DAV/DGVFM
Herbsttagung
2024

Dr. Leonie Ruderer, R+V Re; Jonas Becker, Munich Re

Cyberschäden – ob böswillig oder nicht - Taxonomie und RDS

Herbsttagung DAV, 18.11.2024, Mannheim

DAV Deutsche Aktuarvereinigung e.V.

DGVFM Deutsche Gesellschaft für Versicherungs- und Finanzmathematik e.V.

Agenda

1. Vorstellung der Arbeitsgruppe
2. Cyber Schaden-Taxonomie
3. RDS Ransomware
4. Ausblick

DAV Deutsche Aktuarvereinigung e.V.

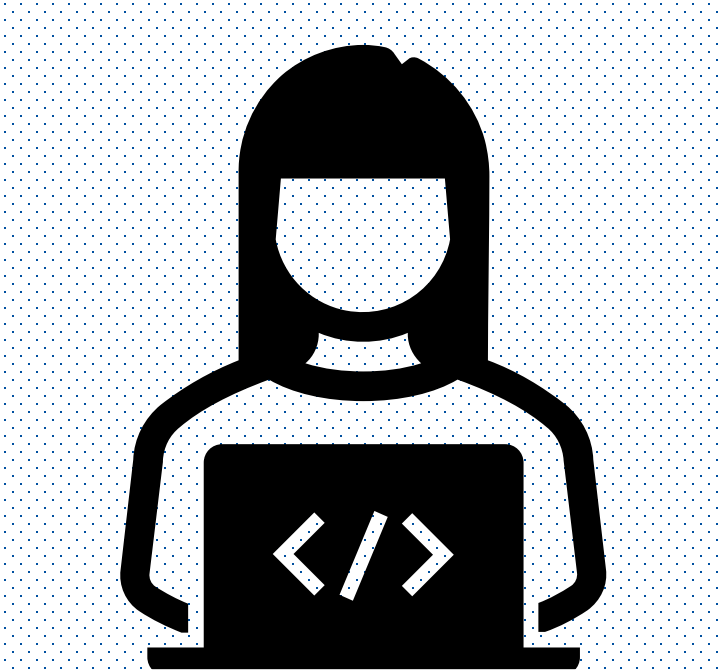
DGVFM Deutsche Gesellschaft für Versicherungs- und Finanzmathematik e.V.

AG Cyber

DAV Arbeitsgruppe „Daten und Methoden zur Bewertung von Cyberrisiken“

Veröffentlichungen:

- Juli 2020 – „*Daten und Methoden zur Bewertung von Cyberrisiken“*
- Juni 2022 – „*Cyberrisiken – Herausforderungen und Einfluss auf das Risikomanagement von Versicherungsunternehmen“*
- November 2022 – „*Use Case zur Modellierung (Beispielportefeuille, Modellansätze inkl. Programmierung)“*



DAV Deutsche Aktuarvereinigung e.V.

DGVFM Deutsche Gesellschaft für Versicherungs- und Finanzmathematik e.V.

Schaden-Situation – Ransomware & mehr

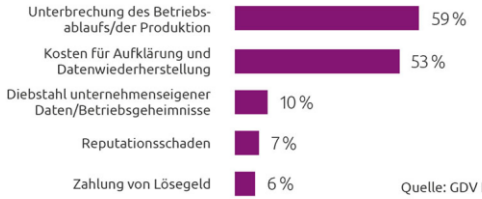
Cybersicherheit

Mehr Cyberschäden – Prävention wichtiger denn je

Die IT-Bedrohungslage in Deutschland hat sich zuletzt verschärft. Das spüren auch die Cyberversicherer. Die Schäden sind 2023 deutlich gestiegen und zehren die Prämieneinnahmen fast vollständig auf.

