



Unterschätzte Gefahr?



Cyberangriffe auf Lieferketten

PizzaSeminar 19.08.2021

Esther Kern & Alexander Szanto

Agenda

Bedrohungsakteure (CTA)

Definition (CSCA)

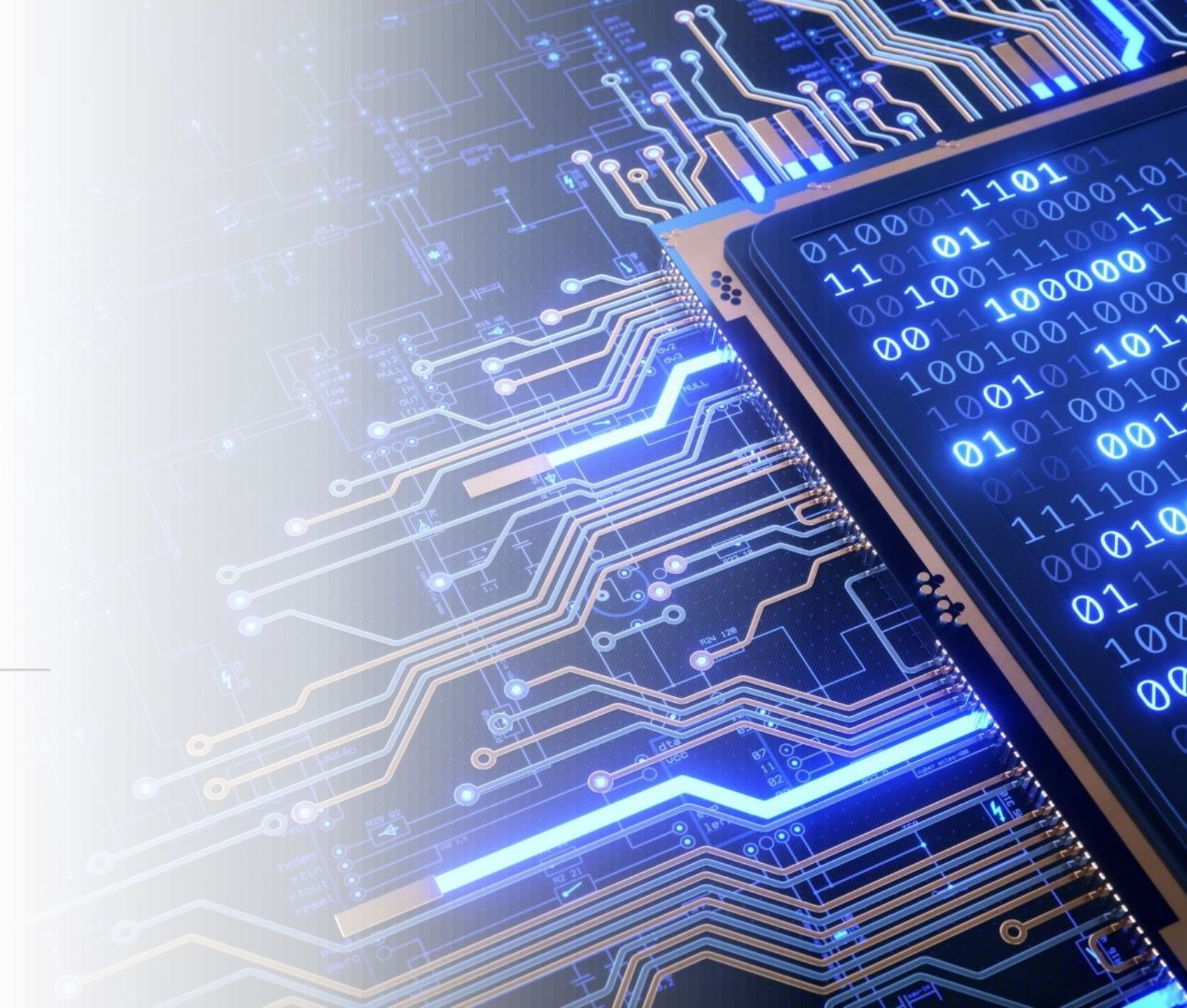
Event Study

Fallstudien

Vorläufige Erkenntnisse



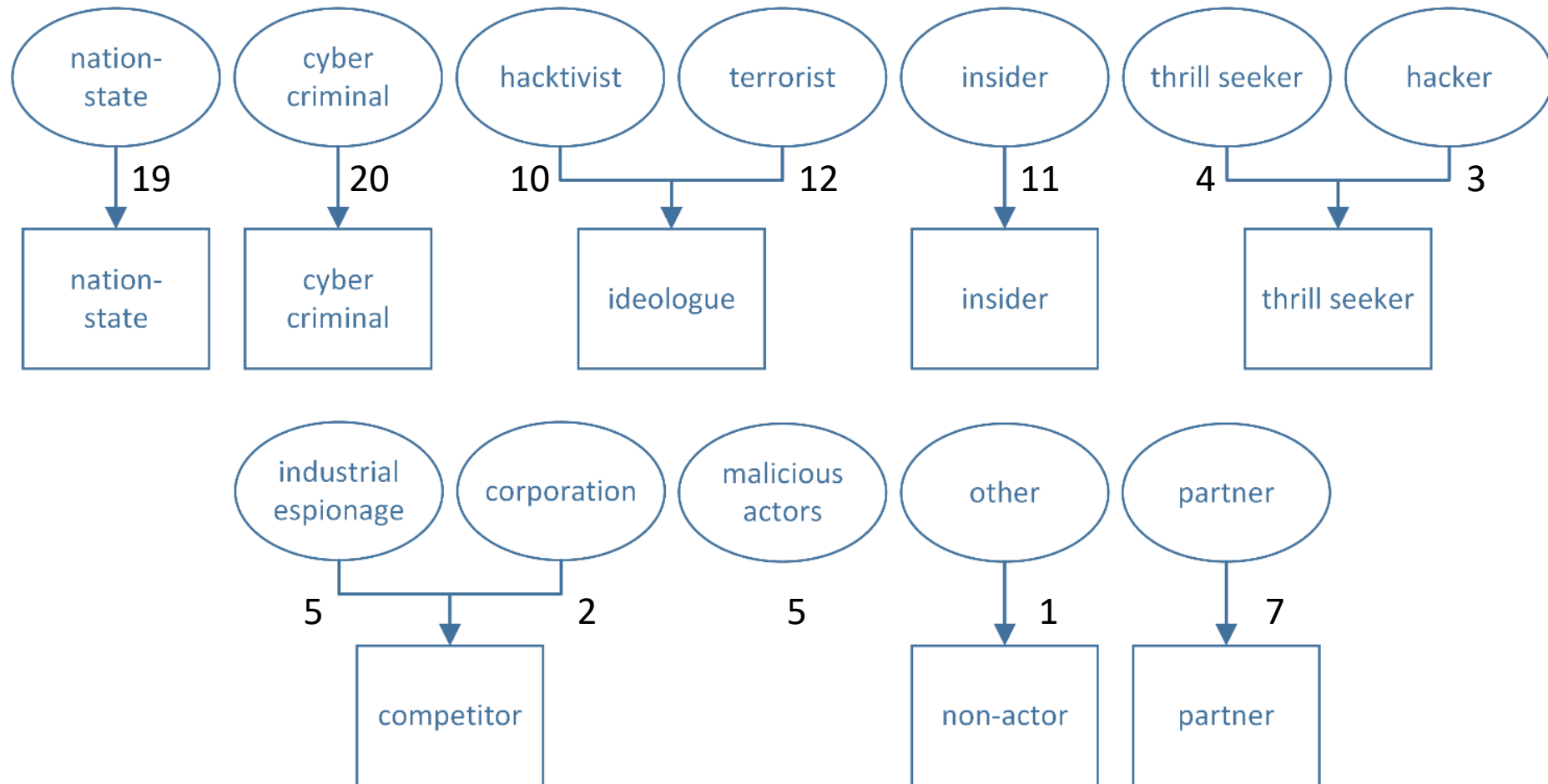
Cyber Threat Actors (CTA)



