wegen Cyberkriminalität (im engeren Sinn) im Jahr 2023, aber vermutlich hohe Dunkelziffer (Quelle: Cybercrime Report 2023 des BKA)
- Studie von KPMG aus dem Jahr 2024 (Befragung von über 1.000 österr. Unternehmen):
  - Jede 6. Cyber-Attacke gegen Unternehmen war erfolgreich (im Vorjahr nur jede 10.) -> Angreifer lernen dazu
  - Top-3-Angriffsarten: Phishing-Attacken, Malware und CEO-Fraud
  - Deepfakes haben sich in Österreich gegenüber dem Vorjahr verdoppelt

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Cyber-Security in Österreich

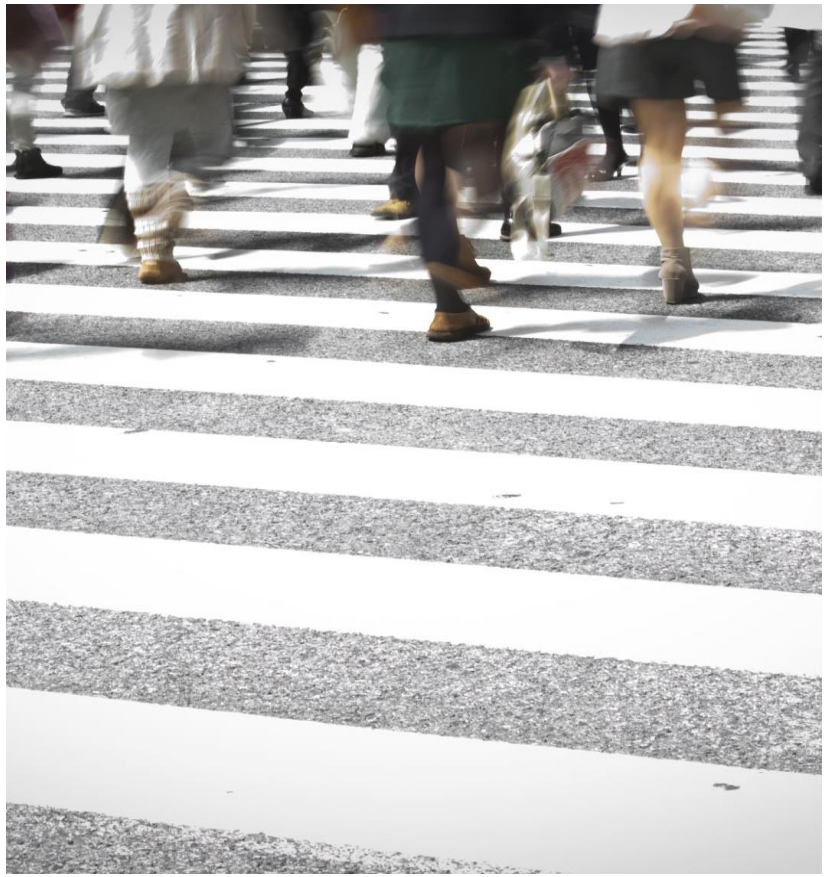
- Zahlreiche Schwachstellen bei österr. Unternehmen (Studie „Realitycheck: IT-Sicherheit im österreichischen Mittelstand“ von Techbold, What‘s next Institute):
  - Bei 58 % hatten Ex-Mitarbeiter noch Zugang auf Unternehmensdaten
  - Bei 26 % konnten Betriebsfremde über Gäste-WLAN relativ leicht auf Firmendaten zugreifen
  - 52 % hatten keine, veraltete oder falsch konfigurierte Firewall
  - 36 % hatten kein funktionierendes Back-Up
  - 36 % hatten keinen ausreichenden Virenschutz

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

2. Überblick Europäische Sicherheitsstrategie

NIS 2-Richtlinie

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY



- NIS 2-Richtlinie („Netz- und Informationssysteme“)
- Ziel: Verbesserung von Resilienz und Reaktion auf Sicherheitsvorfälle in EU
- Hätte bis Oktober 2024 in nationales Gesetz umgesetzt werden müssen -> Verzögerung in Österreich (Problem: Umsetzung benötigt 2/3-Mehrheit im Nationalrat)
- Betroffen sind große und mittlere Unternehmen bestimmter Sektoren (u.a. Versicherungen, Banken, Energie, Verkehr, Post, Abfallwirtschaft, Lebensmittel, Chemie etc.)
- Hohe Strafen für Geschäftsführer persönlich vorgesehen!