DIE SCHÄDEN

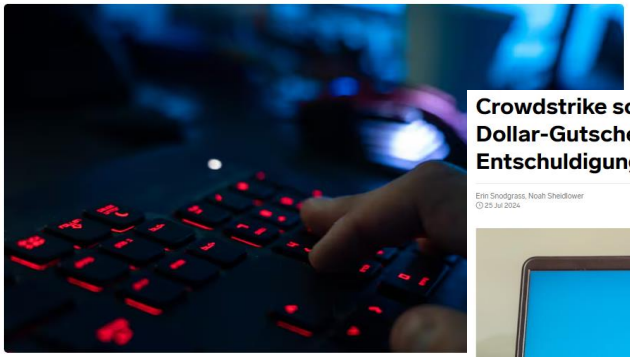
Die Attacken führten zu wirtschaftlichen Schäden durch ...[1]



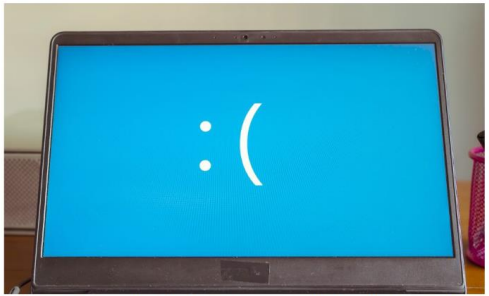
Quelle: GDV Forsa-Umfrage

Wachsende Gefahr durch Cyberkriminalität

Lagebericht: Mehr Opfer von Datenleaks durch Erpressersoftware-Angriffe



Crowdstrike schickt seinen Partnern 10-Dollar-Gutscheine für Uber Eats – als Entschuldigung für den massiven IT-Ausfall



Laut CrowdStrike war ein „Fehler" in einem Update für Windows für den massenhaften Ausfall der Technik in der vergangenen Woche verantwortlich. ©Wachwit

Quellen: GDV, RND/BSI, Business Insider

Was sind die relevanten Schadeninformationen und wie können wir diese klassifizieren?

Schaden-Taxonomie: Kriterien für Umsetzbarkeit

Anwendbarkeit	• Die Taxonomie sollte einfach sein im Sinne der Anwendbarkeit für ihrer Nutzer
Eindeutigkeit	• Für auf der Taxonomie aufbauende Analysen benötigt es eindeutige Zuordnungen
Stabilität	• Insbesondere wichtig für Identifikation von Trends (häufige Änderungen unerwünscht)
IT-Umsetzung	• Die Klassifizierung muss in die IT-Infrastruktur der Versicherer umgesetzt werden können
Aktuarielle Anforderungen	• Die Taxonomie sollte die Anforderungen der verschiedenen aktuariellen Bereichen (bspw. Pricing, Reservierung, Risikomanagement, Rückversicherung) bedienen.

DAV Deutsche Aktuarvereinigung e.V.

DGVFM Deutsche Gesellschaft für Versicherungs- und Finanzmathematik e.V.

Schaden-Taxonomie: Bestehende Ansätze

Cyber-Sicherheitsstandards / nicht aus dem Versicherungsmarkt

- Mitre Att&ck (technische Taxonomie)
- VERIS Framework („Vocabulary for Event Recording and Incident Sharing")

Standards aus dem Versicherungsmarkt

- CRO-Forum (Ereignis-Datenbank)
- GDV (Meldeanleitung)

Ziel: Verbindung der technischen Sicht und der Versicherungskonditionen

DAV Deutsche Aktuarvereinigung e.V.

DGVFM Deutsche Gesellschaft für Versicherungs- und Finanzmathematik e.V.

Vorschlag für Taxonomie – „Art des Vorfalls“

Cyber
Bösartige Cyber-Attacke (Ransomware / mit Lösegeld verbunden)
Bösartige Cyber-Attacke (ohne Lösegeld, ohne BEC und FTF)
Technischer / menschlicher Fehler (ohne externen Akteur, ohne Systemausfall)
Finanzieller Schaden: “Business Email Compromise” (BEC) / “Funds Transfer Fraud” (FTF)
Systemausfall
Dienstleister Vorfall/Ausfall
“Non-Tech” Dienstleister Vorfall/Ausfall
DDoS
Andere (bitte benennen)

„Nicht-Cyber“ Deckungen
Verstoß gegen regulatorische Datenschutz-Anforderungen (bspw. unrechtmäßige Erhebung und Sammlung von Daten)
Medienhaftpflicht
Tech E&O
Weitere Haftpflicht (bspw. für Dienstleistungen oder Produkte)

DAV Deutsche Aktuarvereinigung e.V.

