Cyber Solutions

Gehackt! – und was ist nun versichert?

LSZ Cyber Crime Forum, 18.06.2024

Agenda

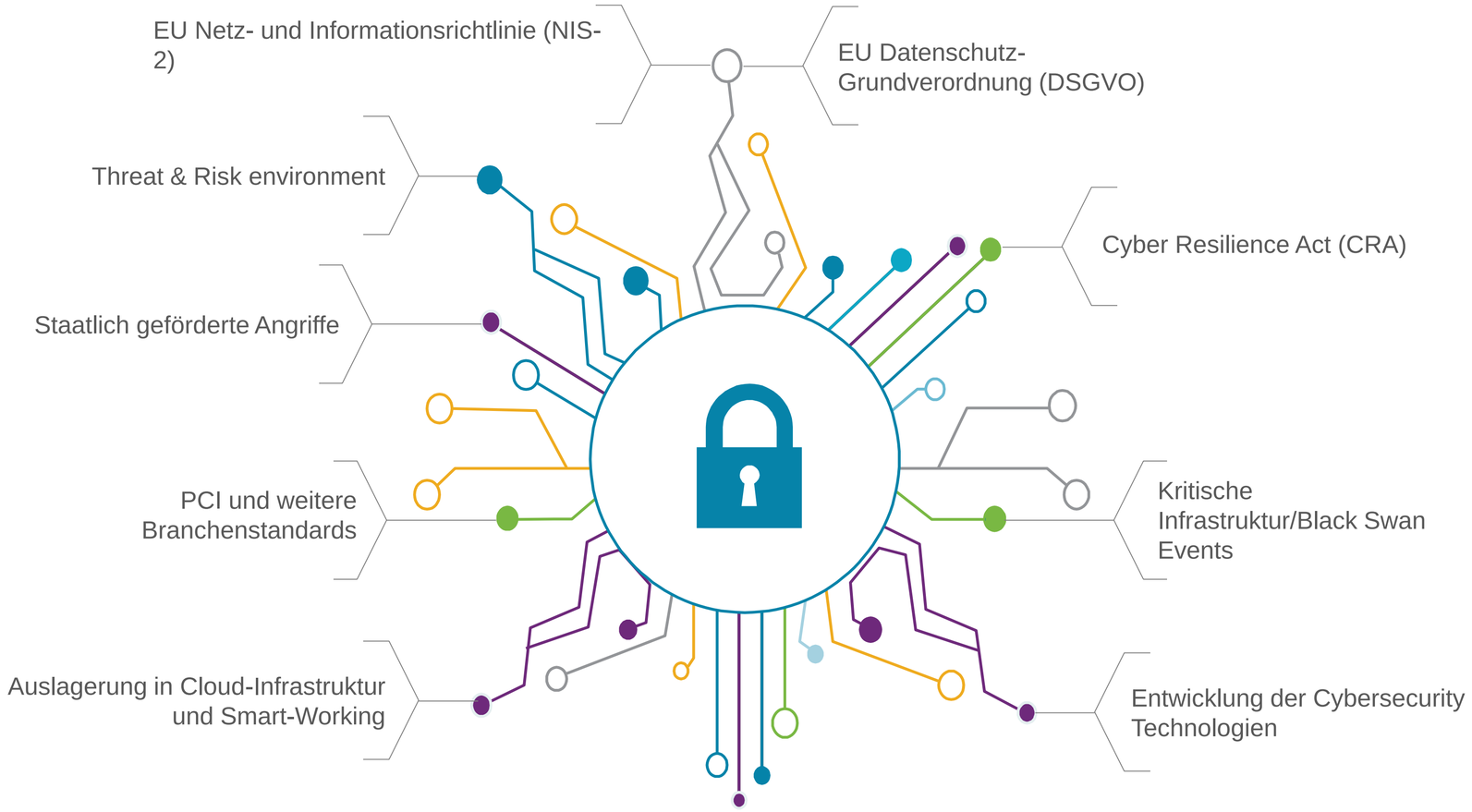
1. Überblick über die aktuelle Schadenlage
2. Aufbau und Umfang der Cyberversicherung
3. Cyber Schäden – Client Stories
4. Underwriting Kriterien & Kosten

