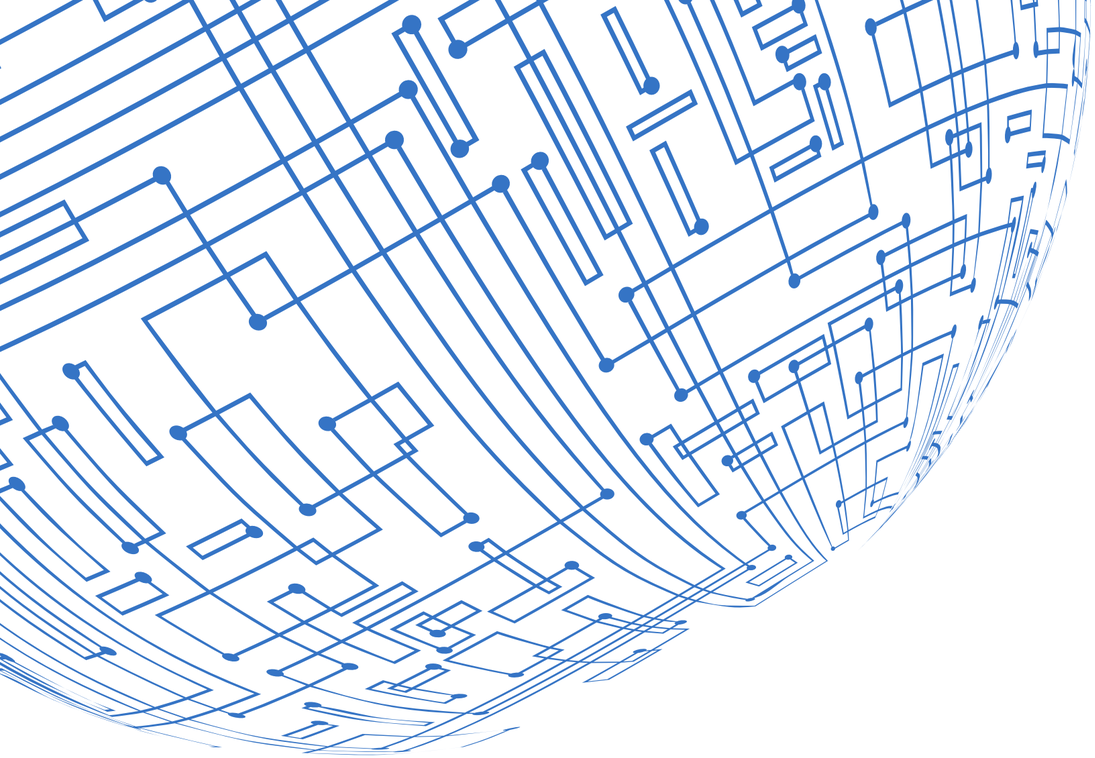


# Bedrohungslage durch Cyber-Crime

## „Risiken kennen und im Voraus handeln!“

DHS
VERSICHERUNGSMAKLER

DHS
VERSICHERUNGSMAKLER

# Bedrohungslage durch Cyber-Crime

## „Risiken kennen und im Voraus handeln!“


**Christian Gerstung**

Direktor Kundenmanagement
Meister des Handwerks
Versicherungs-Enthusiast

DHS
VERSICHERUNGSMAKLER


# Tradition verpflichtet

seit 1922 im Versicherungsgeschäft tätig

Tätigkeitsfelder:

- Ermittlung von Gefährdungspotenzialen
- Versicherungs-, Haftungs- und Vorsorgelösungen
- betriebliche Versorgungswerke
- Schaden-/Leistungsfallbetreuung

Standorte:
Braunschweig, Wolfsburg, Lüneburg, Peine, Salzgitter, Gifhorn, Harzgerode