DGVFM Deutsche Gesellschaft für Versicherungs- und Finanzmathematik e.V.

Vorschlag für Taxonomie – „Schadenkonsequenz“

Schadenkonsequenz							
Betriebsunter-brechung	Datenschutz-verletzung	Regulatorische Konsequenzen	Rechtsstreit (inkl. Sammel-klage)	Rechtsstreit (exkl. Sammel-klage)	Reiner finanzieller Schaden	Erpressungs-geld	Weitere

DAV Deutsche Aktuarvereinigung e.V.

DGVFM Deutsche Gesellschaft für Versicherungs- und Finanzmathematik e.V.

Vorschlag für Taxonomie

Type of Incident		Loss Consequence							
		Business Interruption	Data Breach	Regulatory Action	Class Action litigation	None Class action Litigation	Pure Financial Loss	Ransom demand paid	Other
Cyber	Malicious cyber attack (Ransomware or other ransom demand)	yes/no/unknown	yes/no/unknown	yes/no/unknown	yes/no/unknown	yes/no/unknown	yes/no/unknown	yes/no/unknown	yes/no/unknown
	Malicious cyber attack (without ransom demand, excl. BEC and FTF)	yes/no/unknown	yes/no/unknown	yes/no/unknown	yes/no/unknown	yes/no/unknown	yes/no/unknown		yes/no/unknown
	Accidental/ human error (without external actor) / System Failure	yes/no/unknown	yes/no/unknown	yes/no/unknown	yes/no/unknown	yes/no/unknown	yes/no/unknown		yes/no/unknown
	Financial loss: Business Email Compromist (BEC) / Funds Transfer Fraud (FTF)			yes/no/unknown	yes/no/unknown	yes/no/unknown	yes/no/unknown		yes/no/unknown
	Service Provider Incident/ Failure (e.g. cloud providers etc.)	yes/no/unknown	yes/no/unknown	yes/no/unknown	yes/no/unknown	yes/no/unknown			yes/no/unknown
	Non-Tech Provider Incident/ Failure (e.g. supplier of manufacturing parts etc.)	yes/no/unknown	yes/no/unknown	yes/no/unknown	yes/no/unknown	yes/no/unknown			yes/no/unknown
	DDoS	yes/no/unknown		yes/no/unknown	yes/no/unknown	yes/no/unknown			yes/no/unknown
	Other (please specify)	yes/no/unknown	yes/no/unknown	yes/no/unknown	yes/no/unknown	yes/no/unknown	yes/no/unknown		yes/no/unknown
Non-Cyber Event Coverages	Breach of regulatory requirements on data (e.g. wrongful collection)		yes/no/unknown	yes/no/unknown	yes/no/unknown	yes/no/unknown			yes/no/unknown
	Media liability			yes/no/unknown	yes/no/unknown	yes/no/unknown			yes/no/unknown
	Tech E&O			yes/no/unknown	yes/no/unknown	yes/no/unknown			yes/no/unknown
	Other liability (e.g. liability on services provided or product supplied)			yes/no/unknown	yes/no/unknown	yes/no/unknown			yes/no/unknown

Möglichst eindeutige Sicht auf die Art des Vorfalls sowie Zuordnungen zu den kritischen Schadenkonsequenzen

Beispiel einer Taxonomie-Zuordnung (1)

Schadenvorfall:

- Cyberangriff auf ein Klinikum mit dem Versuch ein Lösegeld zu erpressen
- Neuaufsetzung der IT-Systeme, auf Lösegeldforderung wird nicht eingegangen
- Abfluss von Patientendaten
- Digitale Prozesse auf einen „Analogbetrieb" umgestellt (Terminvergaben und Wartelisten nicht mehr elektronisch)

Taxonomie-Zuordnung – Art des Vorfalls:

- Bösartige Cyber-Attacke (Ransomware / mit Lösegeld verbunden)

Taxonomie-Zuordnung – Schadenkonsequenz:

- Ja: Betriebsunterbrechung, Datenschutz-verletzung
- (noch unbekannt): Regulatorische Konsequenzen und Rechtsstreit inkl. Massenklage möglich

Quelle: Cyberangriff: Kliniken Mittelfranken verhandeln nicht, Neustart der Systeme | heise online

