

FÜR UNTERNEHMEN

Cyberversicherungen: Policen und Schadenregulierung

Was eine gute Police enthalten muss – und
was im Ernstfall wirklich passiert

Benno G. Embser, Ass. jur.

IHK Nord Westfalen · Online-Vortrag · 29. September
2026

Fülling & Meysenburg GmbH & Co. KG ·
Assekuranzmakler seit 1958

Vom Risiko über die Police zum Schadenfall

01



Risiko

Aktueller Fall, Lagebild,
Schadenpraxis

02



Police

Mindeststandards, Bausteine,
Qualität, Grenzen

03



Schadenfall

Szenario, erste Stunden,
Regulierung

Zum Schluss: Fazit und Ihre Fragen. Produktneutral; keine Deckungs- oder Rechtsprüfung im Einzelfall.

01

RISIKO

Warum der Angriff der Normalfall ist – und
was ein Vorfall kostet



Risiko

Aktueller Fall, Lagebild,
Schadenpraxis



Police



Schadenfall

Berlin: 5,8 Terabyte im Darknet



ANGRIFF

7.–12. Aug.

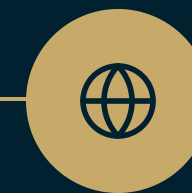
Angriff auf Netze der Berliner Verwaltung – über bekannte, nicht geschlossene Sicherheitslücken



FORDERUNG

30 Bitcoin

rund 2 Mio. € Lösegeld gefordert – der Senat lehnt ab



VERÖFFENTLICHUNG

5. Sept.

Frist abgelaufen: 1,44 Mio. Dateien veröffentlicht – Lohnzettel, Zeugnisse, Bankdaten, Notfallpläne

Quelle: Quellenverzeichnis am Ende der Folien

Der Ablauf betrifft auch Unternehmen

Das ist kein Behördenproblem. Dieselbe Gruppe – Rhysida – verschlüsselt seit Jahren mittelständische Unternehmen, Kliniken und Kommunen. Der Ablauf ist immer gleich:



🔍 LEITFRAGE

Was hätte eine Cyberpolice hier geleistet – und was nicht?

Quelle: [Quellenverzeichnis am Ende der Folien](#)

Der Angriff ist der Normalfall

96 %

der deutschen Unternehmen
waren in den letzten 12
Monaten betroffen oder
vermuten es

80 %

der registrierten
Ransomware-Angriffe treffen
kleine und mittlere
Unternehmen

45 %

sehen ihre Existenz durch
einen erfolgreichen Angriff
bedroht

1/3

der Unternehmen erfüllt
grundlegende IT-
Sicherheitsanforderungen –
nur ein Drittel