1

Überblick über die aktuelle Schadenlage

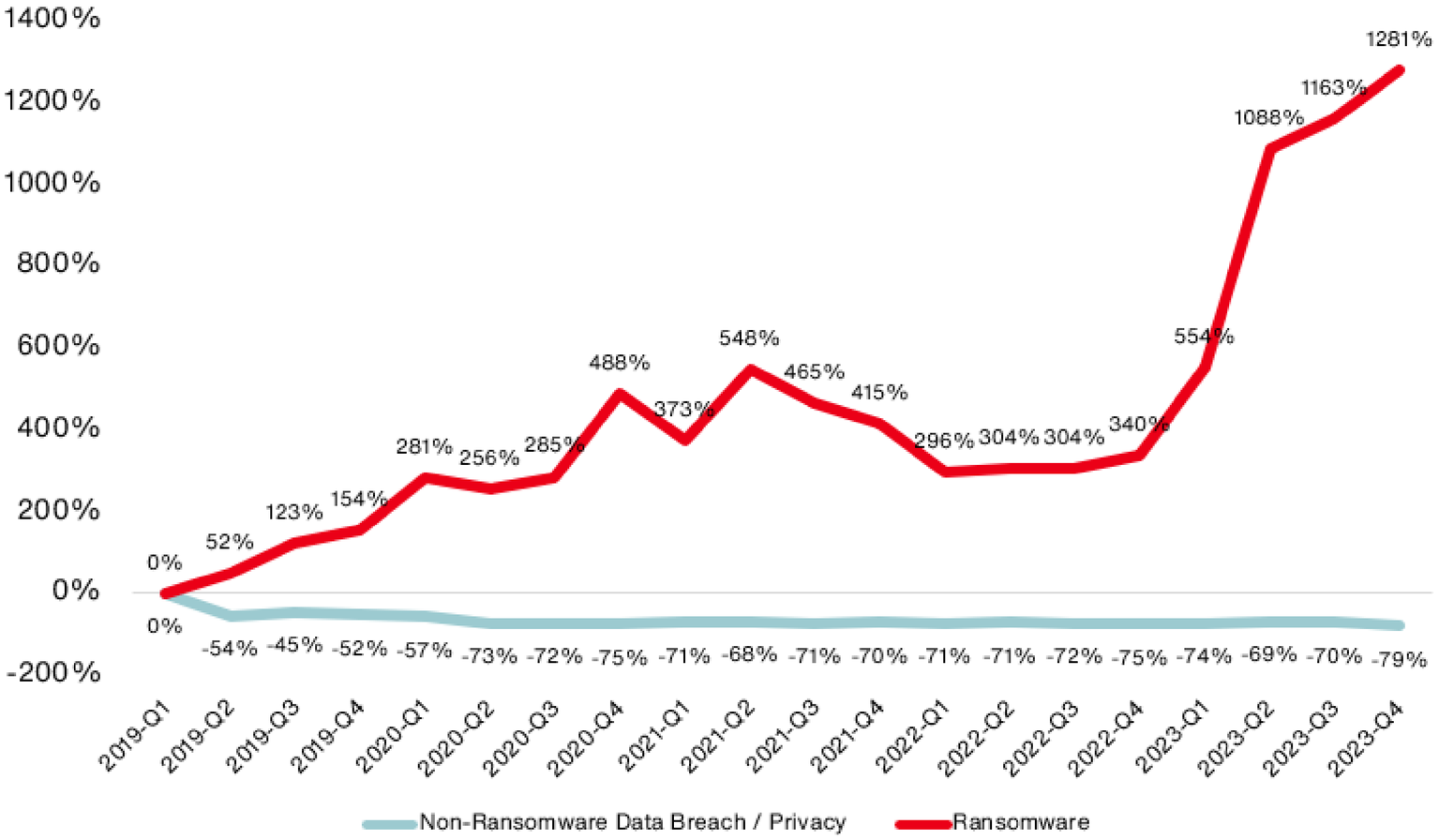
Komplexität der Cyber-Risikosituation

Mannigfaltige Faktoren tragen zu einer immer instabiler werdenden Risikolage bei. Risikomanager müssen unzählige Einfallstore für Cyber-Schäden im Auge behalten. Dabei sind neben Angriffen von außenstehenden Dritten auch weitere Faktoren zu beachten. Insbesondere die sich rasch entwickelnde Gesetzeslage stellt Unternehmen vor neue Herausforderungen.



