

Cyber-Risiken verstehen: Betriebsunterbrechungsschäden erkennen und berechnen



Ihr heutiger Referent



Marvin Knorr

Legal Claims
Handler

- Seit September 2023 im Markel Claims-Team
- Ansprechpartner für Cyber-Schäden
- Schwerpunkt IT-Recht

Auslöser: Ransomware- Angriff

01



Auslöser: Ransomware-Angriff

```
ubuntu@DFIR-WIN11-SB:/mnt/z/PIM-3630_/_Ransomnote und Samples$ cat readme.txt.flocked
```

If you are reading this, then you have been the victim of a cyber attack. We call ourselves Fog and we take responsibility for this incident. You can check out our blog where we post company data: xbkv2qey6u3gd3qxcojynrt4h5sgrhkar6whuo74wo63hijnn677jnyd.onion You might appear there if you opt out of our communication.

We are the ones who encrypted your data and also copied some of it to our internal resource. The sooner you contact us, the sooner we can resolve this incident and get you back to work.

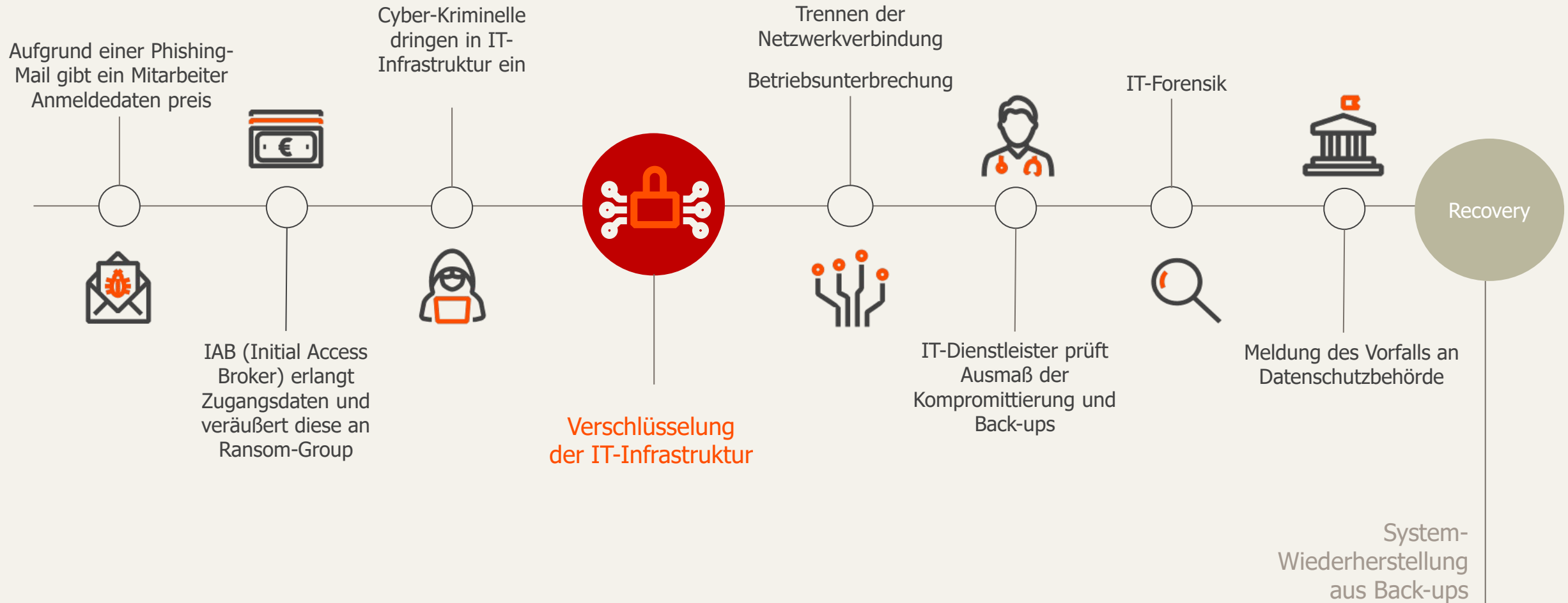
To contact us you need to have Tor browser installed:

1. Follow this link: xql562evsy7njcsngacphc2erzjfecwotdkobn3m4uxu2gtqh26newid.onion
2. Enter the code: HA60UZJPCL1RUZ28U0PC06LA
3. Now we can communicate safely.