Quelle: Quellenverzeichnis am Ende der Folien

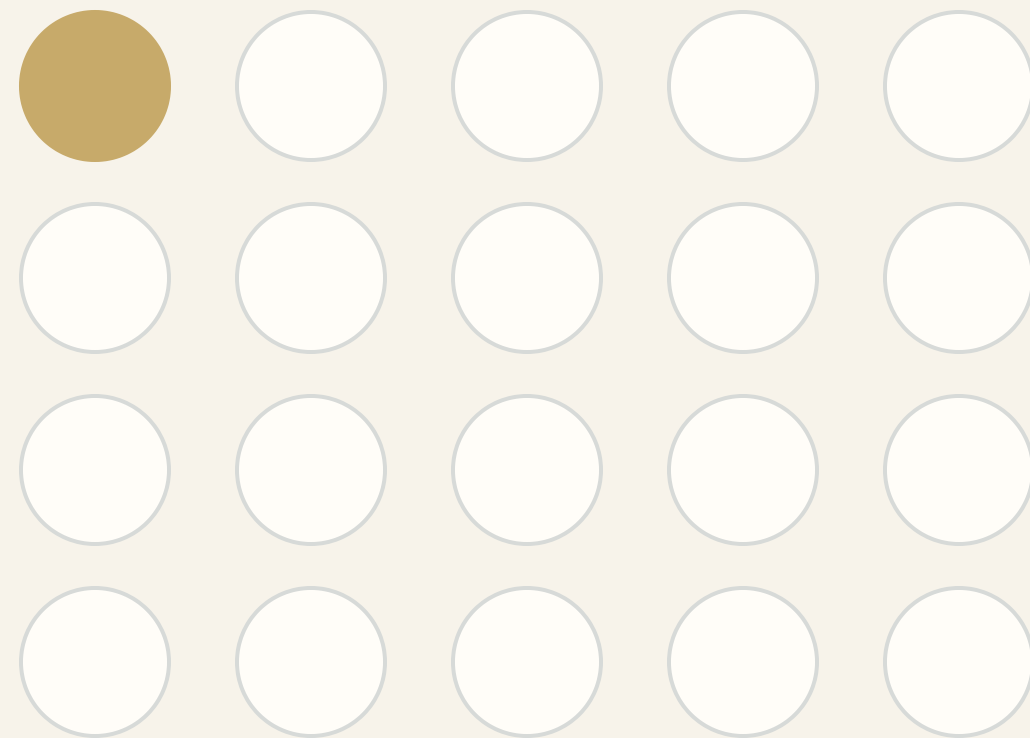
Zu klein zu sein schützt nicht

„Die Annahme, zu klein oder zu unwichtig zu sein, ist ein gefährlicher Trugschluss.“

GDV

Quelle: Quellenverzeichnis am Ende der Folien

Nur eins von 20 Unternehmen ist versichert



● VERSICHERT

5 %

der Unternehmen in Deutschland haben eine Cyberversicherung – trotz 96 % Betroffenheit

157.000

Verträge 2025 – plus 15,7 % gegenüber dem Vorjahr

| 95 % produzieren ohne Feuerlöscher.

Quelle: Quellenverzeichnis am Ende der Folien

Mindeststandards und Schadenleistungen

3 %

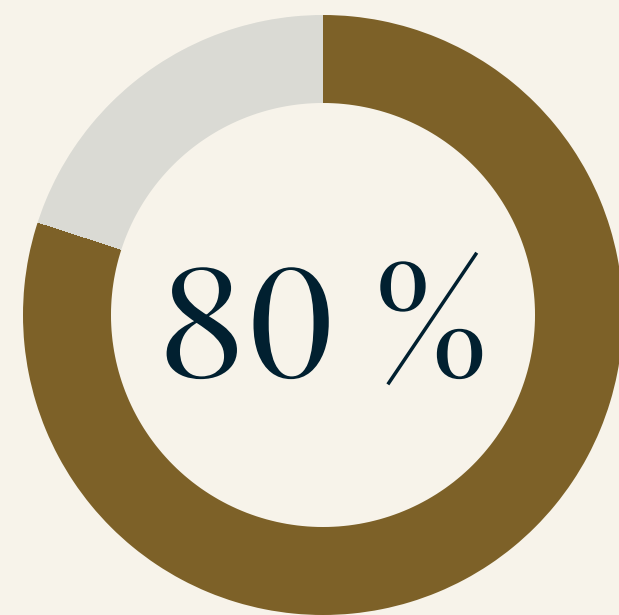
der versicherten Unternehmen melden pro Jahr einen Schaden – die Mindeststandards wirken

43.186 €

Durchschnittsschaden 2025 (+5,8 %), rund 200 Mio. € Leistungen insgesamt

Quelle: Quellenverzeichnis am Ende der Folien

Was ein Vorfall kostet



der Schäden bei einem großen Versicherer sind heute Computerbetrug – meist nach Phishing

43.186 €

Durchschnittsschaden 2025 – ein Ransomware-Fall mit Stillstand liegt praktisch immer sechsstellig

Quelle: Quellenverzeichnis am Ende der Folien

Stillstand, Neuaufbau, Überweisung: drei Fälle



APOTHEKE

10 Tage

Kommissionierautomat
ohne EDV – kein
Medikament mehr
auffindbar, zehn Tage
geschlossen



BAUUNTERNEHMEN

100.000 €

alle Server verschlüsselt,
kein Lösegeld gezahlt –
trotzdem Neuinstallation
an allen Standorten



GROSSUNTERNEHMEN

10,5 Mio. €

Video-Call mit täuschend
echten Deepfake-
Avataren der
Geschäftsführung –
Überweisung freigegeben

Quelle: [Quellenverzeichnis am Ende der Folien](#)

Eine Police ersetzt kein Risikomanagement



AUFGABE DES
UNTERNEHMENS

Vermeiden

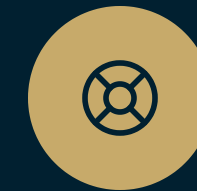
MFA, Patching, Schulung
senken die
Wahrscheinlichkeit.
Backups und Notfallplan
begrenzen das Ausmaß.