- Unternehmerische und operative Konsequenzen
- Betriesbunterbrechung
- Finanzielle und immaterielle Schäden
- Manigfaltige Komplikationen bei der Durchsetzung von Versicherungsansprüchen
- Regulatorische Änderungen

Cyber Incident Rates von Q1 2019 – Q4 2023



Key Observations:

- Ransomware Aktivitäten steigen weiterhin
- **Ransomware Events sind um 1.281%** von Q1 2019 bis Q4 2023 gestiegen
- Im Vergleich zu Q3 2023:
  - Sind Ransomware Events um 9% gestiegen
  - Data Breach/Privacy Events sind um 32% gesunken
- Die am meisten betroffenen Industrien in Q4 2023 waren:
  - Dienstleister/Freiberuflich Tätige
  - **Herstellendes Gewerbe/Produktion**
  - Gesundheitswesen
  - Immobilien / Baubranche
  - Bildungseinrichtungen
  - Öffentlich-rechtliche Körperschaften

Source: Risk Based Security, analysis by Aon. Data as of 1/1/2024; Claim count development may cause these percentages to change over time

2

Aufbau und Umfang der Cyberversicherung

Versicherungsumfang im Detail

Datenlecks

Offenlegung, Verlust oder Beschädigung von Daten und Software

- Kosten für **IT-Forensik**
- Rechts- und PR-Beratung
- Anwaltliche Vertretung vor der **Datenschutzbehörde**
- **Benachrichtigungskosten**

Schadsoftware

Attacke der Systeme mit Schadsoftware bspw. Ransomware

- IT-Krisenberater
- **Lösegelder**
- Kosten für die **Datenwiederherstellung**
- Ersatz der Hardware
- **Systemverbesserungen**

Schadenersatz

Erhebung von Forderungen durch Dritte

- **Abwehr und Freistellung** von Schadenersatz-ansprüchen aufgrund von:
  - Datenschutzverletzungen
  - Geheimhaltungs-pflichtverletzungen
  - Weiterleitung von Schadsoftware

Cyber-BU

Unterbrechung des IT-Betriebs bspw. durch eine DDOS-Attacke od. Fehlbedienung

- **Mehrkosten** für die Auslagerung der IT und die **Fortführung** des Geschäftsbetriebs
- **Entgangener Gewinn**

Crime

Phishing, Social Engineering und Diebstahl

- **Finanzieller Schaden** durch
  - Hacking von Online-Konten
  - Voice-over IP
  - Cyber-Betrug

Nutzen der Cyber-Versicherung

24/7 Krisenreaktion

Mit der Cyber-Versicherung erhalten Sie Zugang zu einem umfangreichen **Krisenreaktionsnetzwerk**, auf welches Sie im Schadenfall zurückgreifen können

Rund-um-Schutz

Die Cyberversicherung versichert nicht nur Angriffe von außenstehenden Dritten sondern versichert auch Handlungen von **Innentätern**, mit Ausnahme der Repräsentanten.

Haftpflicht und Rechtsschutz

„Wo gehobelt wird, da fallen Späne“! Dieser Spruch gilt auch im digitalen Bereich, daher versichert die Cyber-Versicherung auch Haftpflichtschäden und die Kosten der rechtsfreundlichen Vertretung.

Cyberversicherung – Wesentliche Ausschlüsse

- **Personen- und Sachschäden** sind grds ausgeschlossen
- **Vorsatz u. wissentliche Pflichtverletzung** durch Repräsentanten ist ausgeschlossen
- **Hoheitliche Eingriffe** sind grundsätzlich ausgeschlossen, mit Ausnahme von Eingriffen der Datenschutzbehörde
- **Ausfall von Versorgungsleistungen** (z.B.: Strom) Dritter ist nicht versichert
- **Krieg und Cyberoperationen**, die als Teil eines Krieges ausgeführt werden
- **Operative Risiko** die mangelhafte Ausführung der betrieblichen Tätigkeit ist nicht versichert, selbst wenn die Mangelhaftigkeit durch einen Cyber-Angriff verursacht wurde.