In Planung:
Magdeburg und Hannover

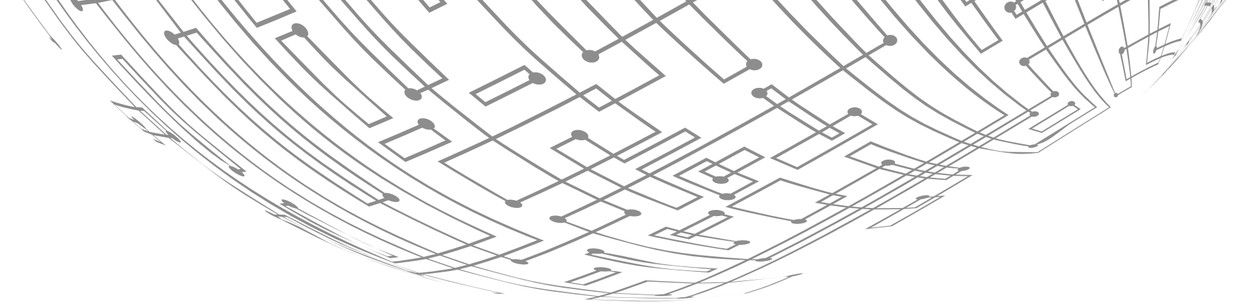

# Tradition verpflichtet

Mitarbeiter:
75 qualifizierte und hoch motivierte Mitarbeiter

Kunden:

- ca. 3.300 gewerbliche Kunden und ca. 10.500 Privatkunden
- über 45.000 Versicherungsverträge
- laufendes Beitragsvolumen ca. 55.000.000 Euro

Kooperation mit über 100 Versicherungsgesellschaften und Assekuradeuren



DHS
VERSICHERUNGSMAKLER

Unternehmen und Organisationen sind im Zeitalter der Digitalisierung auf die Informationstechnologie angewiesen!

Die Digitalisierung bringt neue Gefahren mit sich!

Ein Cyber-Schadenfall kann die Existenz eines Unternehmens bedrohen!

Informationssicherheit ist aufwendig und kostet Geld!

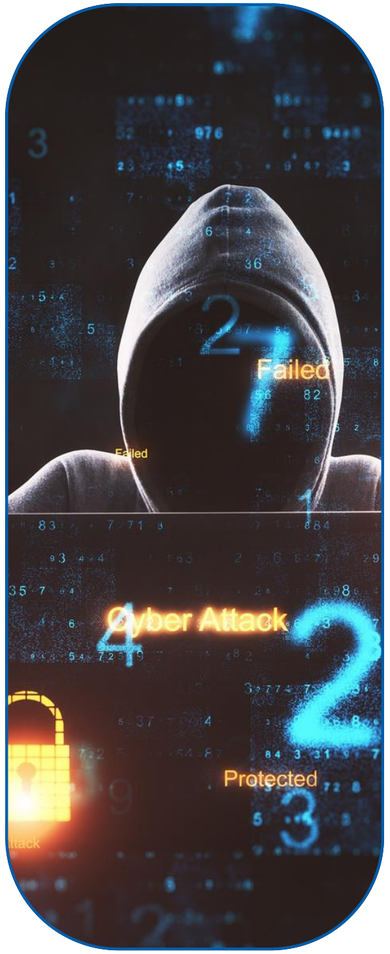
Im Voraus zu handeln macht fast alles weitere planbar!

# Bedrohungslage

Im „Allianz Risk Barometer 2022“ stehen Cyber-Vorfälle auf
Platz 1 der größten globalen Geschäftsrisiken.

Cyber-Gefahren übertreffen damit Covid-19 und die Unterbrechung von Lieferketten.

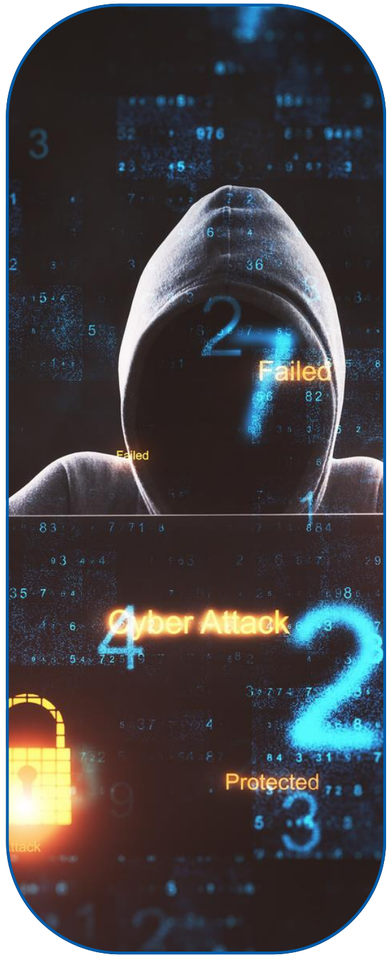
Die Ereignisse der vergangenen zwei Jahre haben uns schonungslos vor Augen geführt,
wie sehr unsere eigene Sicherheit auch von den Maßnahmen anderer abhängt.
Unterbesetzte Security-Teams und die Tatsache, dass viele Unternehmen und Organisationen
ihre Sicherheitsbelange auslagern müssen, vergrößern die Angriffsfläche für Cyberkriminelle
weiter.