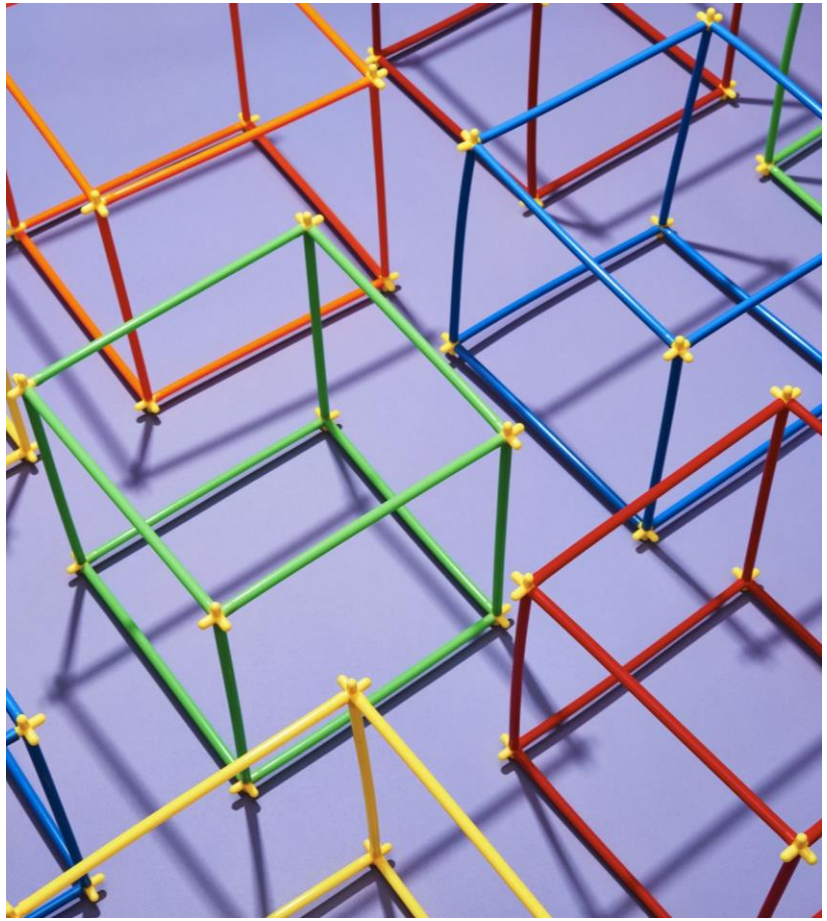
RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

DORA-Verordnung

- DORA-VO („Digital Operational Resilience Act“)
- Ziel: Stärkung der operationellen Resilienz im Finanzsektor, zahlreiche Vorschriften für Technik und Management von IKT-Systemen (Informations- und Kommunikationstechnologie)
- Unterschied zu NIS 2: Gilt nur für Finanzsektor!
- Verordnung -> direkt anwendbar (keine Umsetzung in nationales Recht nötig)
- Anwendbarkeit ab 17.01.2025

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Cyber Resilience Act



- CRA („Cyber Resilience Act“)
- Ziel: Schutz von Verbrauchern und Unternehmen beim Kauf von Software- oder Hardwareprodukte mit einer digitalen Komponente
- Verbindliche Sicherheitsanforderungen, z.B. für intelligente Fernseher, Haushaltsgeräte, Babyphones, Spielzeuge etc.
- Verordnung -> direkt anwendbar
- Am 10.12.2024 in Kraft getreten, aber die wichtigen Verpflichtungen gelten erst ab Ende 2027

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

3. Überblick Cyber-Versicherung

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Cyber-Versicherung

- Cyber-Angriff kann Unternehmen in die Insolvenz stürzen
- Problem: Cyber-Angriffe werden nie zu 100 % verhindert werden können!
  - Geschwindigkeit der Digitalisierung und KI-Entwicklung zu schnell
  - Angreifer lernen zu schnell dazu
  - -> Sisyphos-Arbeit?
- -> Abschluss einer Cyber-Versicherung sinnvoll!
- -> Cyber-Versicherung kann Sicherheitsvorfälle verhindern oder zumindest abfedern

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Cyber-Versicherung

- Junge Versicherungssparte, die in Ö erst seit 2014 angeboten wird
- Cyber-Versicherung als „moderne Feuerversicherung“
- Aber: Nur 22% aller österr. Unternehmen haben Cyber-Versicherung! (KPMG-Studie 2024)
- Auswirkungen und Kostenfolgen eines Cyber-Angriffs werden oftmals unterschätzt!
- Oftmals Spannungsfeld zwischen Vorstand/GF und IT-Leitung, wie sicher die betriebene IT ist

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Beispiele versicherte Risiken

- Malware: Attacke der IT-Systeme mit Schadstoffware (Viren, Würmer, Trojaner) zur Erlangung vertraulicher Daten
- Ransomware: Erpressung durch Verschlüsselung von elektronischen Daten (siehe oben)
- Phishing: Herauslocken von Daten über gefälschte Websites/E-Mails/Kurznachrichten
- „DoS“-Attacken („Denial of Service“): Gezielte Überlastung des IT-Systems durch massenhafte Anfragen an den Server, was zu Funktionsbeeinträchtigungen führt

Ausgestaltung

- Spartenübergreifendes Versicherungsprodukt („Multi-Line-Police“)
- -> Enthält insbesondere Haftpflicht- und Sachelemente
- Aber auch Vertrauensschaden- und Rechtsschutzelemente
- Abgrenzung zu bestehenden Spartenversicherungen (Haftpflichtversicherung, Betriebshaftpflichtversicherung etc.) -> Oftmals Ausschlüsse von Cyber-Risiken in bestehenden Spartenversicherungen