If you are decision-maker, you will get all the details when you get in touch. We are waiting for you.ubuntu@DFIR-WIN11-

*FOG Ransomware

(Möglicher) Ablauf eines Ransomware-Angriffs



Entwicklung Betriebs- unterbrechungs- schäden

02



Entwicklung der Betriebsunterbrechung im Versicherungswesen

Frühe Anfänge:

19. Jahrhundert



- Erste BU-Policen richteten sich vor allem an **Produktions-einrichtungen**.
- **Deckung:** Verdienstausfall nach einem Sachschaden, wie etwa einem Maschinenschaden oder einem Feuer.

Nachkriegszeit:

Aufstieg im 20. Jahrhundert



- Wirtschaftswunder und Industrialisierung: **Verstärkte Nachfrage** nach Versicherungsschutz.
- **Erweiterung der Deckung:** Neben Feuer und Maschinenbruch kamen Risiken wie Überschwemmungen, Sturm und Explosionen hinzu.

Ab den 1980er-Jahren:

Globalisierung und Just-in-Time-Produktion



- **Just-in-Time-Lieferketten:** Erheblicher Anstieg der Anfälligkeit von Unternehmen für Betriebsunterbrechungen
- **Erweiterung der Deckung:** Nun werden auch Rückwirkungsschäden erfasst.

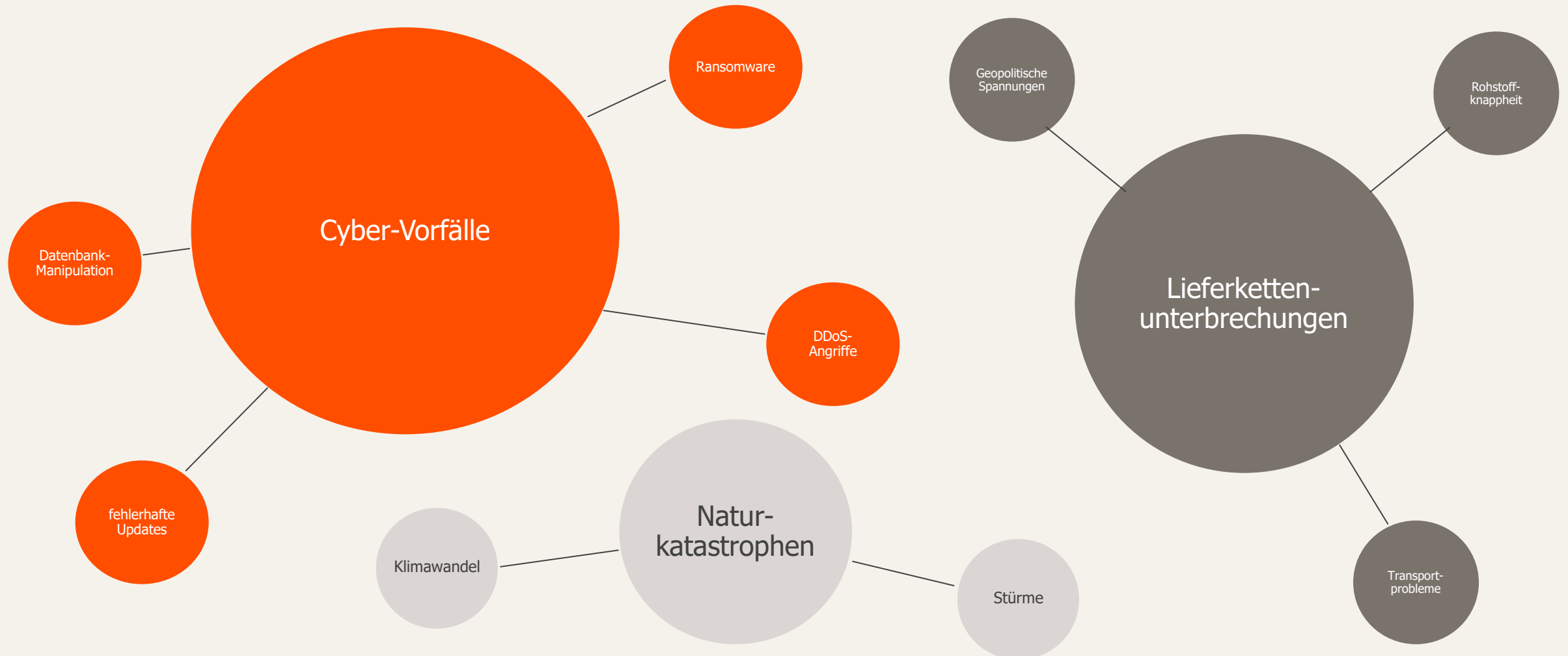
Seit den 2000er-Jahren:

Digitalisierung und neue Risiken



- **Digitalisierung:** Abhängigkeit von IT-Systemen führt zu neuen Risiken.
- **Globale Krisen:** Die Finanzkrise 2008, die COVID-19-Pandemie und geopolitische Konflikte haben gezeigt, dass Betriebsunterbrechungen heute oft globale Dimensionen annehmen.

Die größten BU-Risiken in der heutigen Zeit



Betriebsunterbrechungsschaden nach GDV-Musterbedingungen

Betriebsunterbrechung

Voraussetzung

→ Wenn infolge der Informationssicherheitsverletzung elektronische Daten oder informationsverarbeitende Systeme des Versicherungsnehmers nicht zur Verfügung stehen oder nicht die übliche Leistung erbringen und daraus ein Unterbrechungsschaden entsteht.

Unterbrechungsschaden

Definition

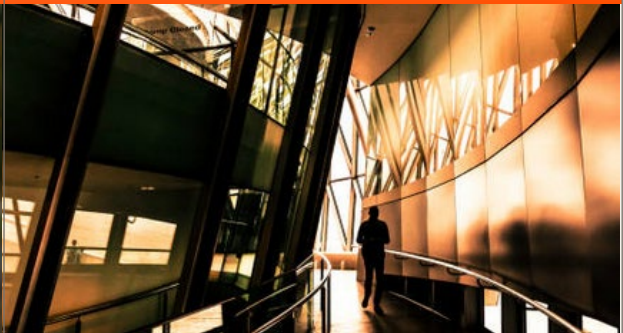
→ Der Unterbrechungsschaden ist der Betriebsgewinn und die fortlaufenden Kosten, die im Zeitraum der Betriebsunterbrechung, längstens jedoch der Haftzeit durch den Versicherungsnehmer, nicht erwirtschaftet werden können.

Betriebs- unterbrechung

03



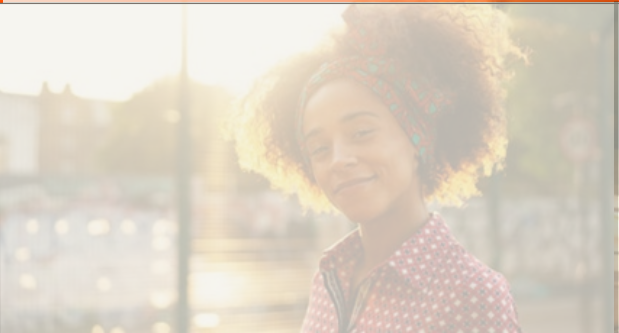
Beispiele der Betriebsunterbrechung

Dienstleistungen	Produktion	Verkauf	Lager
			
- Daten aus Dokumenten-Management-System sind verschlüsselt und können nicht abgerufen werden. - Trennung des Netzwerks führt dazu, dass an Endgeräten nicht mehr gearbeitet werden kann.	- Steuereinheiten der Produktionsmaschinen stehen aufgrund eines Cyber-Angriffs nicht mehr zur Verfügung. - Buchhaltung kann nicht mehr auf Daten zugreifen. - Keine Überweisungen möglich.	- Kassensysteme sind aufgrund von Cyber-Angriff offline. - Preise können nicht abgerufen werden. - Warenbestellungen sind nicht möglich.	- Daten aus Lagerverwaltungssystem können nicht abgerufen werden. - Einschränkungen bei Lieferung bzw. Verkauf der eingelagerten Waren.

Beispiele der Betriebsunterbrechung

Dienstleistungen	Produktion	Verkauf	Lager
			
- Daten aus Dokumenten-Management-System sind verschlüsselt und können nicht abgerufen werden. - Trennung des Netzwerks führt dazu, dass an Endgeräten nicht mehr gearbeitet werden kann.	- Steuereinheiten der Produktionsmaschinen stehen aufgrund eines Cyber-Angriffs nicht mehr zur Verfügung. - Buchhaltung kann nicht mehr auf Daten zugreifen.	- Kassensysteme sind aufgrund von Cyberangriff offline.	- Daten aus Lagerverwaltungssystem können nicht abgerufen werden. - Einschränkungen bei Lieferung bzw. Verkauf der eingelagerten Waren.