CTA für die Fabrik der Zukunft (FoF)

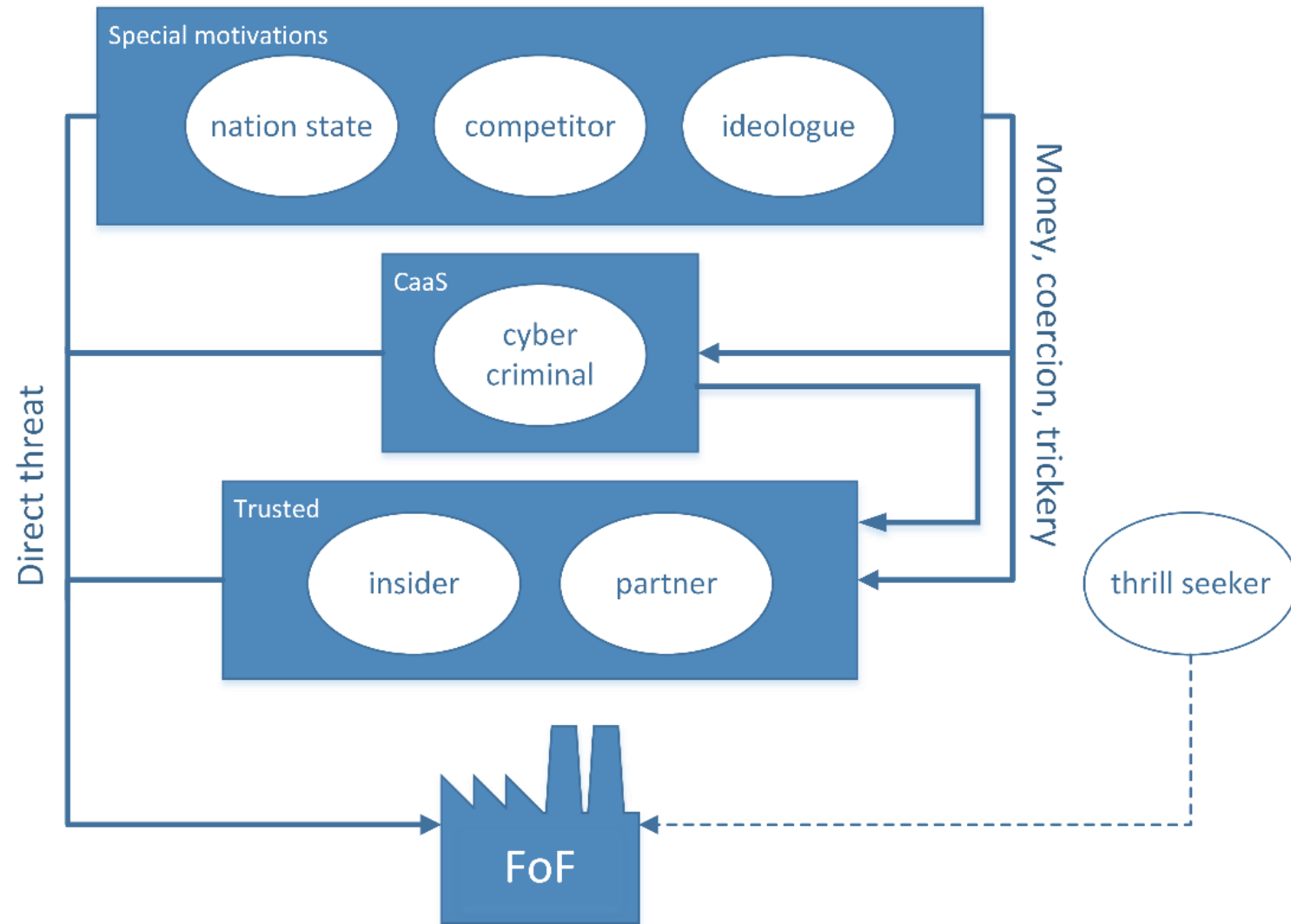
- ❑ Konnektivität, flexible Automatisierung, Kollaboration, *Intelligence*
- ❑ Identifizierung von Bedrohungsakteuren als Grundvoraussetzung für eine robuste Cyberabwehr
- ❑ Keine einheitliche Definition
- ❑ Tendenz sich eher auf quantitative (Anzahl der Erwähnungen von Bedrohungsakteuren in Berichten) und nicht auf qualitative Faktoren (Wettbewerbsanalyse) zu beziehen