Beispiel einer Taxonomie-Zuordnung (2)

Schadenvorfall:

- Ein unbekannter Dritter hat sich Zugriff zum System des Versicherten besorgt.
- Die hinterlegten Zahlungsmodalitäten des PayPal-Accounts wurden geändert und in einem Zeitraum wurden auf diese Weise 123.456 € an Umsatz aus dem Onlinegeschäft des Versicherten entwendet

Taxonomie-Zuordnung – Art des Vorfalls:

- Finanzieller Schaden: “Business Email Compromise” (BEC) / “Funds Transfer Fraud” (FTF)

Taxonomie-Zuordnung – Schadenkonsequenz:

- Ja: Reiner finanzieller Schaden

DAV/DGVFM
Herbsttagung
2024

Umfrage

Kommen RDS in Ihrem Unternehmen zum Einsatz?

RDS Szenario Malware - Einordnung

- Der Einsatz von Random Disaster Scenarios ist in Cyber verbreitet.

Malware

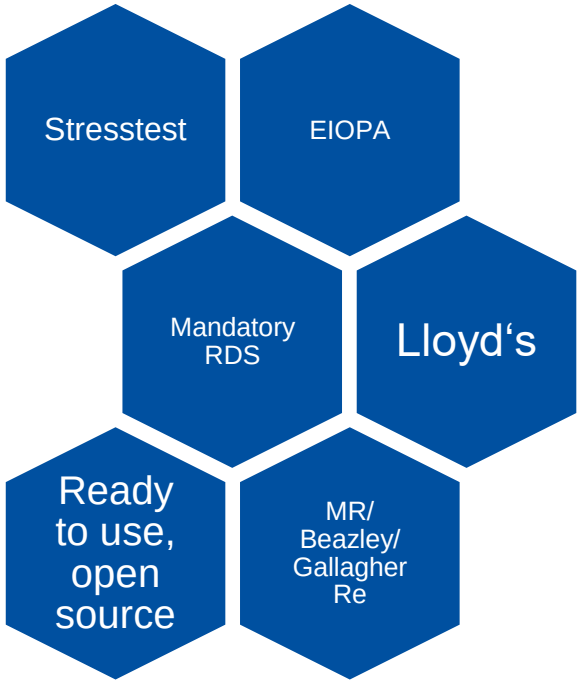
Cloud Outage

Data Theft

Power Outage

…

- Komplexität von Cyber erschwert Schätzung durch probabilistische Modellierung
- Szenarioanalysen ermöglichen schnelle Anpassungen
- Prospektives Arbeiten und Berücksichtigung hypothetischer Szenarien sind möglich



RDS Szenario Malware - Narrativ

- Verwendet wird das Narrativ der EIOPA (verkürzt wiedergegeben)

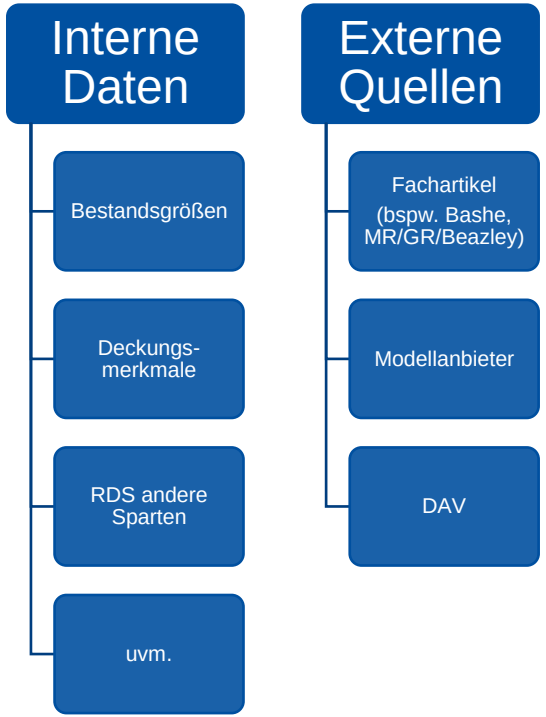
A ransomware attack targeting the employees' computers via phishing or the data center itself through some software vulnerability, encrypts the computers and spreads all through the organization and triggers the disconnection of the unaffected offices in order to avoid infection.