Beispiele der Betriebsunterbrechung

Dienstleistungen	Produktion	Verkauf	Lager
			
- Daten aus Dokumenten-Management-System sind verschlüsselt und können nicht abgerufen werden. - Trennung des Netzwerks führt dazu, dass an Endgeräten nicht mehr gearbeitet werden kann.	- Steuereinheiten der Produktionsmaschinen stehen aufgrund eines Cyber-Angriffs nicht mehr zur Verfügung. - Buchhaltung kann nicht mehr auf Daten zugreifen.	- Kassensysteme sind aufgrund von Cyberangriff offline.	- Daten aus Lagerverwaltungssystem können nicht abgerufen werden. - Einschränkungen bei Lieferung bzw. Verkauf der eingelagerten Waren.

Beispiele der Betriebsunterbrechung

Dienstleistungen	Produktion	Verkauf	Lager
			
- Daten aus Dokumenten-Management-System sind verschlüsselt und können nicht abgerufen werden. - Trennung des Netzwerks führt dazu, dass an Endgeräten nicht mehr gearbeitet werden kann.	- Steuereinheiten der Produktionsmaschinen stehen aufgrund eines Cyber-Angriffs nicht mehr zur Verfügung. - Buchhaltung kann nicht mehr auf Daten zugreifen.	- Kassensysteme sind aufgrund von Cyber-Angriff offline.	- Daten aus Lagerverwaltungssystem können nicht abgerufen werden. - Einschränkungen bei Lieferung bzw. Verkauf der eingelagerten Waren.

Beispiele der Betriebsunterbrechung

Dienstleistungen	Produktion	Verkauf	Lager
			
➤ Daten aus Dokumenten-Management-System sind verschlüsselt und können nicht abgerufen werden. ➤ Trennung des Netzwerks führt dazu, dass an Endgeräten nicht mehr gearbeitet werden kann.	➤ Steuereinheiten der Produktionsmaschinen stehen aufgrund eines Cyber-Angriffs nicht mehr zur Verfügung. ➤ Buchhaltung kann nicht mehr auf Daten zugreifen.	➤ Kassensysteme sind aufgrund von Cyberangriff offline.	➤ Daten aus Lagerverwaltungssystem können nicht abgerufen werden. ➤ Einschränkungen bei Lieferung bzw. Verkauf der eingelagerten Waren.