Klassifikation von CTA



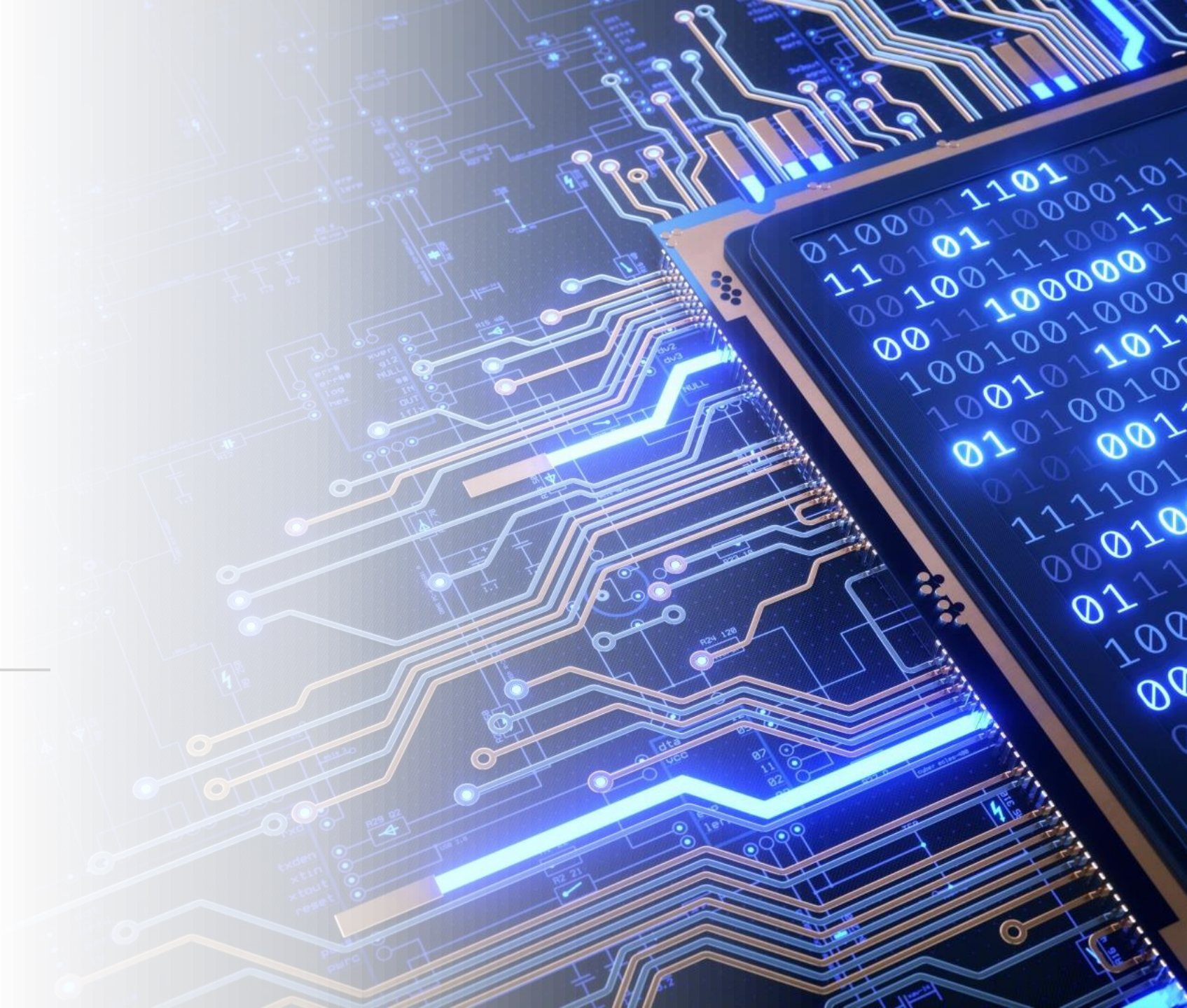
Hierarchie der Bedrohungsakteure

- ❑ Die CTAs an der Spitze der Hierarchie nutzen andere Akteure als Bedrohungsvektoren
- ❑ Kriminelle können angeheuert werden (CaaS), und vertrauenswürdige Akteure können bestochen, genötigt oder getäuscht werden.
- ❑ Thrill seekers stellen nur eine geringe Bedrohung für das FoF-Umfeld dar.



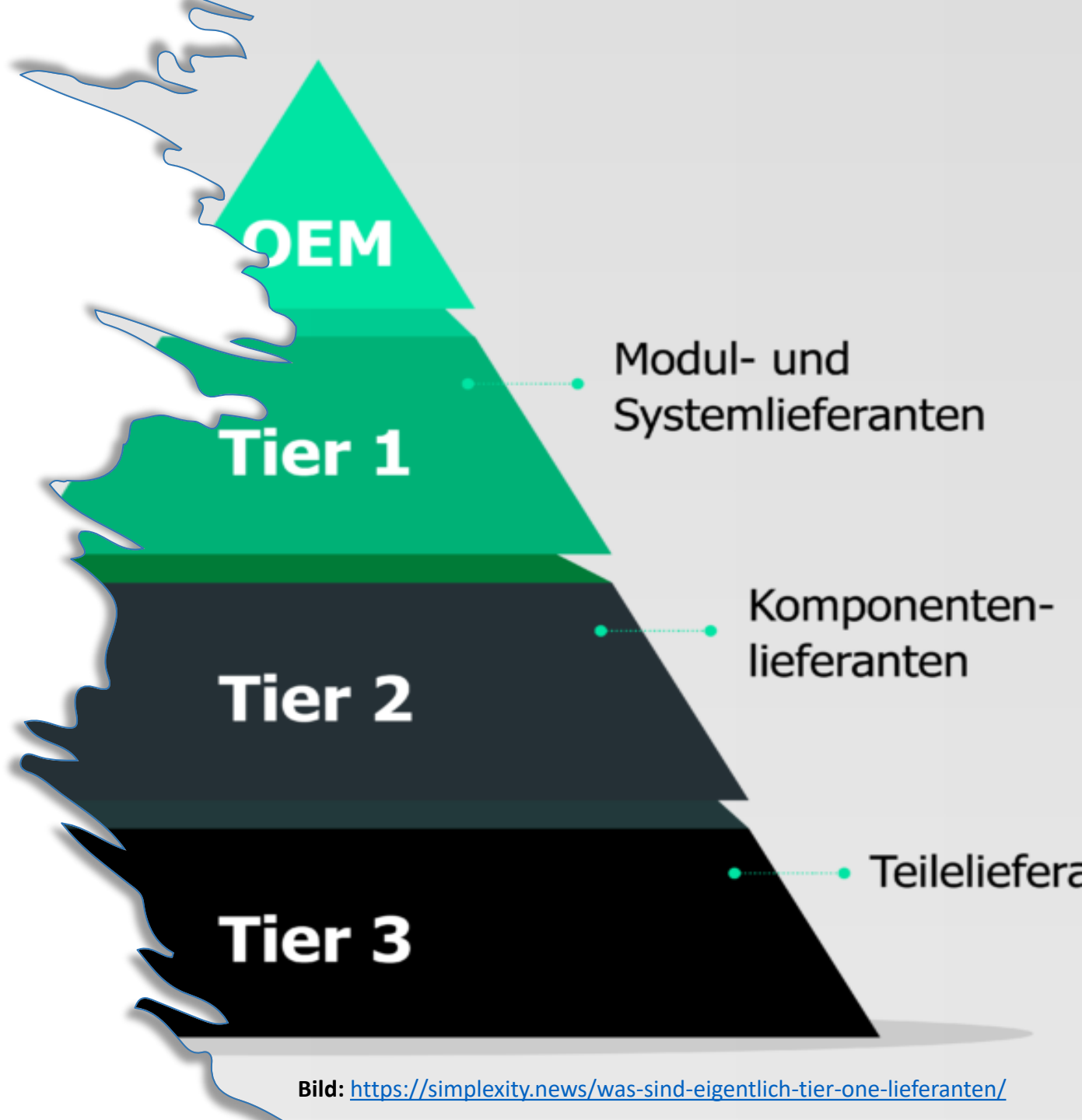


Definition (CSCA)



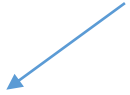
Definition von Cyberangriffen auf Lieferketten

Cyber Supply Chain Attacks (CSCAs) are threats that make use of trusted channels (external tiers, goods, and data) in the supply chain in order to compromise the final target particularly via operational endpoint-vulnerabilities. Furthermore, CSCAs in a broader sense are threats that directly impair operations at different points along the supply chain (e.g. production, distribution, logistical operations from Tier 1 to Tier 3).