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Cyber-Versicherung

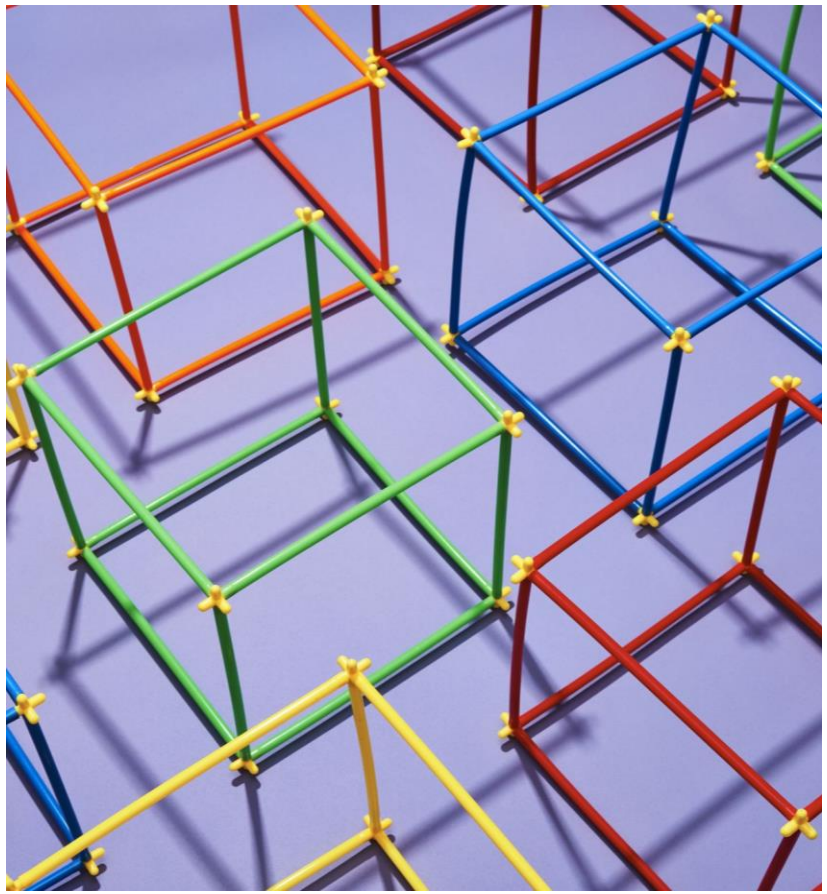
- Strukturelle Verwandtschaft mit der Feuerversicherung (-> Cyberversicherung als „moderne Feuerversicherung“)
- Ähnlich wie die Feuerversicherung kombinierte, verbundene Versicherung
- -> Deckung von Eigenschäden, Drittschäden und Haftpflichtansprüchen
- -> Bündelung in einem einzigen Versicherungsvertrag