GRENZE DER IT-SICHERHEIT

Restrisiko

Zero-Day-Lücken,
Innentäter, Deepfakes,
menschliche Fehler. Kein
System schützt zu 100
%.



AUFGABE DER
VERSICHERUNG

Transferieren

Fängt den Großschaden
auf und liefert
Forensiker, Anwälte,
Krisenmanager – setzt
aber Mindeststandards
voraus.

Quelle: Quellenverzeichnis am Ende der Folien

02

POLICE

Was Versicherer voraussetzen, was drin sein muss – und woran der Schutz scheitert



Risiko



Police

Mindeststandards,
Bausteine, Qualität,
Grenzen



Schadenfall

Versicherer fragen Mindeststandards ab

STUFE 2 MFA · 4-Augen-Prinzip und Schulung · IT-Notfallplan

Grundvoraussetzung bei praktisch jedem Anbieter



Regelmäßige Backups – getrennt

täglich ab 1 Mio. € Umsatz,
auf separaten Systemen;
besser: getestet und offline



Firewall und Virenschutz

an allen
Internetübergängen,
automatisch aktualisiert



Keine Altsysteme am Netz

Systeme ohne Hersteller-
Updates isolieren oder
ablösen

Quelle: Quellenverzeichnis am Ende der Folien

Weitere Anforderungen hängen vom Risiko ab

Zunehmend abgefragt – ab ca. 10 Mio. € Umsatz meist Pflicht



MFA für Fernzugriff
und Admins

Zwei-Faktor oder VPN – bei
vielen Anbietern die Frage,
die über das Angebot
entscheidet



4-Augen-Prinzip
und Schulung

Überweisungen über 10.000
€ freigeben lassen;
Phishing-Training



IT-Notfallplan

schriftlich, mit
Verantwortlichen und
Telefonnummern – auch
ohne IT lesbar

STUFE 1 Getrennte Backups · Firewall und Virenschutz · keine Altsysteme

Quelle: [Quellenverzeichnis am Ende der Folien](#)

Antworten müssen zur tatsächlichen IT passen

Risikofragen im Antrag

Backups auf separaten Systemen ☒ Ja ☐ Nein

Firewall und Virenschutz ☒ Ja ☐ Nein

MFA für Fernzugriff und Admins ☒ Ja ☐ Nein

Schematische Darstellung, kein Originalformular

Jede Antwort im Antrag
wird Vertragsbestandteil –
und im Schadenfall
geprüft.

 PRAXIS

Antworten
dokumentieren!

Quelle: Quellenverzeichnis am Ende der Folien

Eigenschaden und Betriebsunterbrechung

BAUSTEINE DER POLICE

 Eigenschaden

 Betriebsunterbrechung

 Cyber-Erpressung

 Vertrauensschaden

 Haftpflicht

 Prävention

Eigenschaden **KERN**

Der Kern: Notfallhilfe, IT-Forensik, Wiederherstellung von Daten und Systemen, Anwälte, Krisenkommunikation

Betriebsunterbrechung

Ertragsausfall und Mehrkosten, solange der Betrieb steht – bei Ransomware der größte Posten

Quelle: [Quellenverzeichnis am Ende der Folien](#)

Erpressung und Vertrauensschaden unterscheiden

BAUSTEINE DER POLICE

 Eigenschaden

 Betriebsunterbrechung

 **Cyber-Erpressung**

 **Vertrauensschaden**

 Haftpflicht

 Prävention

Cyber-Erpressung

Verhandler und Krisenberatung; Lösegeld nur mit Zustimmung des Versicherers

Vertrauensschaden

Betrug ohne Hack: Fake President, manipulierte Rechnungen, Deepfake – die häufigste Schadenart