Definition von Cyberangriffen auf Lieferketten

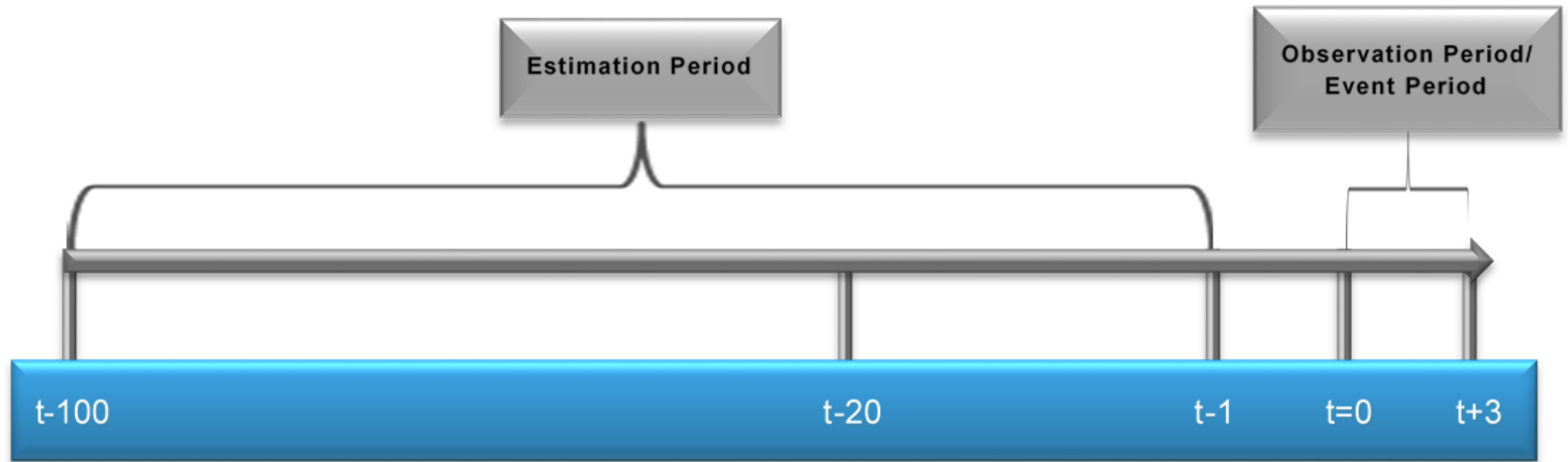
Targeted Attacks vs. Collateral Damages

- 
- ❑ Zielunternehmen werden nicht direkt, sondern über **"trusted third-parties"** angegriffen, welche Zugang zum Zielnetzwerk haben
 - ❑ Ausnutzen von Verbindungen durch bsp. Software zwischen externen Unternehmen und dem Zielunternehmen sowie den (potenziellen) geringeren Sicherheitsstandards bei Dritten

- 
- ❑ Kein spezifisches Zielunternehmen, sondern Cyberangriffe, die die Infrastruktur von Lieferketten und den steigenden Grad der Verflechtungen zwischen Unternehmen ausnutzen, um u.a. Schadsoftware so weit wie möglich zu verbreiten und somit die Angriffsfläche so groß wie möglich zu machen



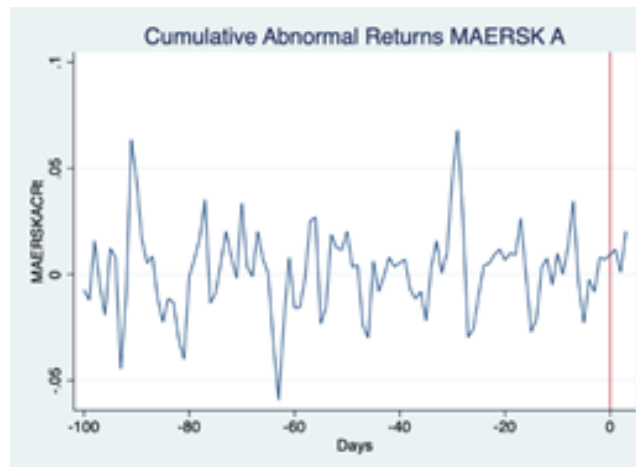
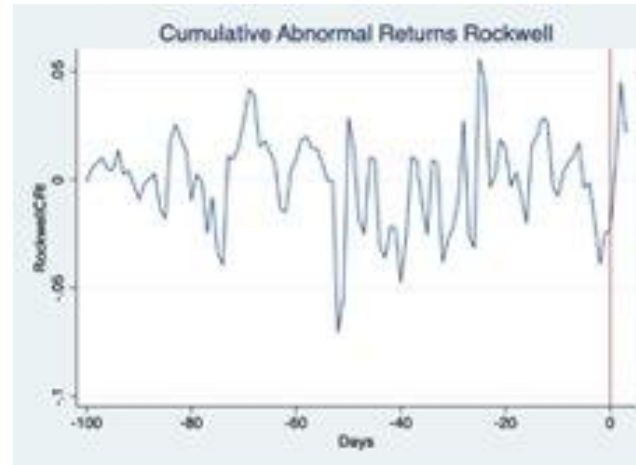
Event Study (Ereignisstudie)



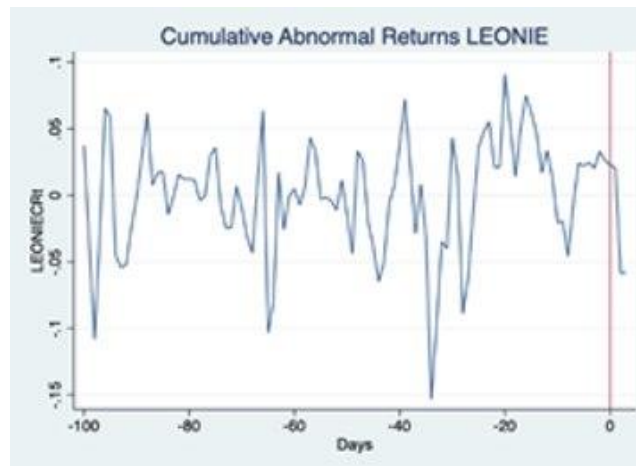
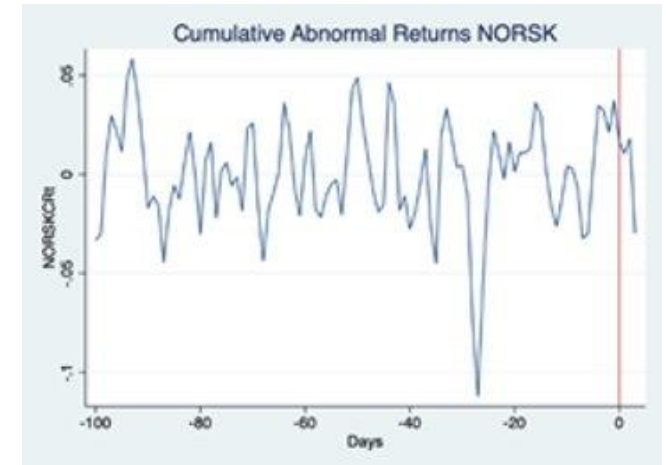
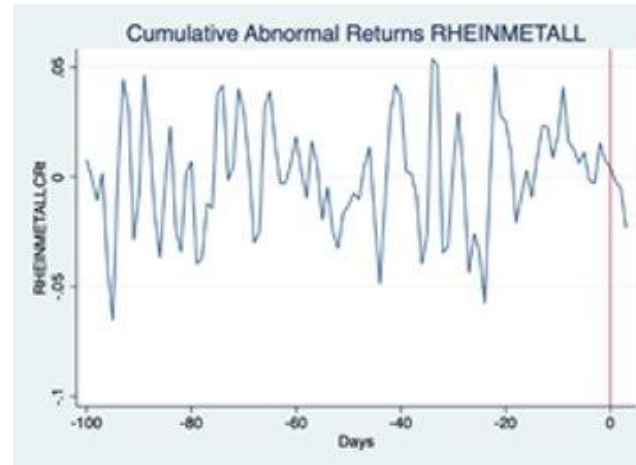
Methodik