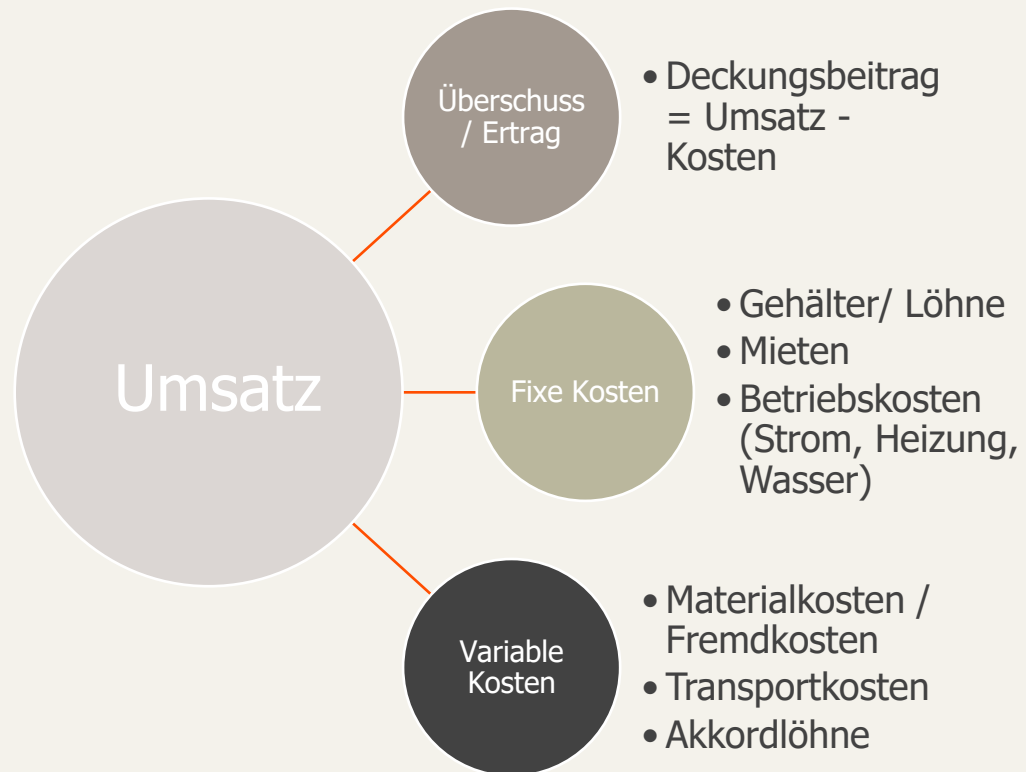
Unterbrechungs- schaden

04

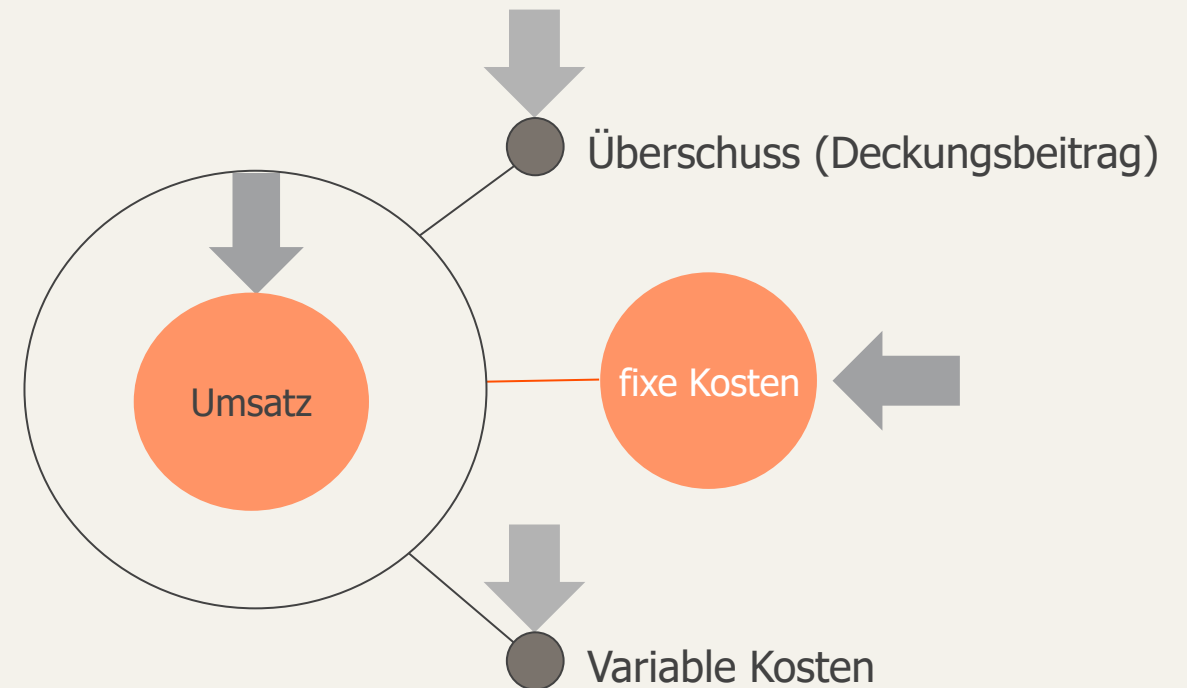


Betriebswirtschaftliche Auswirkungen bei Unterbrechungsschaden

Gewöhnlicher Betriebsablauf



Betriebsstörung/-unterbrechung



Berechnung Betriebsunterbrechungsschaden

1. Bestimmung des versicherten Anteils am Umsatz

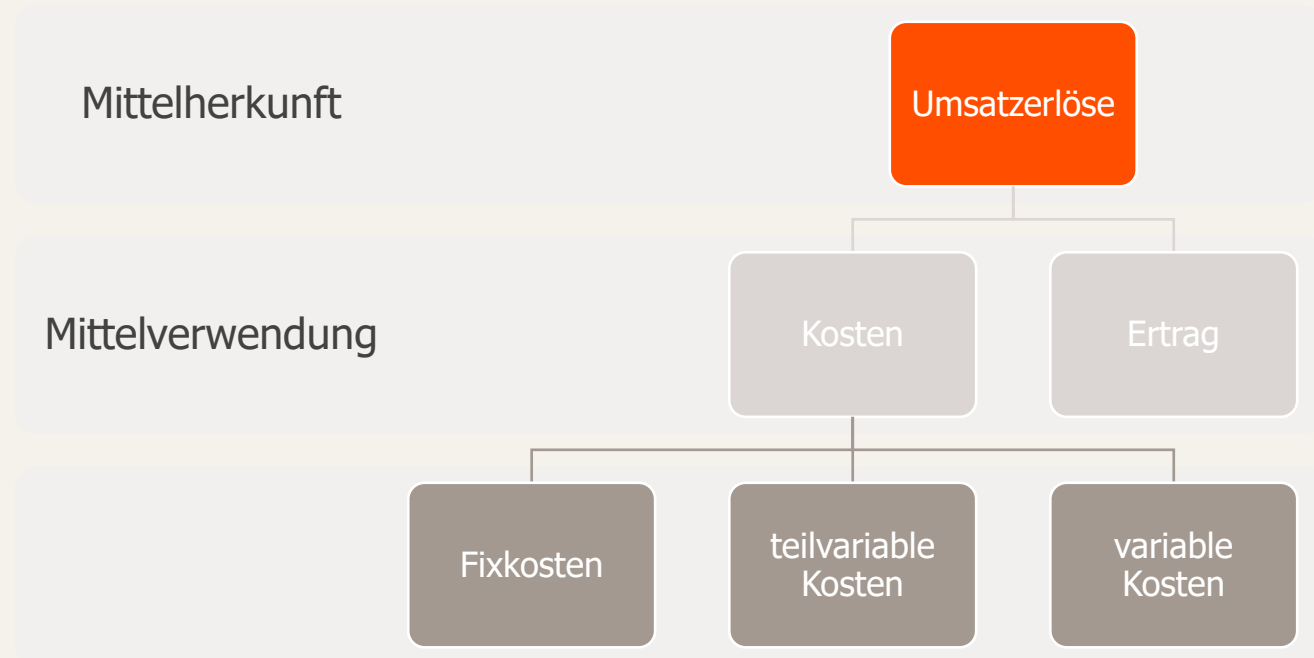
$$\begin{aligned} &\text{Umsatzerlöse} \\ &- (\text{variable Kosten} + \text{teilvariable Kosten}) \\ &= \textbf{versicherter Anteil} \\ &(\textbf{fixe Kosten} + \textbf{Gewinn}) \end{aligned}$$



Produktionsbetrieb
Ca. 40-60%



Dienstleistungen/
beratend
Ca. 70-90%



Berechnung Betriebsunterbrechungsschaden

2. Bestimmung des Umsatzausfalls

$$\begin{array}{l} \text{SOLL-Umsatz} \\ - \text{IST-Umsatz} \\ \hline = \textbf{Umsatzausfall} \end{array}$$

Betrachtet wird hierbei die Zeitspanne zwischen Betriebsstörung und Wiederaufnahme des Geschäftsbetriebs (= Störungs-/bzw. Unterbrechungszeitraum) - Im Verhältnis zur Vergangenheit (und Entwicklung nach Wiederherstellung)