Quelle: [Quellenverzeichnis am Ende der Folien](#)

Haftpflicht und Prävention ergänzen den Schutz

BAUSTEINE DER POLICE

 Eigenschaden

 Betriebsunterbrechung

 Cyber-Erpressung

 Vertrauensschaden

 Haftpflicht

 Prävention

Haftpflicht

Ansprüche Dritter nach Datenschutzverstößen oder weitergegebener Schadsoftware, Behördenverfahren

Prävention

Schulungsplattform, Phishing-Simulation, Notfallplan-Vorlage – oft im Beitrag enthalten

Quelle: [Quellenverzeichnis am Ende der Folien](#)

Bausteine sind eine Risikoentscheidung

Nicht jeder Anbieter bietet alle Bausteine – und nicht jeder Baustein ist automatisch enthalten. Die Auswahl ist eine Risikoentscheidung.

Produktneutral: Maßgeblich ist der konkrete Vertrag, nicht die Bezeichnung des Bausteins.

Quelle: Quellenverzeichnis am Ende der Folien

Gute Notfallhilfe beginnt schon bei Verdacht

SECHS PRÜFPUNKTE

01

02

03

04

05

06

01

Notfallhilfe schon bei Verdacht

rund um die Uhr

ohne Selbstbehalt

ohne Anrechnung auf die Summe

gute Policen zahlen 2–3 Forensik-Tagessätze
auch, wenn sich kein Schaden bestätigt

Quelle: Quellenverzeichnis am Ende der Folien

02

Echter Zugang zu IT-Forensikern

das eigentliche Highlight – im Ernstfall sonst
kaum zu bekommen; eigener IT-Dienstleister
nach Absprache erlaubt

Auslöser und Betriebsunterbrechung weit fassen

SECHS PRÜFPUNKTE

01

02

03

04

05

06

03

Betriebsunterbrechung weit gefasst

auch für die Dauer der Forensik, bei Ausfall des Cloud-Anbieters und bei technischer Störung

zeitlicher Selbstbehalt **8–12 h**, nicht 24–48 h



Quelle: [Quellenverzeichnis am Ende der Folien](#)

04

Kein „nur gezielte Hackerangriffe“

Homeoffice

private Geräte

Bedienfehler

ungezielte Massenangriffe

ausdrücklich eingeschlossen

Reichweite und Versicherungssumme prüfen

SECHS PRÜFPUNKTE

01

02

03

04

05

06

05

Weltweit und lange nachmeldbar

- inklusive USA
- Daten beim Cloud-Anbieter mitversichert
- Vorfälle bleiben gedeckt, auch wenn sie erst Jahre später auffallen

06

Versicherungssumme passend zum Risiko

$$\text{Tagesumsatz} \times \text{Ausfalldauer} + \text{Wiederherstellung} + \text{Dritte}$$

im Mittelstand meist 1–2 Mio. €, oft 2-fach pro Jahr verfügbar

Quelle: [Quellenverzeichnis am Ende der Folien](#)

Ein mitverschlüsseltes Backup schützt nicht

IM ANTRAG ANGEKREUZT

- ✓ „Tägliche Datensicherung auf separaten Systemen.“

≠

TATSÄCHLICH

Das Backup lief auf ein Netzlaufwerk im selben Netz – und wurde mitverschlüsselt.

🚫 Drei Wochen Stillstand

Quelle: Quellenverzeichnis am Ende der Folien

Verschulden und Kausalität entscheiden

SCHWERES VERSCHULDEN

Vorsatz / grob fahrlässig
Rücktritt; keine Leistung,
soweit der Fehler den
Schaden verursacht hat

Einfach fahrlässig
Kündigung oder
Vertragsanpassung –
Leistung bleibt

KEIN VERSCHULDEN

Schuldlos /
richtig angegeben
☑ voller Schutz

Darstellung der Vorlage zu §§ 19, 21 VVG; keine pauschale Deckungszusage. Wortlaut und Einzelfall prüfen.