- ❑ Annahme informationseffizienter Märkte und rationaler Investoren
- ❑ Event Study Analyse > wichtigste Methode zur Analyse der Auswirkungen von Cyberangriffen auf die Unternehmenswerte
- ❑ 34 Fälle > 13 Unternehmen

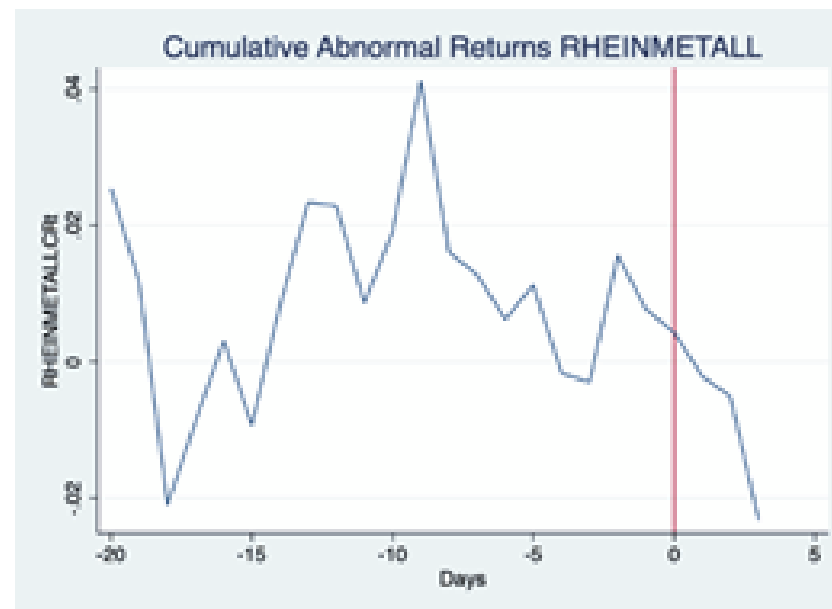
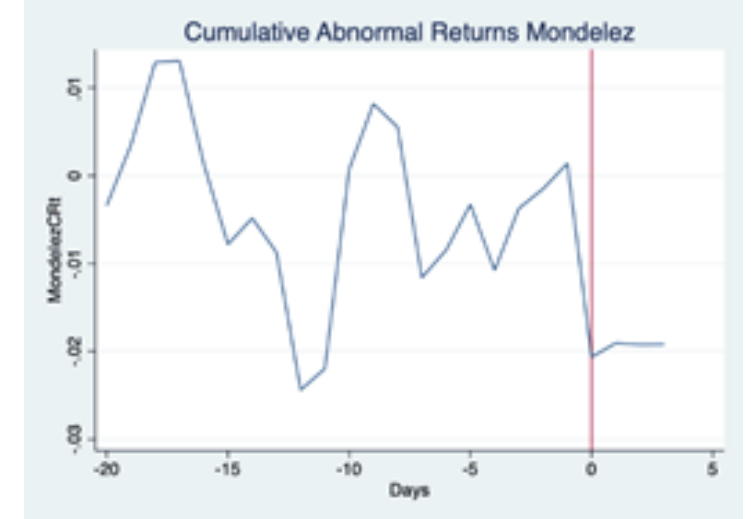
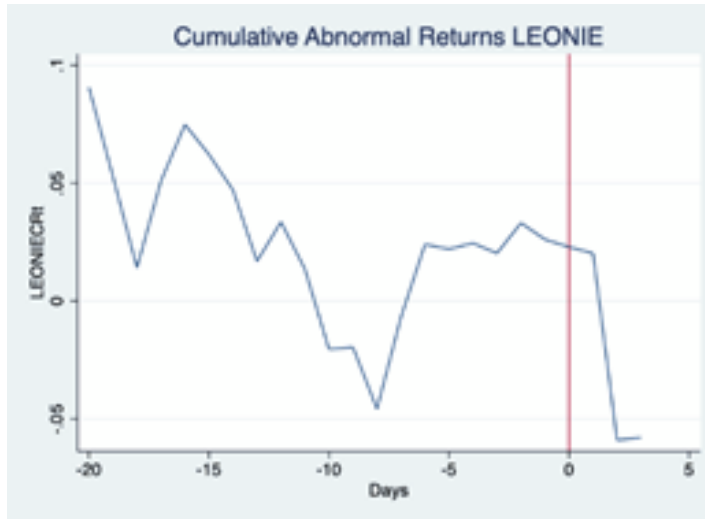
Cumulative
Abnormal Returns
(CAR) – 100 Days
Estimation Period
(not influenced)



Cumulative
Abnormal Returns
(CAR) – 100 Days
Estimation Period
(negative swing)



Cumulative
Abnormal Returns
(CAR) – 20 Days
Estimation Period
(influenced)



Ergbenisse Stichproben t-Test I.