# Bedrohungslage

Cyberkriminelle manipulieren die Gefühle ihrer Opfer ohne Skrupel und machen selbst vor geopolitischen Krisen keinen Halt. Mit anlassbezogenen Phishing-Mails machen sie sich etwa die Angst und Unsicherheit ihrer Opfer zunutze. Angesichts der aktuellen globalen Ereignisse sind Geopolitik und Cybersicherheit heute untrennbar miteinander verschweißt:

**Technologie und IT werden als politische Waffe instrumentalisiert.**



Digitalisierung

↓

Vernetzung der Gesellschaft

↓

Angriffsfläche für Cyberangriffe vergrößert

↓

... von wem auch immer...

Büro 121? APT? Cyber-Crime? Hacktivism? (...)

DHS
VERSICHERUNGSMAKLER

# Es gibt drei Arten von Hackern:

**White-Hat-Hacker oder White Hats** sind quasi die **«guten».**
Sie helfen ihren Auftraggebern, Sicherheitslücken in deren Systemen zu finden und zu beheben.

**Black-Hat-Hacker oder Black Hats** hingegen sind die **«bösen».**
Sie nutzen ihre Fähigkeiten, um in Computersysteme einzudringen, Daten zu stehlen oder Malware zu verbreiten.

**Grey-Hat-Hacker oder Grey Hats** wiederum bewegen sich in einer rechtlichen Grauzone zwischen den beiden anderen.
Sie können illegale Aktivitäten durchführen, haben aber nicht die Absicht, Schaden anzurichten.

DHS
VERSICHERUNGSMAKLER

# Wer sind die „bösen Akteure“?

**Cyber-Aktivisten:** Angreifer, die durch einen Cyber-Angriff auf einen politischen, gesellschaftlichen, sozialen, wirtschaftlichen oder technischen Missstand aufmerksam machen oder eine diesbezügliche Forderung durchsetzen wollen („Hacktivismus“). Die Motivation hinter dem Angriff ist Einflussnahme. Der durch einen Cyber-Angriff entstandene Schaden wird in Kauf genommen bzw. forciert, um eine höhere Aufmerksamkeit zu erlangen. Sogenannte ethische Hacker fokussieren sich auf gesellschaftliche oder soziale Themen.

**Cyber-Kriminelle:** Die Motivation von Cyber-Kriminellen ist es, mit Hilfe der Informationstechnik auf illegalen Wegen Geld zu verdienen. Hier sprechen wir inzwischen von Cyber-Crime Industrie.

**Cyber-Terroristen:** Terroristen können Cyber-Angriffe wie staatliche Akteure und Kriminelle nutzen,
um unterschiedliche Ziele anzugreifen und somit ihre Ideologie zu verbreiten und ihren Einfluss auszuweiten.

**Wirtschaftsspione:** Durch die Vorteile des Internets ergeben sich für Spione neue Möglichkeiten. Wirtschaftsspionage und Konkurrenzausspähung dienen finanziellen Interessen.

# Wer sind die „bösen Akteure“?

**Staatliche Nachrichtendienste im Cyber-Raum:** Cyber-Angriffe durch staatliche Nachrichtendienste dienen – im Gegensatz zur Wirtschaftsspionage – nicht primär finanziellen Interessen, sondern der Informationsbeschaffung und der Einflussnahme.

**Staatliche Akteure im Cyber-War:** Im militärischen Sektor wird der Cyber-Raum inzwischen vielfach als weitere wichtige Domäne neben den klassischen militärischen Domänen Land, See, Luft und Weltraum angesehen.

**Skript-Kiddies:** Die Gruppe der Skript-Kiddies führt Cyber-Angriffe durch, um Fähigkeiten und Wissen in der Praxis auszutesten. Es werden keine finanziellen Interessen verfolgt. Die Auswahl der Angriffsziele ist unspezifisch und vielfach allein vom Grad der Absicherung abhängig. Diese Tätergruppen unterscheiden sich vor allem hinsichtlich ihrer Motivation, Zielsetzungen und Ressourcen.

# KI-basierte Angriffsmethoden

Kriminelle erwirtschaften heute schon Milliardenbeträge durch Social-Engineering-Taktiken, wie Business Email Compromise oder Romance Scams.

Mit KI-basierten Angriffsmethoden, wie Deepfakes und Voice Cloning, maximieren Cyberkriminelle ihre Gewinne.