Quelle: Quellenverzeichnis am Ende der Folien

Was üblicherweise nicht versichert ist



Krieg und staatliche Angriffe
bei 37 % Geheimdienst-
Zurechnung ein wachsendes
Thema: Klausel und Beweislast
prüfen



Ausfall öffentlicher Infrastruktur
Strom, Internet, Telekom (anders als
der eigene Cloud-Anbieter)



Bekannte Lücken
und Vorschäden
was bei Antragstellung bekannt
war, ist nicht gedeckt



Vorsatz, Erfüllungsansprüche,
Vertragsstrafen
soweit nicht ausdrücklich
eingeschlossen

Quelle: Quellenverzeichnis am Ende der Folien

03

SCHADENFALL

Was im Ernstfall wirklich passiert – Stunde für Stunde, Euro für Euro



Risiko



Police



Schadenfall

Szenario, erste Stunden,
Regulierung

FIKTIVES BEISPIEL · SZENARIO

Montag, 7:30 Uhr: „Your files have been encrypted.“

FIKTIVER, TYPISCHER FALL



Produktionsbetrieb



80 Mitarbeitende



Backups getestet



MFA vorhanden

Quelle: Quellenverzeichnis am Ende der Folien

Die ersten zehn Tage kosten rund 95.000 €

TAG 0	 Erkennen, Netz trennen, Hotline		0 € Selbstbehalt Notfallhilfe
TAG 1–3	 Forensik, Krisenstab, DSGVO-Meldung	█	~35.000 €
TAG 3–10	 Neuaufbau, Notbetrieb	█	~60.000 €
TAG 10 FF.	 Und die Produktion steht noch.		

Die ersten zehn Tage: Erkennen, Forensik, Neuaufbau – bis hierhin rund 95.000 €. 0 € = Notfallhilfe ohne Selbstbehalt, nicht generell kostenlose Forensik.

Quelle: Quellenverzeichnis am Ende der Folien

Der Stillstand ist der größte Posten

TAG 0		Erkennen, Netz trennen, Hotline		0 € Selbstbehalt Notfallhilfe
TAG 1–3		Forensik, Krisenstab, DSGVO-Meldung	■	~35.000 €
TAG 3–10		Neuaufbau, Notbetrieb	■	~60.000 €
TAG 10–20		Produktion läuft wieder an · Ertragsausfall	■	~180.000 €
MONAT 2–3		Abrechnung, Härtung	■	~15.000 €

SUMME

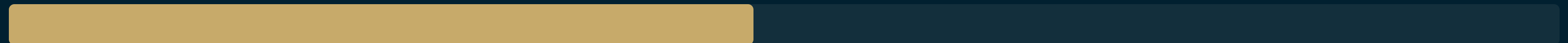
Rund 290.000 €

Quelle: Quellenverzeichnis am Ende der Folien

FIKTIVES BEISPIEL · BILANZ

Rund 290.000 € – mit getesteten Backups

MIT GETESTETEN BACKUPS



Rund 290.000 € – der größte Posten ist der Stillstand.

OHNE GETESTETE BACKUPS



Über 500.000 € · 4–6 Wochen Ausfall · Lösegeldfrage akut

Quelle: Quellenverzeichnis am Ende der Folien

Netz trennen, Spuren sichern, Hotline anrufen



Netz trennen – Strom lassen

Spuren im Arbeitsspeicher
braucht die Forensik; Stecker
ziehen zerstört sie



Fehlerbild sichern

Foto vom Bildschirm; nichts
löschen, nichts „reparieren“



Hotline anrufen – sofort

schon bei Verdacht; Nummer
gehört ausgedruckt in den
Notfallplan

Quelle: Quellenverzeichnis am Ende der Folien

Die ersten drei Schritte muss das ganze Team kennen

Die ersten drei Punkte gehören jedem Mitarbeitenden bekannt gemacht – nicht nur der IT.

Dringende Eindämmung darf nicht auf Freigabe warten; Abweichungen dokumentieren. Herunterfahren mit der Forensik abstimmen.

Quelle: Quellenverzeichnis am Ende der Folien

Abstimmen, Fristen prüfen und dokumentieren



Nur abgestimmt beauftragen
eigener IT-Dienstleister ja –
aber nach Absprache; eigene
Kanäle nutzen, die Firmen-IT
gilt als kompromittiert



Fristen einhalten

DSGVO 72 h

NIS-2 24 h

Strafanzeige bei der ZAC



Alles dokumentieren

Wer hat wann was
entschieden? Kosten separat
buchen – Grundlage der
Abrechnung

DSGVO: bei Risiko für Betroffene, ab Kenntnis. NIS-2: nur betroffene Einrichtungen. Strafanzeige:
keine starre Frist.