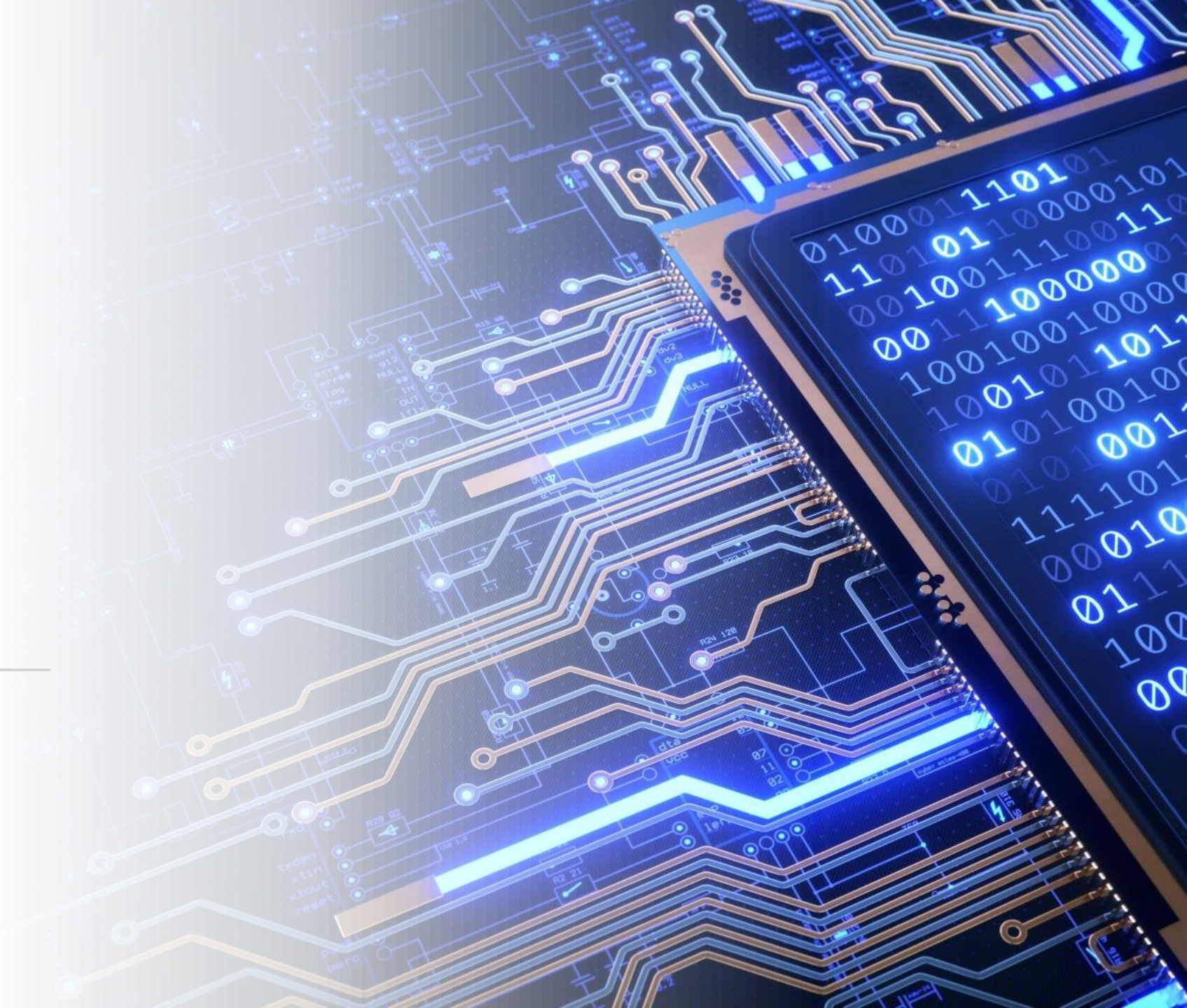
Company	Reported Losses	t-Test Results	
		Mean Abnormal Return (100 days) p-value (critical value = 0.1)	Mean Abnormal Return (20 days) p-value (critical value = 0.1)
Maersk A	250-300 million USD according to Maersk Annual Report 2017	No significant negative abnormal return 0.8288	No significant negative abnormal return 0.8468
Maersk B	250 - 300 million USD according to Maersk Annual Report 2017	No significant negative abnormal return 0.8284	No significant negative abnormal return 0.8848
Leonie	40 million EUR	No significant negative abnormal return 0.2685	Significant negative abnormal return 0.0513
Norsk Hydro	650 - 750 million NOK according to annual report. Company has Cyber Insurance	No significant negative abnormal return 0.3046	Marginally Significant negative abnormal return 0.1495
X-Fab	No cost data available yet; incident very recently	No significant negative abnormal return 0.6022	No significant negative abnormal return 0.6311
Honda	No cost data available yet; incident very recently	No significant negative abnormal return 0.3620	No significant negative abnormal return 0.1807

Ergbenisse Stichproben t-Test II.

Company	Reported Losses	t-Test Results	t-Test Results
		Mean Abnormal Return (100 days) p-value (critical value = 0.1)	Mean Abnormal Return (20 days) p-value (critical value = 0.1)
Rheinmetall	No cost data available yet; incident very recently	No significant negative abnormal return 0.2315	Significant negative abnormal return 0.0499
Stadler Rail	No cost data available yet; incidents very recently	No significant negative abnormal return 0.5521	No significant negative abnormal return 0.5919
Clarkson	minimal financial damage according to annual report	Significant negative abnormal return 0.0667	Marginally Significant negative abnormal return 0.1180
Mondelez International	114 million USD	Significant negative abnormal return 0.0496	Significant negative abnormal return 0.0402
FedEx	400 million USD according to FedEx Annual Report 2018	No significant negative abnormal return 0.6432	No significant negative abnormal return 0.3913
Rockwell Automation	no costs induced	No significant negative abnormal return 0.8397	No significant negative abnormal return 0.8454
Saint-Gobain	67 million EUR	No significant negative abnormal return 0.6158	No significant negative abnormal return 0.8333



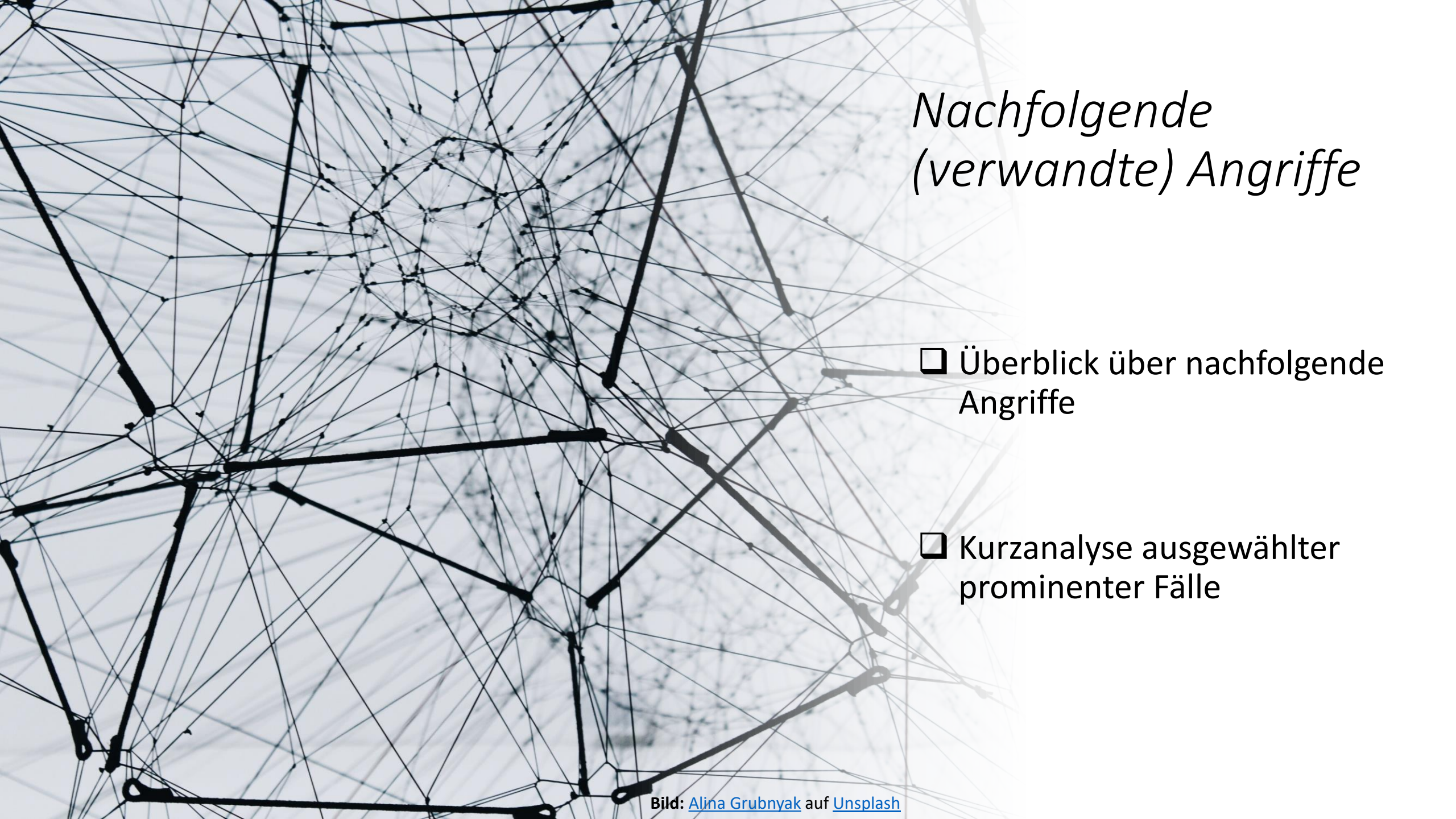
Fallstudien



Merkmale des Cyberangriffs und forensische Analyse

- ☐ Wie und wann hat die Organisation zuerst bemerkt, dass sie angegriffen wurde?
- ☐ Welche Teile der Organisation wurden kompromittiert?
- ☐ Was war(en) der/die Angriffsvektor(en)?