Diese Cyber-Crime Industry feilt weiterhin an ihren Angriffsmethoden.

Die Angreifenden spielen nun immer gekonnter mit menschlichen Verhaltensmustern. Ihre Opfer zahlen dafür oft wortwörtlich einen hohen Preis, etwa wenn sie unwissentlich schädliche Inhalte anklicken oder sensible Daten preisgeben.

# KI über KI

Bietet KI eine Chance oder Bedrohung für die Gesellschaft???

ChatGPT schreibt, dass KI eine Chance und eine Bedrohung zur selben Zeit darstellt und es lediglich abhängig davon ist, wie KI genutzt wird!

# Nach wie vor…

**…hat sich an grundlegenden Risiken nichts geändert!**

E-Mail, Fehlkonfiguration, veraltete Software, fehlende Sensibilisierung und …

**…hat sich an grundlegenden Maßnahmen nichts geändert!**

Back-Up, Verschlüsselung, Segmentierung, Patchmanagement, Schulung, Monitoring, Notfallplan, (…), …. Versicherung?!

**Technische Einfallstore**

Schwachstellen, Fehlkonfigurationen, veraltete Systeme, …

**Menschliche Eigenschaften**

Unaufmerksamkeit, Neugier, Arglosigkeit, Hilfsbereitschaft, …

# Cyber-Security Lage in Zahlen

**223 Mrd. Euro** jährlicher Gesamtschaden durch Cyber-Angriffe in Deutschland

**86 %** aller deutschen Unternehmen haben durch Cyber-Angriffe verursachte Schäden zu beklagen.

**358 %** Steigerungsrate, der verursachten Schäden durch Erpressung und Systemausfälle seit 2019

**43 %** der mittelständischen Unternehmen geben jährlich weniger als 10.000 Euro für Cyber-Security aus.

**Cyber-Kriminalität erbeutet weltweit inzwischen mehr Geld als der globale Drogenhandel und Prostitution  zusammen!!!**

# Angriffsszenarien

**Ransomware**:
Angreifer verschlüsseln die Daten eines Unternehmens und verlangen eine Zahlung, um den Zugang wiederherzustellen

**Malware**:
Software, die ein System schädigt

**Social-Engineering-Bedrohungen**:
Ausnutzung menschlicher Fehler, um Zugang zu Informationen oder Diensten zu erhalten

**Bedrohungen der Datensicherheit**:
gezielte Angriffe auf Datenquellen, um unbefugten Zugriff zu ermöglichen

# Angriffsszenarien

**Bedrohungen der Verfügbarkeit – Denial of Service:**
Angriffe, mit denen verhindert wird, dass Benutzer auf Daten oder Dienste zugreifen können

**Bedrohungen der Verfügbarkeit - Internet-Bedrohungen**:
Bedrohungen der Verfügbarkeit des Internets

**Desinformation/Fehlinformation:**
die Verbreitung irreführender Informationen

**Angriffe auf die Versorgungskette:**
Angriff auf die Beziehungen zwischen Organisationen und Lieferanten

# Beispielablauf: Ransomwarevorfall

Ausnutzung der Schwachstelle

Erlangung weitgehender Rechte

Installation von Backdoors in eigenen und Fremdsystemen

Deaktivieren der Sicherheitsmechanismen

Analysieren den Kunden

Exfiltrieren der Daten

Löschen der Backups

Rollout des Verschlüsselungstrojaners

# Ablauf einer Cyber-Attacke

Eine Sicherheitslücke in einer verwendeten Software ermöglichte das Eindringen einer Ransomware in das Unternehmensnetzwerk.
Die Ransomware ist in der Lage die einzelnen Schritte weitgehend zu automatisieren.

# Organisation im Unternehmen

IT-Abhängigkeit und Anfälligkeit evaluiert

Ist ein Notfall-/Krisenplan vorhanden

Informationssicherheitsbeauftragter vorhanden

Übergreifendes Risiko-Management implementiert

Ad-hoc-Zugriff auf spezialisierten Dienstleister im Schadenfall

Umgang mit Gesetzgebung und Rechtsprechung (DSGVO)

# Sensibilisierung der Belegschaft

Phishing erkennen und abwehren?!