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

4. Musterbedingungen Cyber-Versicherung (ABC 2018)

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

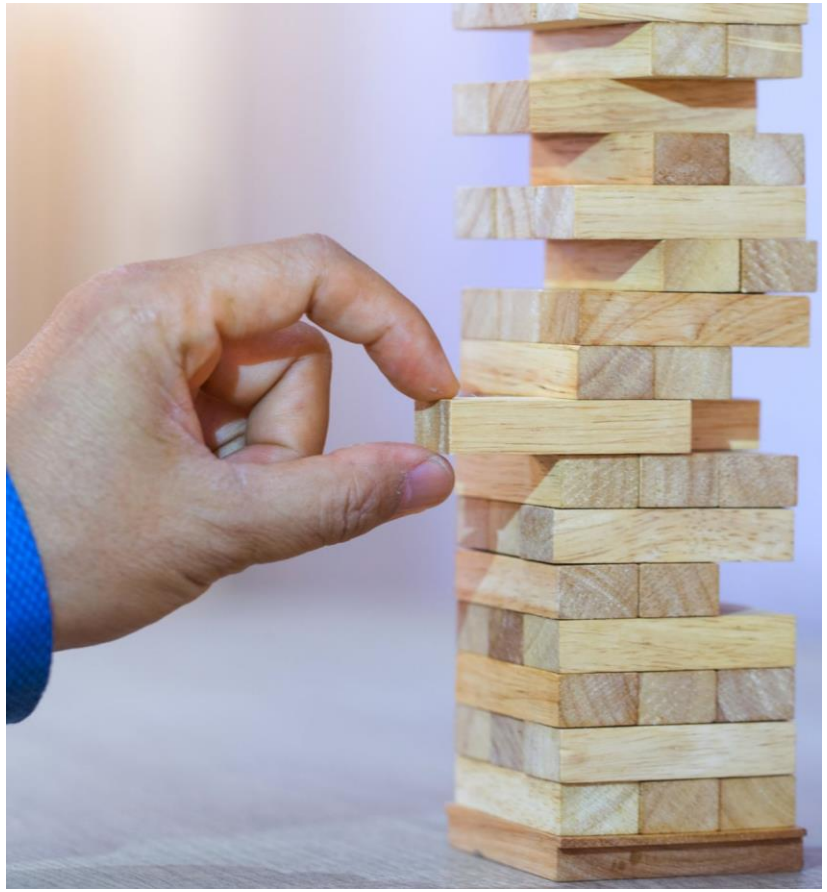
Musterbedingungen ABC 2018



- Musterbedingungen für die Cyberrisiko-Versicherung (ABC 2018) des Versicherungsverbands Österreichs
- Aber: In der Praxis sehr unterschiedliche Bedingungen unterschiedlicher Versicherer
- -> Musterbedingungen haben sich in Österreich noch nicht durchgesetzt!
- Geäußerte Kritik: ABC 2018 wenig kundenfreundlich? -> Sehr viele Ausschlüsse und Obliegenheiten

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Bausteinprinzip



- Bausteinprinzip: Flexible Gestaltung durch Bausteine
  - Service- und Kosten (Baustein A)
  - Betriebsunterbrechung (Baustein B)
  - Datenwiederherstellung (Baustein C)
  - Haftpflicht (Baustein D)
- Aufbau:
  - Gemeinsame Bestimmungen (gelten immer)
  - Besondere Bestimmungen (gelten nur für gewählten Baustein)

Gegenstand der Versicherung

- Gegenstand der Versicherung sind reine Vermögensschäden, die durch eine Informationssicherheitsverletzung (= Cyber-Angriff) verursacht wurden (Art. 1 ABC 2018)
- Informationssicherheitsverletzung = Cyber-Angriff = Beeinträchtigung der Verfügbarkeit/Integrität/Vertraulichkeit von elektronischen, vom VN verarbeiteten Daten oder von informationsverarbeitenden Systemen, die der VN zur Ausübung seiner betrieblichen/beruflichen Tätigkeit nutzt

Gegenstand der Versicherung

- Reine Vermögensschäden: Keine Deckung von Personen- oder Sachschäden
- Elektronische Daten gelten nicht als Sachen im Sinne der Bedingungen -> Vermögensschäden durch Verlust elektronischer Daten sind daher als reine Vermögensschäden versichert
- „Elektronische Daten“ umfasst auch Software und Programme

Risikoausschlüsse

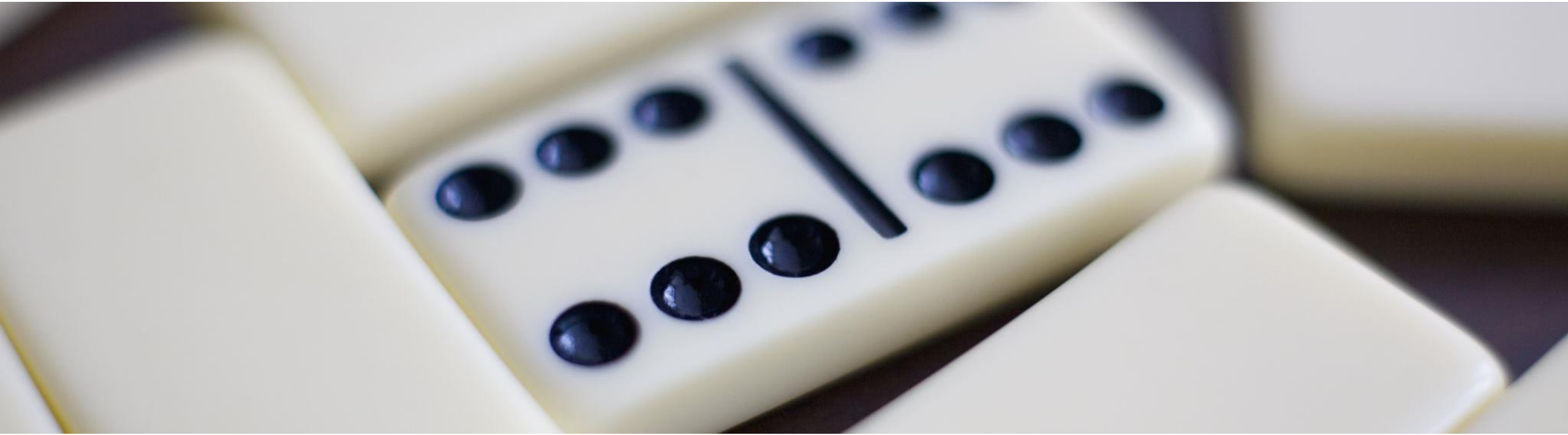
- Risikoausschlüsse z.B. (vgl. Art. 2 ABC 2018):
  - Schäden aufgrund des Ausfalls von Infrastruktur
  - Schäden im Zusammenhang mit Kraftfahrzeugen
  - Schäden aus der Zahlung von Lösegeld/Erpressungsgeld
  - Schäden durch vorsätzliches Abweichen von Gesetzen, Verordnungen etc. durch Arbeitnehmer oder Organmitglieder
  - Schäden durch Kriegsereignisse oder Terrorakte