3. Bestimmung Betriebsunterbrechungsschaden

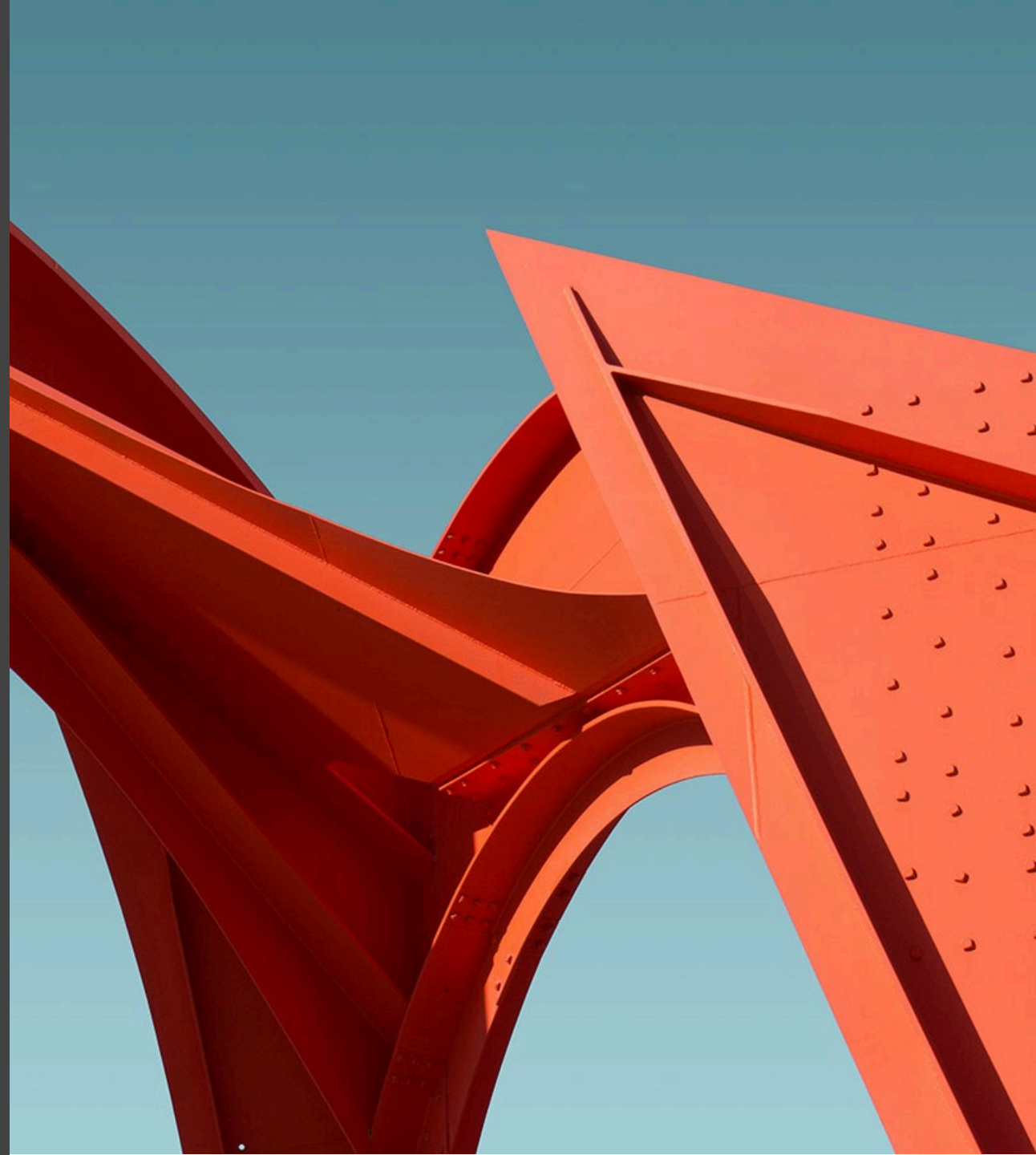
$$\begin{array}{l} \text{Umsatzausfall} \\ - \text{"nicht-versicherter Anteil" (variable Kosten)} \\ \hline = \textbf{Betriebsunterbrechungsschaden (i.e.S.)} \end{array}$$