It will be technically impossible to recover encrypted information without decryption key. The victim cannot be certain that this key is provided even in the case that a ransom payment is made, therefore in the context of this scenario, the encrypted data is considered destroyed for all practical purposes.

This attack may include threat of public disclosure of sensitive data and/or client data in which cases the scenario would also include dealing with the GDPR national authority.

RDS Szenario Malware - Datengrundlage

- Schadendaten
- Taxonomie, Datenintegrität
- Aktualität, Repräsentanz



RDS Szenario Malware - Berechnung

Infektionsrate

- Die Infektionsrate $\lambda_{i,j}$ gibt an, mit welcher Wahrscheinlichkeit ein Risiko infiziert wird.

Schadenhöhe

- Die Schadenhöhe $l_{i,j}$ hängt von der Länge des Ausfalls ab: $l_{i,j} = \frac{j \cdot pm_{i,j}}{360} \cdot Duration \cdot d_i$
- Zusätzliche Kosten werden als proportional angenommen: $c_{i,j} = \frac{l_{i,j}}{(1-f_j)} - l_{i,j}$

Ransom Zahlung

- Die erwartete Zahlung ist gegeben durch $rp_{i,j} = rv_{i,j} \cdot pr_{i,j}$.

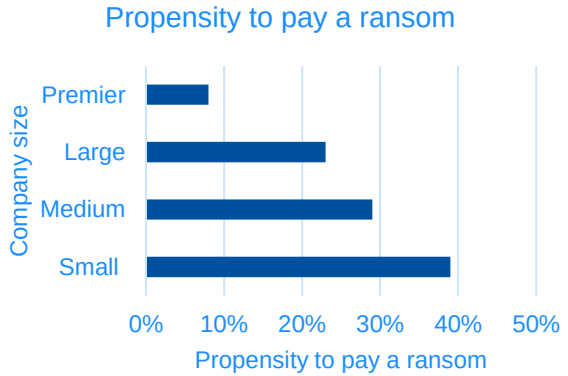
RDS Schaden

$$RDS_k = \lambda_{i,j} \cdot min\left(limit_k, \max\left(0, l_{i,j} + c_{i,j} + rp_{i,j} - deduction_k\right)\right);\ RDS = \sum_k RDS_k.$$

k Risiken; i: Industriesektor des Risikos; j: Größe des Risikos (bspw. per Umsatz); pm_i,j: Profit Margin; d_i: Abhängigkeit von IT-Systemen; rp_i,j; Ransom Payment; rv_i,j: Ransomwert; pr_i,j: Wahrscheinlichkeit zu zahlen

RDS Szenario Malware – Bsp. Parametrisierung

- **Infektionswahrscheinlichkeit** λ_i,j: Datengrundlage Fachartikel Bashe Attack Scenario X1 (schweres Szenario, ungefähr 95 % Quantil) → Sector-spezifische Infektionsrate liegt zwischen 3 % - 21 %, mittlere Infektionsrate liegt bei 9%
- **Wahrscheinlichkeit, eine Ransomzahlung zu leisten**: Fachartikel Bashe Attack → Modellierung mit dem Wert 10% unter der Annahme, dass dies keinen Einfluss auf die BU-Dauer haben wird.



Bashe attack: Global infection by contagious malware. CyRim Report 2019; Cambridge Center for Risk Studies; 2019;