Risikoausschlüsse

- Zahlreiche weitere Risikoausschlüsse in Art. 2 ABC 2018
- Aktuell diskutiert: Kriegs- und Terrorklauseln
- -> Cyber-Angriffe, die als Terrorakt zu qualifizieren sind, sind von der Deckung ausgenommen
- Debatte: Gilt Cyber-War ohne physischen Krieg als Krieg?
  -> Unterschiedliche Meinungen

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

5. Versicherbare Bausteine



Versicherbare Bausteine

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Service- und Kostenversicherung
(Baustein A, Art. 15-17)

Betriebsunterbrechungsversicherung
(Baustein B, Art. 18-22)

Datenwiederherstellungsversicherung
(Baustein C, Art. 23-27)

Haftpflichtversicherung
(Baustein D, Art. 28-36)

Service- und Kostenversicherung

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

- Forensik/Schadenfeststellungskosten
- Benachrichtigungskosten infolge Verletzung datenschutzrechtlicher Vorschriften (bei besonderer Vereinbarung)
- Call-Center-Kosten für Beantwortung von Fragen infolge Verletzung datenschutzrechtlicher Vorschriften (bei besonderer Vereinbarung)
- Krisenkommunikation und PR-Maßnahmen zur Erhaltung oder Wiederherstellung der öffentlichen Reputation (bei besonderer Vereinbarung)

Betriebsunterbrechungsversicherung

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

- Betriebsunterbrechung: Wenn infolge der Cyber-Attacke elektronische Daten oder informationsverarbeitende Systeme des VN nicht zur Verfügung stehen oder nicht die übliche Leistung erbringen und daraus ein Schaden entsteht (Art. 18)
- Entschädigung: Der längstens während der Haftungszeit eingetretene Unterbrechungsschaden, höchstens jedoch die Haftungssumme (Art. 20)
- Jahreshöchstentschädigung

Betriebsunterbrechungsversicherung

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

- Besondere Risikoausschlüsse: Unterbrechungsschäden
  - für den Zeitraum einer geplanten Abschaltung informationsverarbeitender Systeme
  - durch eine geplante Löschung oder Veränderung elektronischer Daten
  - durch die Einführung neuer Systeme oder Software
  - durch den Einsatz ungetesteter Systeme oder Software
  - durch die Verwendung von Systemen/Softwaren, zu deren Nutzung der VN nicht berechtigt ist
  - durch Softwarefehler ohne Cyber-Attacke

Datenwiederherstellungsversicherung

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

- Kosten für notwendige Aufwendungen zur Wiederherstellung der von der Cyber-Attacke betroffenen Daten (Art. 23)
- Kosten für die Entfernung der Schadsoftware
- Versicherte Daten = elektronische Daten, zu deren Nutzung der VN berechtigt ist und die sich in den informationsverarbeitenden Systemen des VN befinden und von der Cyber-Attacke betroffen sind

Datenwiederherstellungsversicherung

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

- Umfang der Entschädigung: Höhe der tatsächlich angefallenen und erforderlichen Kosten zur Wiederherstellung in den Zustand vor der Cyber-Attacke sowie für Entfernung der Schadsoftware (Art. 25)
- Keine Entschädigung:
  - Für Mehrkosten durch Änderungen oder Verbesserungen, die über die Wiederherstellung hinausgehen
  - Nach Ablauf eines bestimmten Zeitrahmens
  - Für den vom VN zu bezahlenden Selbstbehalt

Datenwiederherstellungsversicherung

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

- Besondere Risikoausschlüsse: Aufwendungen für die Wiederherstellung von Daten, die verlorengegangen sind durch
  - eine geplante Abschaltung informationsverarbeitender Systeme
  - eine geplante Löschung/Veränderung elektronischer Daten
  - die Einführung neuer Systeme oder Software
  - den Einsatz ungetesteter Systeme oder Software
  - die Verwendung von Systemen/Softwaren, zu deren Nutzung der VN nicht berechtigt ist
  - durch Softwarefehler ohne Cyber-Attacke

Haftpflichtversicherung

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

- Versicherungsfälle, die dem versicherten Risiko und der versicherten Betriebsart entspringen und aus welchen dem VN wegen einer Cyber-Attacke und des daraus resultierenden reinen Vermögensschadens Schadenersatzverpflichtungen erwachsen oder erwachsen könnten (Art. 28)

Haftpflichtversicherung

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

- Versicherer übernimmt
  - Erfüllung von Schadenersatzverpflichtungen, die dem VN wegen eines reinen Vermögensschadens aufgrund gesetzlicher Haftpflichtbestimmungen privatrechtlichen Inhalts erwachsen
  - Kosten der Feststellung und der Abwehr einer von einem Dritten behaupteten Schadenersatzverpflichtung
- Ob Cyber-Attacke beim VN, einem mitversicherten Unternehmen oder beim Anspruchsteller eingetreten ist, spielt keine Rolle