Nachfolgende (verwandte) Angriffe

- ☐ Überblick über nachfolgende Angriffe
- ☐ Kurzanalyse ausgewählter prominenter Fälle



Kosten

- ☐ Was waren die unmittelbaren Kosten?
- ☐ Was waren die späteren finanziellen Auswirkungen?

Lessons Learnt von dem Cyberangriff

- ☐ Welche Lehren zog das primär angegriffene Unternehmen aus dem Angriff?
- ☐ Welche weiteren Lehren und Maßnahmen können generell aus den Angriffen gezogen werden?



SolarWinds – Targeted Attack

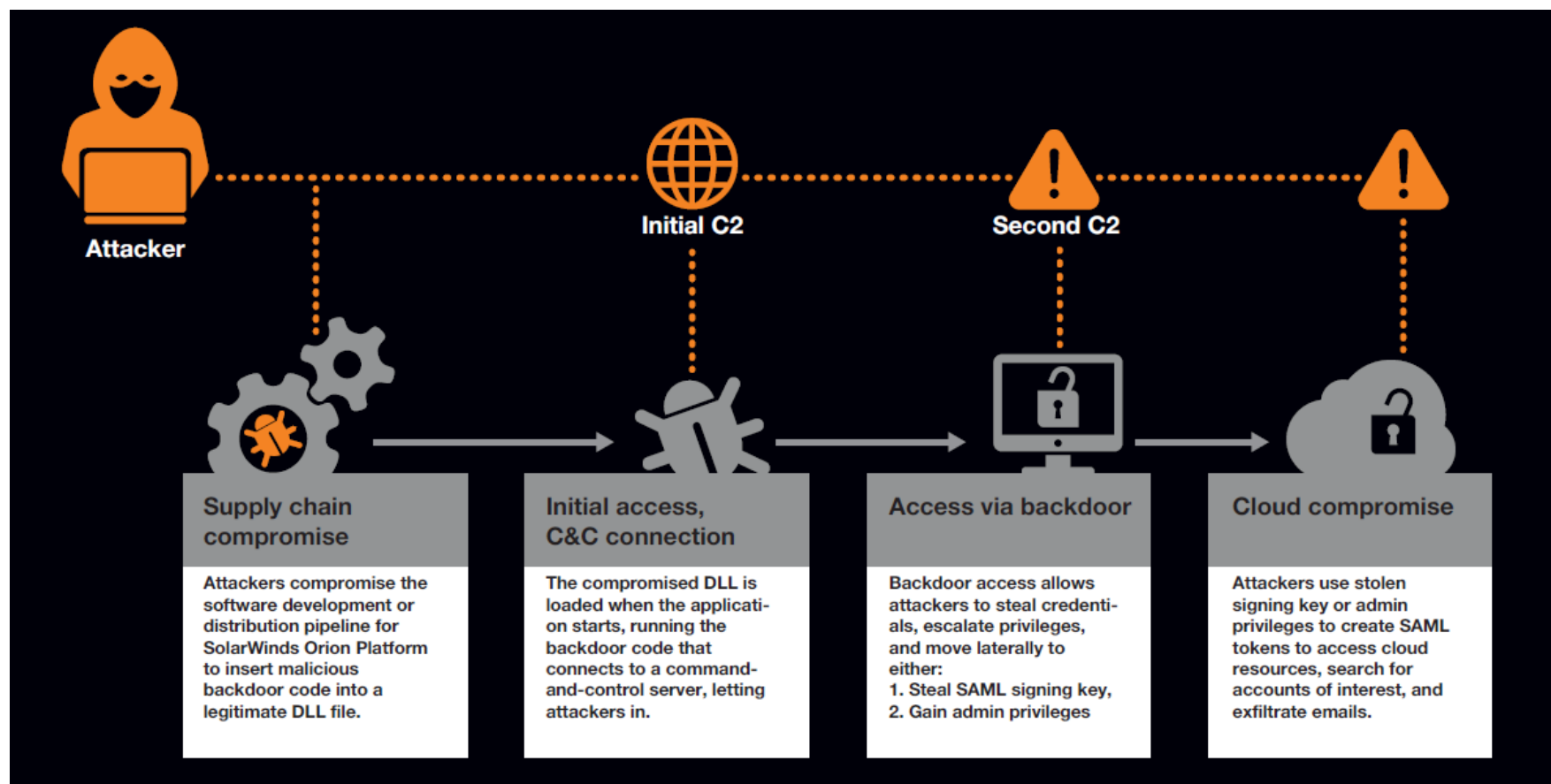
- ❑ Fokus auf Entwicklung von Netzwerkmanagement-Software
- ❑ Kundenspektrum von Fortune 500 Unternehmen zu Behörden

Cyberangriff seit September 2019

- ❑ Angriff auf Orion Plattform, eine skalierbare Überwachungs- und Verwaltungsplattform für die gesamte IT-Infrastruktur
- ❑ Installation einer Hintertür "Sunburst" durch die Malware Sunspot; Einspielen durch reguläres Softwareupdate in Netzwerken der Kunden
- ❑ Entdeckung im Dezember 2020
- ❑ Angreifer: vermutl. ein russischer Geheimdienst
- ❑ Vermutlich eine Spionagekampagne
- ❑ Kosten: mind. \$18 Millionen im 1. Quartal von 2021 für SolarWinds alleine

SolarWinds operation is like a "burglar who wants to break into a single apartment but manages to turn off the alarm systems for every home and every building in the entire city. Everybody's safety is put at risk."