Personal-/Mitarbeiterkosten

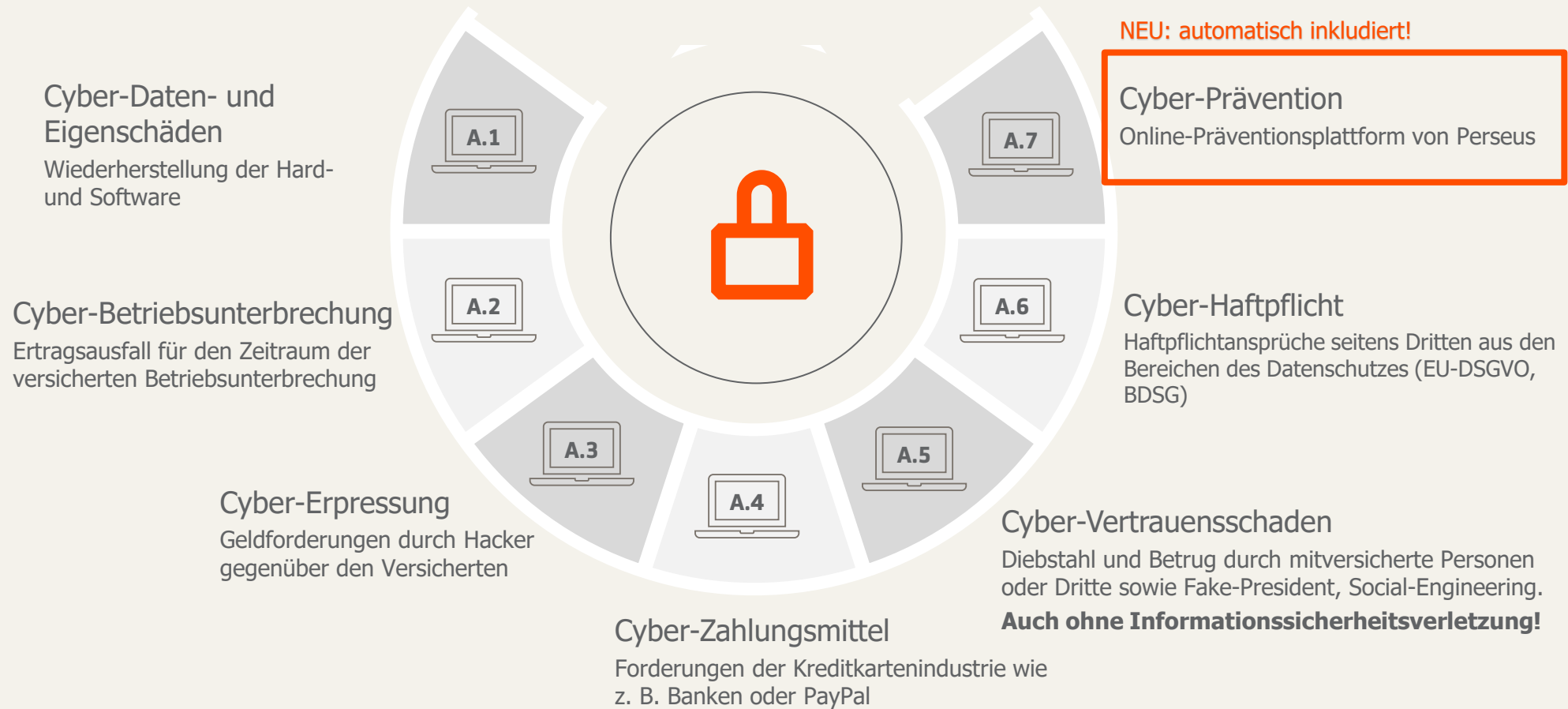
Mehraufwendungen	Betriebsunterbrechungsschaden (i.e.S.)	"Ineffizienzen"
- <u>Gesonderte Vergütungen</u> - zusätzlich zu gewöhnlichem Gehalt - aufgrund von <u>Mehrarbeit/Überstunden/Zuschlägen</u> zur Schadenbehebung bzw. -minderung. - Fallen im "normalen" Geschäftsbetrieb nicht an. - Z. B. IT-Abteilung arbeitet an Wiederherstellung der IT-Systeme, hierbei fallen zusätzliche Vergütungen (etwa für Nachschichten, Wochenendarbeit) an. - Hierunter fallen keine Gehälter/Löhne, die üblicherweise gezahlt werden – auch wenn Mitarbeiter ihrer gewöhnlichen Tätigkeit nicht oder nur eingeschränkt nachgehen können ("Ineffizienzen").	- Mitarbeitergehälter und -löhne sind <u>fixe fortlaufende Kosten</u> im Sinne des Betriebsunterbrechungsschadens. - Voraussetzung für Erstattungsfähigkeit ist jedoch, dass Gehälter/Löhne "nicht erwirtschaftet" werden konnten. -> d. h. den gezahlten Gehältern/Löhnen stehen keine entsprechenden Einnahmen gegenüber (Umsatz bzw. Ertragsausfall) - Z. B. Rechtsanwälte einer Kanzlei arbeiten auf Stundenhonorarbasis, in den letzten Monaten 100% Auslastung, während Störzeitraum keine Erträge. - (!) Keine "doppelte Erstattung", wenn Kosten bereits als Mehraufwendungen berücksichtigt wurden.	- Mitarbeiter können nicht ihrer regelmäßigen Arbeit nachgehen, hierdurch entsteht jedoch <u>kein Umsatz- bzw. Ertragsausfall.</u> - <u>Kein Betriebsunterbrechungsschaden!</u>

Markel Pro Cyber v2

05



Modularer Versicherungsschutz Markel Pro Cyber



MARKEL