Haftpflichtversicherung

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

- Besondere Risikoausschlüsse: U.a.
  - Gewährleistungsansprüche für Mängel
  - Vertragliche Ansprüche, die über den Umfang der gesetzlichen Schadenersatzpflicht hinausgehen
  - Erfüllung von Verträgen
  - Ersatz von Vermögensschäden wegen Verzögerung der vertraglich geschuldeten Leistung
  - Ansprüche für Schäden, die dem VN selbst und dessen Angehörigen sowie seinen Gesellschaftern/Geschäftsteilhabern und deren Angehörigen zugefügt werden

Haftpflichtversicherung

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

- Zusatzdeckungen (Art. 30):
  - Rechtswidrige elektronische Kommunikation: Ansprüche wegen Persönlichkeitsrechts-, Namensrechts-, Urheber- und Markenrechtsverletzungen für durch den VN veröffentlichte elektronische Medieninhalte
  - E-Payment: Vertragsstrafen gegen den VN durch einen E-Payment Service Provider wegen Verletzung eines Payment Card Industry Datensicherheitsstandards
  - Vertragliche Schadenersatzansprüche: Ansprüche Dritter gegen den VN wegen vergeblicher Aufwendungen im Vertrauen auf ordnungsgemäße Vertragserfüllung sowie Mehraufwendungen wegen Verzögerung der Leistung

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

6. Obliegenheiten des Versicherungsnehmers

Obliegenheiten

- Obliegenheiten des VN vor Eintritt des Versicherungsfalls u.a. (vgl. Art. 9 ABC 2018):
  - Alle für den versicherten Betrieb geltenden gesetzlichen Sicherheitsvorschriften sind einzuhalten
  - Informationsverarbeitende Systeme müssen in technisch einwandfreiem Zustand gehalten werden
  - Individuelle Zugänge für Nutzer sind mit ausreichend komplexen Passwörtern gesichert
  - Zusätzlicher Schutz bei erhöhtem Risiko (z.B. Firewall, Verschlüsselung von Datenträgern mobiler Geräte etc.)

Obliegenheiten

- Obliegenheiten des VN vor Eintritt des Versicherungsfalls u.a. (vgl. Art. 9 ABC 2018):
  - Schutz gegen Schadsoftware, der automatisch auf dem aktuellen Stand gehalten wird (Virenscanner etc.)
  - Regelmäßige Sicherungsprozesse -> im Versicherungsfall kein gleichzeitiges Zugreifen auf Originale und Duplikate möglich
  - Verschlüsselung schutzbedürftiger E-Mails
  - Regelmäßige Schulung von Mitarbeitern

Obliegenheiten

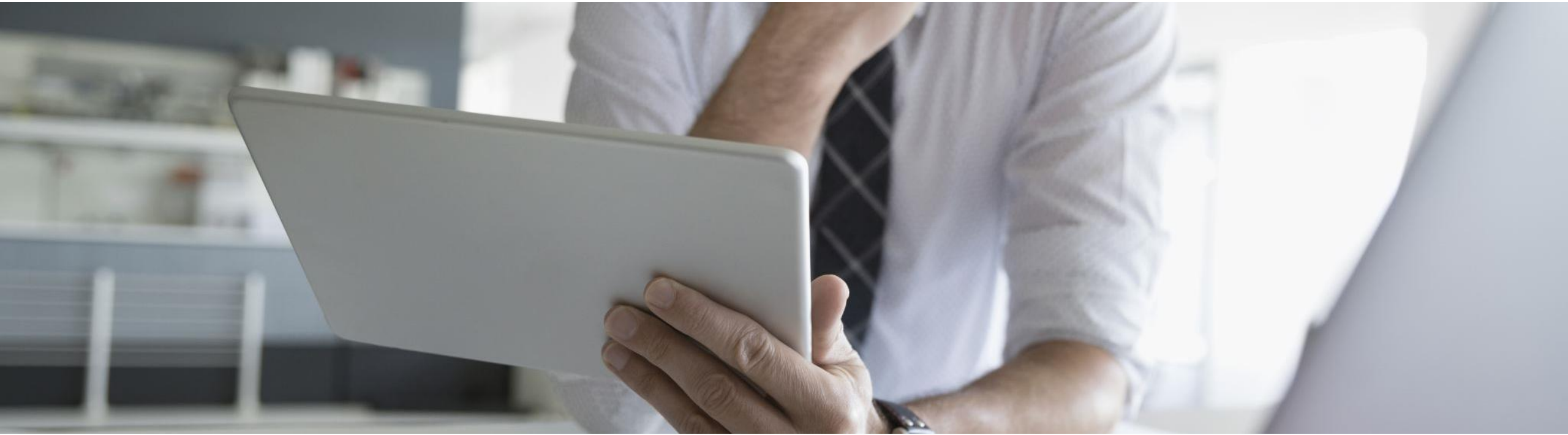
- Obliegenheiten des VN nach Eintritt des Versicherungsfalls u.a. (vgl. Art. 10 ABC 2018):
  - Schadenabwendungs- und Schadenminderungspflicht
    - Für Erhaltung/Rettung/Wiedererlangung der Daten sorgen
    - Weisung des Versicherers einholen und einhalten
    - Betroffene Hardware, Software und Daten sichern
    - Alle Informationen und Daten dem Versicherer übermitteln bzw. dem vom Versicherer eingebundenen Experten zur Verfügung stellen