Quelle: Quellenverzeichnis am Ende der Folien

Drei Akten beschleunigen die Regulierung



Was passiert ist
Zeitpunkt, betroffene
Systeme, Angriffsweg,
Maßnahmen

liefert die Forensik



Was es gekostet hat
Rechnungen, Mehrkosten,
Stillstandsdauer,
Umsatzvergleich zum
Vorjahr

liefert das
Rechnungswesen ab Tag 1



Was vereinbart wurde
Schadenmeldung,
Freigaben, beauftragte
Dienstleister, Zusagen des
Versicherers

führt der Makler mit

Quelle: Quellenverzeichnis am Ende der Folien

Liquidität entscheidet vor der Schlussabrechnung

 PRAXISTIPP

Fordern Sie früh Abschlagszahlungen an – die Liquidität in den ersten Wochen entscheidet, nicht die Schlussabrechnung.

Quelle: Quellenverzeichnis am Ende der Folien

FAZIT

Früher war es die Feuerversicherung – heute ist es die Cyberversicherung

Kein Unternehmen würde ohne
Feuerschutz produzieren – und keins
ohne Brandmelder und Feuerlöscher.

95 % Bei Cyber tun es
heute 95 %.

| Prävention und Police gehören zusammen.

Quelle: Quellenverzeichnis am Ende der Folien

Drei Gedanken zum Mitnehmen



VORSORGE

Ohne Mindeststandards
keine Police – und ohne
Police kein Schutz vor
dem Großschaden.



BAUSTEINE

Die Bausteine
entscheiden:
Betriebsunterbrechung
und Vertrauensschaden
gehören dazu.



ERNSTFALL

Im Ernstfall zählt der
Anruf, nicht der Scheck –
Hotline bei Verdacht,
keine Alleingänge, alles
dokumentieren.

Quelle: Quellenverzeichnis am Ende der Folien

FAZIT

Ihre Fragen

REFERENT

Benno G. Embser, Ass.
jur.
Fülling & Meysenburg
GmbH & Co. KG
Assekuranzmakler seit
1958 · Berlin – Essen –
Stuttgart

KONTAKT

☎ Tel. 0201 82018-11
☎ Mobil 0151 12527422
✉ benno.embser@f-u-m.de

ADRESSE

Am Lichtbogen 46
45141 Essen
🌐 www.f-u-m.de

Quellen: Lage und Schäden

- 01 Berliner Datenschutzbeauftragte; Berlin.de; Euronews und dpa (September 2026)
- 02 Bitkom: Wirtschaftsschutz 2026 (26.08.2026); BSI: Lagebericht 2025 (17.11.2025)
- 03 GDV: Statistik Cyberrisikoversicherung (09/2025); Medieninformationen 05.09.2024, 05/2026 und 18.09.2026
- 04 Hiscox Cyber Readiness Report 2025; Stoik Cyber-Schadenbericht 2024

Produktneutraler Vortrag; keine Deckungs- oder Rechtsprüfung im Einzelfall. Maßgeblich bleiben der konkrete Vertrag und die Prüfung Ihrer Situation.

Quellen: Vertrag und Recht

- 05 GDV: AVB Cyber (Musterbedingungen); BSI: Ersthilfe bei Ransomware
- 06 NIS-2-Umsetzungsgesetz / BSIG n. F. §§ 32, 38; DSGVO Art. 32, 33, 34, 82, 83
- 07 VVG §§ 19, 21, 28; GmbHG § 43
- 08 Anonymisierte Bedingungswerke, Risikofragebögen, Sideletter und Notfallplan-Vorlagen zweier Versicherer (2024–2026); Gespräch mit einer Cyber-Schadenabteilung (09/2026)

Produktneutraler Vortrag; keine Deckungs- oder Rechtsprüfung im Einzelfall. Maßgeblich bleiben der konkrete Vertrag und die Prüfung Ihrer Situation.