3

Cyber Schäden – Client Stories

Sample Case Study 2

Lebensmittelproduzent wird Opfer eine Ransomware-Attacke

Der Kunde wurde Opfer einer Ransomware-Attacke, die zu einem Betriebsausfall in der Dauer von 1,5 Wochen geführt hat. Die vollständige Wiederherstellung aller Daten und Systeme hat über 2 Monate gedauert.

Der Angriff erfolgte mittels Double-Extortion-Ransomware, die Angreifer forderten sowohl für die Entschlüsselung als auch für die Geheimhaltung der offengelegten Daten ein Lösegeld in Höhe von mehreren Millionen Bitcoins.

In enger Abstimmung mit Aon und dem beteiligten Versicherer wurde ein Maßnahmenplan ausgebarbeitet und Stakeholder-Entscheidungen vorbereitet.

Aufgrund der schnellen und professionellen Krisenunterstützung durch den Versicherer war eine teilweise Aufrechterhaltung des Betriebes möglich. Die Lösegeldverhandlungen wurden von unabhängigen Verhandlern übernommen. Die Bezahlung eines Lösegeldes wurde auf Wunsch des Kunden unterlassen.

Die vollständige Wiederherstellung der Daten und Systeme hat über 2 Monate in Anspruch genommen.

Client / Insurer Roles Managed

11

Unternehmen/Rollen waren dauerhaft involviert

Data subjects affected

+60k

Anzahl der infizierten Datensätze

Cyber Insurance Claim Recovery

€5m +

Kosten für Incident Response, Datenwiderherstellung und Betriebsunterbrechungsschaden

Aon Cyber Loss Recovery Support

Quantifizierung und Vorfallsmanagement.

Unterstützung durch Cyber Claims Specialists

Sample Case Study 1

Global tätiges Life Science Unternehmen wurde Opfer einer Ransomware-Attacke

Ein globales Life-Science Unternehmen wurde Opfer einer Ransomware-Attacke. Die Betriebstätigkeit des Unternehmens inklusive der Produktion war für 2 Wochen teilweise unterbrochen.

Aufgrund der Diversität der IT-Infrastruktur mussten unzählige workstreams eingeführt werden, um die Fortführung des Produktionsbetriebes aufrechtzuerhalten und kritische Systeme so rasch wie möglich wiederherstellen zu können.

Die professionelle und rasche Kommunikation und Abstimmung mit der Versicherung in Bezug auf den Maßnahmenplan war ein essentielles Element und hat maßgeblich zu der reibungslosen Abwicklung des Schadenfalles beigetragen.

Aon hat dabei sowohl die Kommunikation zum Versicherer übernommen sowie den Klienten bei der Koordination der mannigfaltigen externen Dienstleister unterstützt. Zur Aufbereitung des Betriebsunterbrechungsschaden hat der Klient zudem das Forensic Accounting Team von Aon beauftragt.

Dies hat zu einer Versicherungsdeckung in Höhe von über EUR 80 Mio geführt.

Client / Insurer Roles Managed

18

Unternehmen/Rollen waren dauerhaft involviert

Insured Hours Committed

2500

Betriebsunterbrechungs- und Wiederherstellungszeitraum

Cyber Insurance Claim Recovery

€80m+

Gesamtschaden für Betriebsunterbrechung und Wiederherstellung

Aon Cyber Loss Recovery Support

Quantifizierung und Vorfallsmanagement.

Unterstützung durch Cyber Claims Specialists & Forensic Accountants

Worauf Sie achten müssen…..