Obliegenheiten

- Obliegenheiten des VN nach Eintritt des Versicherungsfalls u.a. (vgl. Art. 10 ABC 2018):
  - Schadenmeldungspflicht
    - Unverzügliche Meldung bei Hotline des Versicherers
    - Unverzüglich behördliche Anzeige bei Verdacht auf Vorliegen einer strafbaren Informationssicherheitsverletzung
  - Schadenaufklärungspflicht
    - Dem Versicherer ist nach Möglichkeit jede Untersuchung über Ursache und Höhe des Schadens zu gestatten
    - Unterstützende Mitwirkung bei Schadensermittlung

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

7. Abgrenzungen zur Vertrauensschadenversicherung



RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Vertrauensschadenversicherung

- Achtung: Wird oft mit Cyberversicherung verwechselt
- -> Teilweise Überschneidungen, aber zahlreiche Unterschiede zwischen beiden (siehe unten)
- Vertrauensschadenversicherung: Weder gesetzliche Regelung noch Musterbedingungen -> Sehr unterschiedliche Bedingungen von unterschiedlichen Versicherern

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Vertrauensschadenversicherung

- Schutz vor Vermögensschäden, die durch vorsätzliche Handlungen eigener Mitarbeiter ("Vertrauenspersonen") oder unternehmensfremder Dritter verursacht werden
- Ursprünglicher Zweck: Schutz vor Vermögensschäden durch strafbare Handlungen eigener Mitarbeiter („Vertrauenspersonen“) -> Vorsätzliche Innentäter
- -> Veruntreuung, Unterschlagung etc. durch Mitarbeiter
  -> Vertrauensschadensversicherung hat ursprünglich nichts mit Cyber-Angriffen zu tun

Vertrauensschadenversicherung

- Später wurden – in begrenztem Umfang - auch Schäden durch externe Dritte hinzugenommen -> also auch Außentäter
- In der Regel keine Deckung für fahrlässiges Handeln (z.B. fahrlässiger Fehler von Mitarbeiter)
- In der Regel:
  - Bei Schäden von Vertrauenspersonen Allversicherung
  - Bei Schäden von externen Dritten hingegen nur Deckung bei bestimmten definierten Straftaten, z.B. Hackerangriffe

Vertrauensschadenversicherung

- -> Hackerangriffe bei Vertrauensschadenversicherung oftmals gedeckt (in begrenztem Umfang)
- Aber: In der Regel keine Deckung mittelbarer Schäden -> entgangener Gewinn, Betriebsunterbrechung und Reputationsschäden sind in Vertrauensschadenversicherung meistens nicht versichert
- Bsp.: Hacker legt Unternehmen für eine Woche lahm -> Vertrauensschadenversicherung ersetzt zerstörte Hard- und Software, aber Cyberversicherung deckt Umsatzeinbußen

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

„Fake President Fraud“

- „Fake President Fraud“: Hacker gibt sich in der digitalen Korrespondenz fälschlicherweise als Chef aus
- „Fake President Fraud“ ist in der Regel kein Schaden der Cyberversicherung, sondern Vertrauensschaden
- Grund: Oft findet gar kein Cyber-Angriff statt, sondern Fälschung/Täuschung -> kein Fall der Cyber-Versicherung!
- -> Wird oftmals verwechselt, da beim „Fake President Fraud“ des Luftfahrtzulieferers FACC AG im Jahr 2016 in den Medien ein Cyber-Angriff kommuniziert wurde

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

8. Streitfrage Lösegeldversicherung

Streitfrage Lösegeldversicherung

- Anwendungsfall: Datenerpressung inklusive Lösegeld
- Lösegeldversicherung wurde früher als sittenwidrig angesehen
- Aber: Im Zusammenhang mit Cyber-Angriffen werden keine Personen entführt, sondern lediglich Daten erpresst
- Dennoch Problem: Erpresser wissen, dass Unternehmen zahlen, wenn sie eine entsprechende Versicherung haben -> Gefahr, dass Angriffsrisiko dadurch erhöht wird

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Streitfrage Lösegeldversicherung

- Lösegeldversicherung wurde von der FMA 2018 verboten und 2019 unter strengen Voraussetzungen wieder erlaubt
- -> Lösegeldversicherung derzeit also erlaubt, wenn bestimmte Voraussetzungen eingehalten werden (siehe unten)
- In ABC 2018 Lösegeldforderungen von Deckung ausgenommen (Art. 2 ABC 2018)

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Streitfrage Lösegeldversicherung

- Voraussetzungen für Zulässigkeit:
  - Für die Lösegeldversicherung darf nicht geworben werden
  - Darf nur im Rahmen einer Cyber-Versicherung gebündelt werden
  - Unterliegt strenger Geheimhaltung (max. 3 Personen dürfen Bescheid wissen)
  - Präventive Beratung durch ein Sicherheitsunternehmen
  - Anzeigepflicht Polizei und Abstimmung mit öffentlichen Stellen