RDS Szenario Malware – Parametrisierung

Summary Overview of the shocklevels set for the ransomware scenario

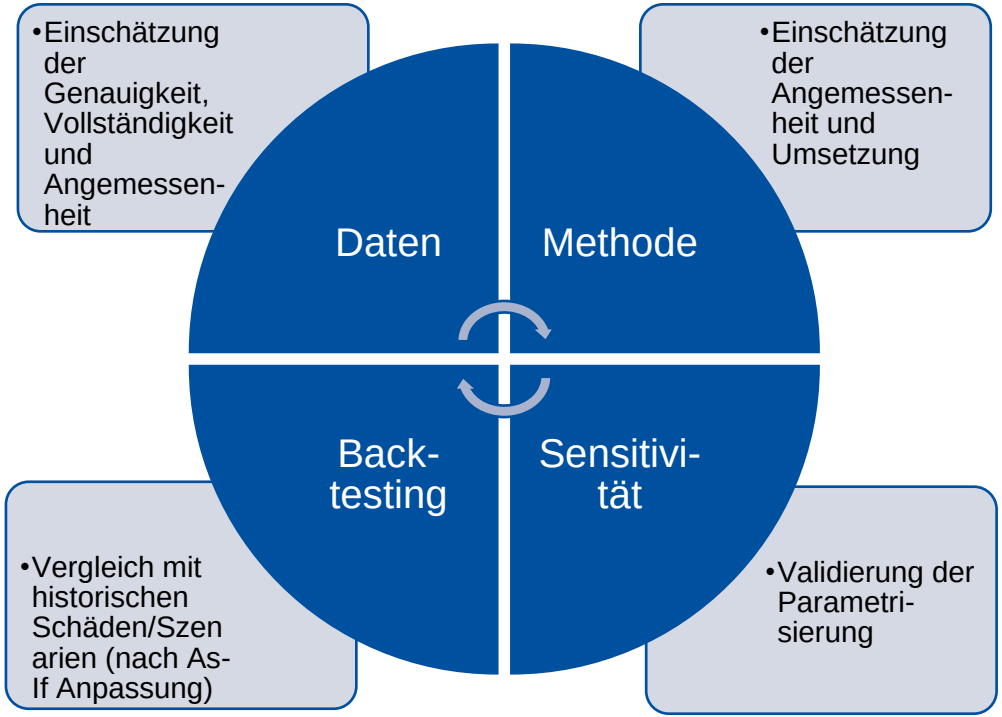
Shock	**Shocklevel**
Infection rate	Average 9%
Propensity to pay a ransom	10%
Amount of ransom	• 20.000 EUR for each policyholder
Duration	ten days
Loss in profit	30% gross profit margin on revenue
Cost per claim	• 100% of BI-loss for risks with less than 10 Mio. EUR revenue • 67% of BI-loss for risks with more than 10 Mio. EUR revenue

Ergebnis

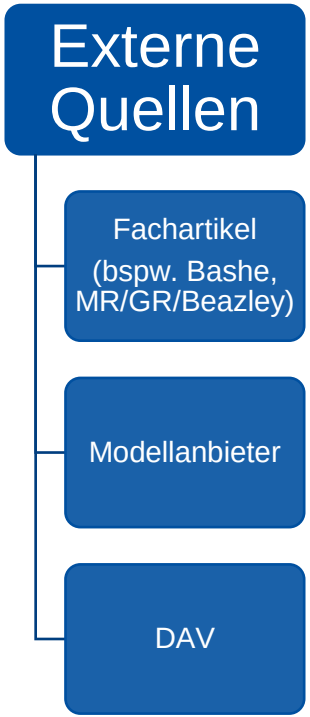
- Für ein gut diversifiziertes Beispielbuch mit 10-14 Mio. Prämie eines deutschen Versicherers mit ca. 5000 Risiken ergeben sich:

21.2 Mio. €	151-212%
Gesamtschaden	Schadenquote

RDS Szenario Malware - Validierung



Erinnerung:



Ausblick

2024/Anfang 2025

- Veröffentlichung Ergebnisbericht RDS
- Veröffentlichung Ergebnisbericht Taxonomie

2025

- Reservierungsmethoden/Abwicklungs-verfahren für Cyberschäden, Basisschadenschätzung
- Ereignismodellierung
- uvm.

Interesse geweckt? Sprechen Sie uns an!

Datenspende

- Kein Interesse mitzuarbeiten aber die Sache erscheint unterstützenswert?

→ Unterstützen Sie uns mit einer Datenspende!

Kontakt

Dr. Leonie Ruderer

R+V Versicherung AG - Rückversicherung
Front Office
Portfolio Undewriter Cyber

Leonie.Ruderer@ruv.de

https://www.linkedin.com/in/leonie-ruderer-486b9928b/

Jonas Becker

Cyber Underwriting Actuary
Europe & Latin America

jgbecker@munichre.com

https://www.linkedin.com/in/jonas-becker-9a76a67a/