- **Geeignetheit des Krisenberaters** hinterfragen Sie welche Krisenberater im Schadenfall für Sie tätig werden und ob diese die Maßgaben der NIS-2-Richtlinie kennen

- **Reaktionsgeschwindigkeit des Krisenberaters** vergewissern Sie sich, dass der Krisenberater unverzüglich für die Bearbeitung Ihres Schadensfalles zur Verfügung steht

- **Kontaktdaten des Krisenberaters** hinterfragen Sie, ob die in der Polizze angegebene Hotline-Nummer wirklich zu einem Krisenberater gehört oder ob dahinter ein Call-Center steht

- **Beweislastumkehr** stellen Sie sicher, dass die Beweislast im Schadenfall den Versicherer trifft

- **Versicherungsschutz für interne Kosten** stellen Sie sicher, dass auch interne Kosten vom Versicherungsschutz umfasst sind

- **Obliegenheiten** stellen Sie sicher, dass in den Versicherungsbedingungen keine Obliegenheiten in Bezug auf die IT-Sicherheit festgeschrieben werden

4

Underwriting Kriterien & Kosten

Cyberversicherung – Underwriting-Kriterien & Kosten

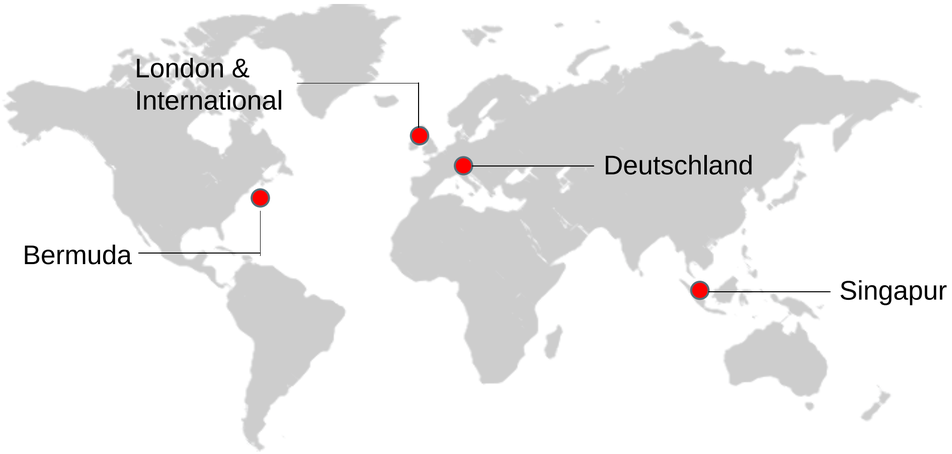
Multi-factor Authentication (MFA)	**Endpoint Protection & Response (EDR)**	**Phishing Exercise / Cyber Awareness Training**
Patch Management / Zero Day Vulnerability	**Secure RDP / VPN**	**Incident Response Plan / Ransomware Exercise**
Access Control / Service Account	**Disaster Recovery / Backups**	**Email Filtering**
Supply Chain Risk Management	**Network Segmentation / Network Monitoring (IT/OT)**	**M&A Due Diligence & Integration**

Versicherungs-summe	**Umsatz**		
	bis EUR 50 Mio	bis EUR 100 Mio	bis EUR 250 Mio
EUR 5 Mio	**EUR 7.600,00 – 8.800,00**	**EUR 22.800,00 – EUR 31.000,00**	**EUR 47.800,00 – EUR 60.000,00**
Die oben dargestellten Prämien stellen Nettoprämien (exkl. der VSt iHv 11%) dar. Die dargestellten Prämien sind Beispielprämien und stellen keine verbindlichen Angebotsprämien dar.			

Marktüberblick

Internationale Cyber-Märkte

Im Bereich der Cyberversicherung bietet aktuell der deutsche Markt die attraktivsten Lösungen, insbesondere auch für den Aufbau einer Programmstruktur. Weitere Kapazitäten können bei Bedarf am Londoner Markt angefragt werden. Darüber hinaus können beim Aufbau bedeutender Deckungstürme auch Kapazitäten auf den asiatischen und bermudischen Märkten genutzt werden, um die Wettbewerbs-fähigkeit zu erhöhen und optimale Kapazitätsraten zu erzielen.



+ 21

Anzahl der Risikoträger in Österreich

Die Anzahl der den österreichischen Versicherungsmarkt bedienenden Risikoträger steigt weiterhin an und liegt derzeit bei über 21 Anbietern, die entweder eine Grundvertrags- oder eine Exzedent-Deckung anbieten.

Ich freue mich auf einen Austausch mit Ihnen!

Mag. Kerstin Keltner
Director Financial Lines & Cyber

t +43 676 830 425 337
kerstin.keltner@aon-austria.at