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

9. DSGVO und Cyber-Versicherung

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

DSGVO und Cyber-Versicherung

- Art. 82 DSGVO: Anspruch auf Schadenersatz, wenn aufgrund eines DSGVO-Verstoßes ein immaterieller Schaden entstanden ist
- Drei neue EuGH-Entscheidungen zum immateriellen Schadenersatz, die potentiell auch Auswirkungen auf die Cyberversicherung haben
- -> Trend des EuGH, die Haftung von Unternehmen zu verschärfen

Neue EuGH-Judikatur

- Auch die berechtigte Angst vor einem möglichen Datenmissbrauch kann einen Anspruch auf Schmerzensgeld gem. Art. 82 DSGVO begründen
- Keine Erheblichkeitsschwelle -> auch bei Bagatellschäden kann ein Anspruch auf Schmerzensgeld bestehen
- Aber: Es muss einen tatsächlichen Schaden geben; ein rein hypothetisches Risiko der missbräuchlichen Verwendung von Daten kann nicht zu einer Entschädigung führen!

Auswirkungen auf Cyber-Versicherung

- Schadenersatzansprüche von Kunden für reine Vermögensschäden sind grundsätzlich in der Cyber-Versicherung gedeckt (Baustein Haftpflichtversicherung)
- Aber: Gilt immaterieller Schadenersatzanspruch als reiner Vermögensschaden? -> In Ö bisher nicht (OGH, 7 Ob 19/09h)
- -> Wäre demnach in ABC 2018 nicht gedeckt

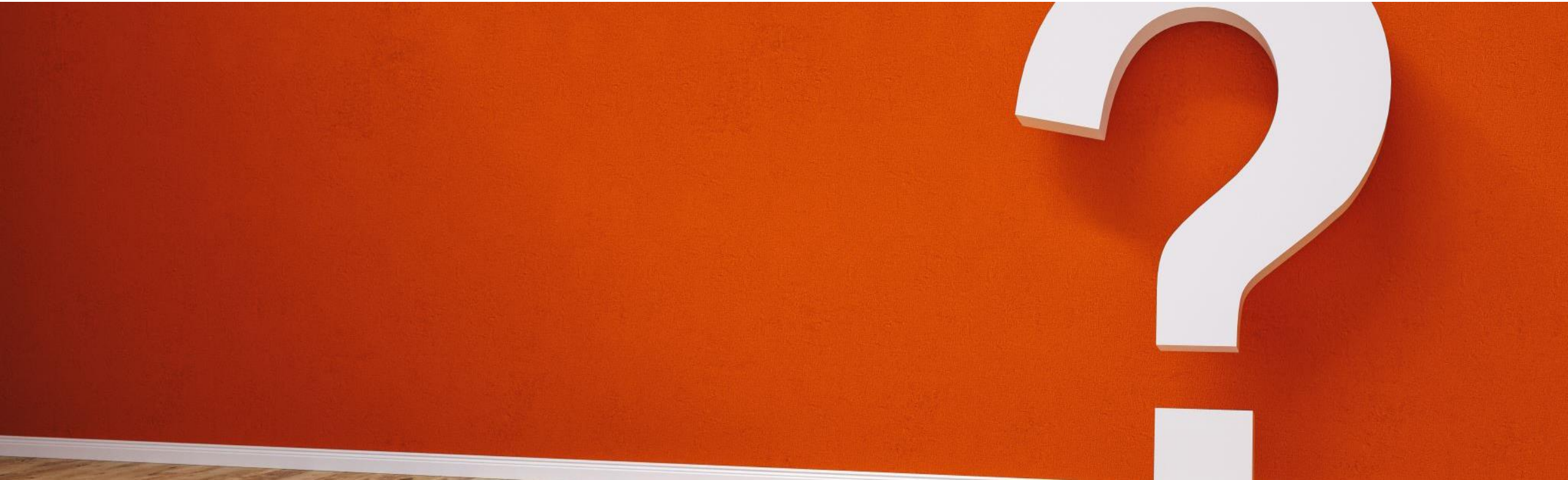
RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Auswirkungen auf Cyber-Versicherung

- -> Kann aber in Bedingungen bestimmter Versicherer gedeckt sein -> Hängt von konkreten Bedingungen ab
- -> In Zukunft wohl Bedarf an zusätzlicher, expliziter Deckung von immateriellem Schadenersatz
- Schadenersatzforderungen können in Millionenhöhe gehen, wenn Tausende Kundendaten entwendet werden und jedem Kunden Schadenersatz zusteht -> potentiell existenzbedrohend

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

FRAGEN?



RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Vielen Dank
für Ihre Aufmerksamkeit!

Literatur

RECHTSANWALTSKANZLEI
MAG. STEPHAN M. NOVOTNY

Promok, Lisa Katharina (Hrsg.): Cyberversicherung, facultas 2022

Cybercrime Report Österreich 2023 (BKA)

Studie „Cyber Security Österreich“ (KPMG)

Studie „Realitycheck: IT-Sicherheit im österreichischen Mittelstand“ (Techbold, What‘s next Insititute)