Brad Smith, Präsident von Microsoft



SolarWinds – Targeted Attack

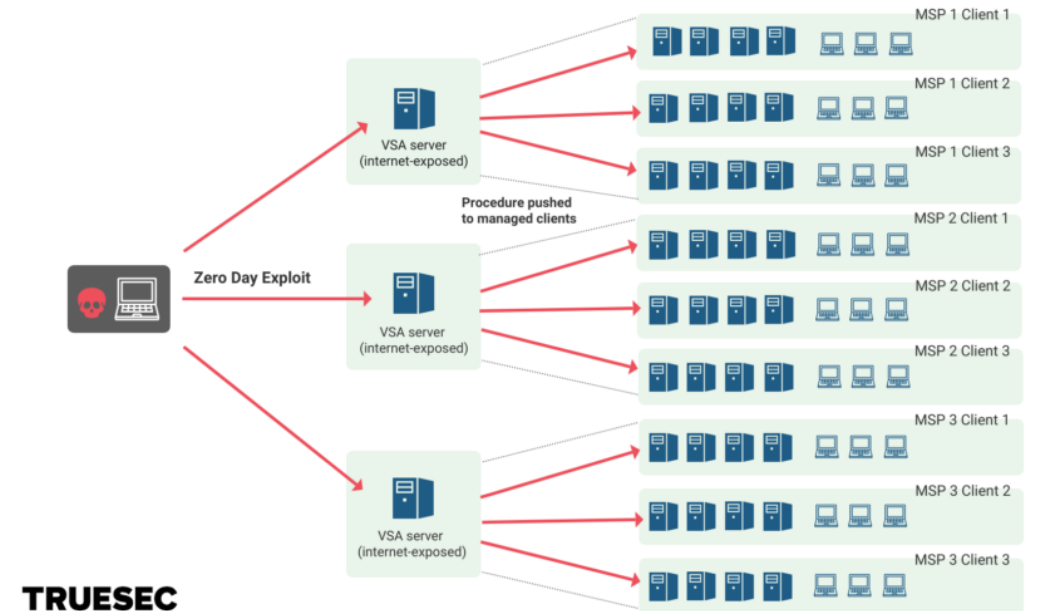
Quelle: Orange Cyberdefense (2021), Winds of change –
Underlying causes and implications of the SolarWinds attack, S. 7.

Kaseya – Collateral Damage

- ❑ Fokus auf Entwicklung von Software für die Verwaltung von Netzwerken und Systemen sowie Informationstechnologie-Infrastruktur
- ❑ Kundenswerpunkt = Management Service Providers (MSP)

Angriff am 2. Juli 2021

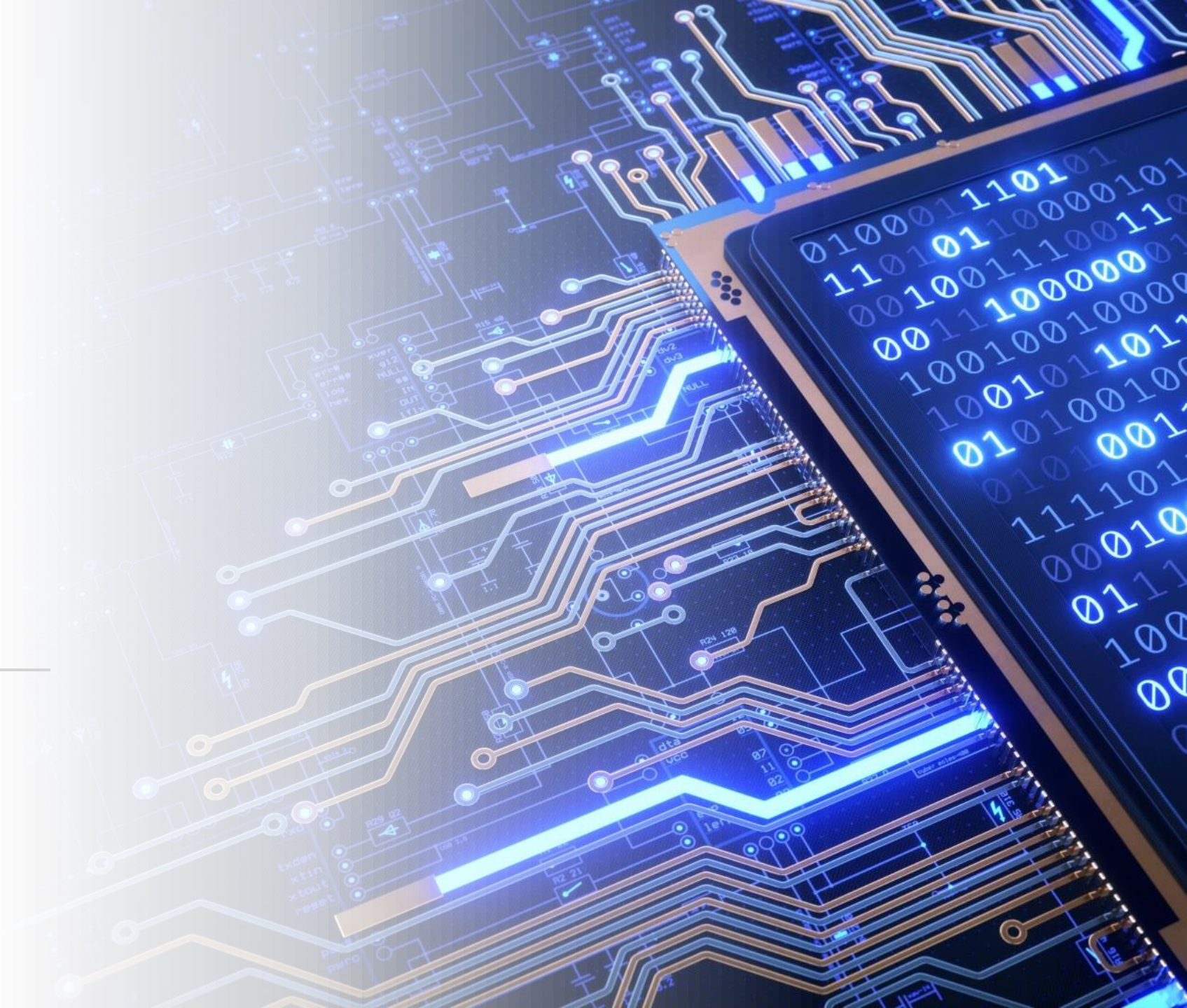
- ❑ Angriff auf VSA-Software durch Zero-Day Exploit
- ❑ 60 betroffene MSP und mindestens 1000 Kunden dieser MSP
- ❑ Angreifer: ReEvil-Gruppe; Forderung von \$70 Mio. am 5. Juli 2021



Überblick über den Angriff, Quelle: Truesec,
<https://blog.truesec.com/2021/07/04/kaseya-supply-chain-attack-targeting-msps-to-deliver-revil-ransomware/>



Vorläufige Erkenntnisse



Vorläufige Erkenntnisse I.

- ❑ Fabrik der Zukunft ist digital, vernetzt und dadurch auch verwundbar
- ❑ Überblick über die eigenen Lieferketten und Schnittstellen schaffen
- ❑ Überblick über kritische Vermögenswerte
- vor allem immaterielle Vermögenswerte und indirekte Kosten
- ❑ Ganzheitliche Risikobewertung (Teil einer Kette; Resilienz, Robustheit, Redundanz)

Vorläufige Erkenntnisse II.

- ❑ Business Continuity Management
Konzept: Handbuch/Leitfaden für das Vorgehen im *Worst-Case* Szenario (Verantwortlichkeiten; technische und betriebliche Aspekte; interne und externe Kommunikation; Reaktion auf Zwischenfälle)
- ❑ Problem der Intransparenz und mangelnde Bereitschaft, Daten mit anderen Geschäftspartnern auszutauschen
- ❑ Cyberversicherungen können zu einem höheren allgemeinen IT-Schutzniveau beitragen



Adresse

Brandenburgisches Institut für Gesellschaft und Sicherheit
gGmbH (BIGS)/ Brandenburg Institute for Society and
Security

Dianastr. 46
14482 Potsdam
Deutschland



Kontakt

Tel.: +49 331 704406 – 0
Fax: +49 331 704406 – 19
E-Mail: info@big-s-potsdam.org
Twitter: @BIGS_Potsdam
Facebook: @bigspotsdam

Geschäftsführender Direktor: Dr. Tim Stuchtey