Sichere Passwörter erstellen und merken

Sicheres Verhalten am Arbeitsplatz

Umgang mit mobilen Geräten

Social-Engineering-Angriffe erkennen und abwehren

Sicher unterwegs

DHS
VERSICHERUNGSMAKLER

**Wir Menschen haben ein großes Bedürfnis an Sicherheit!**

**Wie gehen wir z.B. mit dem Risiko aus der Gefahr – Feuer um?**

**Schon im Kindesalter hören wir immer wieder:**

# Spiel nicht mit dem Feuer!

# Brandschutz

## Was tun wir gegen die Gefahr/Risiko Feuer?

Vorhandene/mögliche Sicherungsmaßnahmen:

- E-Check & TÜV geprüfte Geräte
- Rauchmelder
- Brandmeldeanlagen
- Brandmauern
- Notausgänge
- Rettungspläne
- Sprinkleranlagen & Feuerlöscher
- Löschsysteme,…usw.

- Brandschutzbeauftragte

# Brandschutz

## Wenn`s doch brennt?!

112 Notrufnummer


Feuerwehr

# Cyberschutz

**Was tun wir gegen die Gefahr/Risiko Cyber-Crime?**

Vorhandene/mögliche Sicherungsmaßnahmen:

- Virenscanner/Firewall
- Patch-Management-Prozess
- ISMS Zertifizierung, Standards/Normen
- Zwei-Faktor-Authentifizierung (2FA o. MFA)
- Sensibilisierung Mitarbeit*innen
- Datensicherungssysteme
- Vier-Augen-Prinzip

- Informationssicherheitsbeauftragte

# Cyberschutz

## Wenn nichts mehr geht?!

## Krisen-Hotline 24/7

## Krisenmanagement

# Brandschutz vs. Cyberschutz

## Gefahr/Risiko:Feuer

Maßnahmen:

- E-Check & TÜV
- Geprüfte Geräte
- Rauchmelder
- Brandmeldeanlagen
- Notausgänge
- Rettungspläne
- Sprinkleranlagen & Feuerlöscher
- Löschsysteme

- Brandschutzbeauftragte

Notrufnummern & Feuerwehr

## Gefahr/Risiko: Cyber

Maßnahmen:

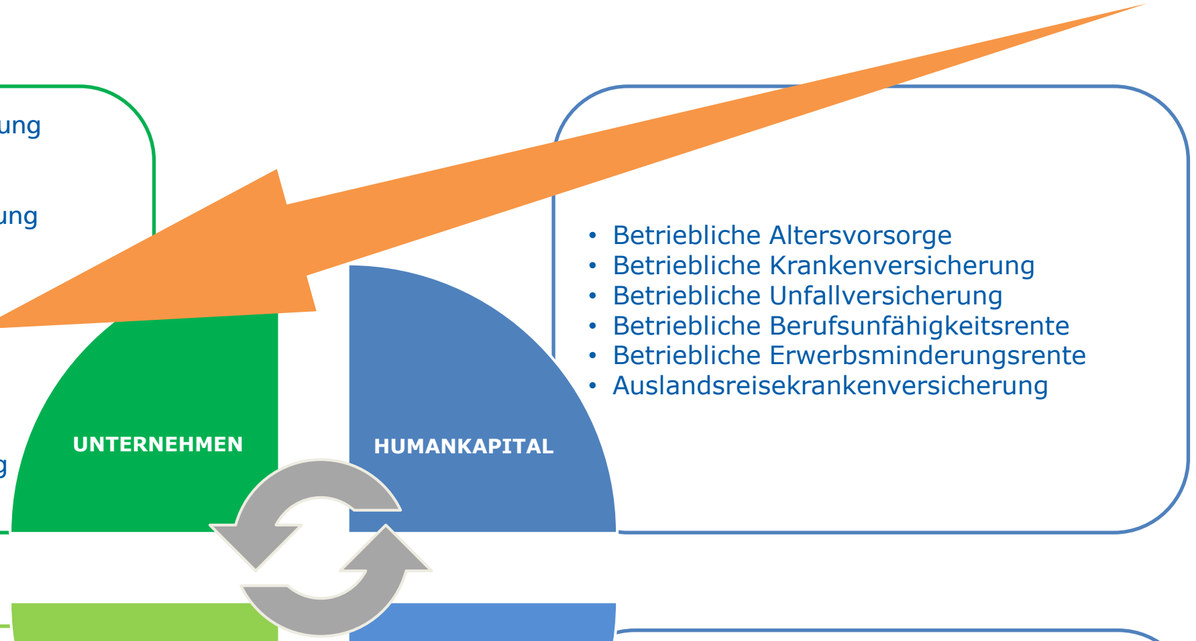
- Vier-Augen-Prinzip
- Regelmäßige Auditierungen
- Virenscanner & Firewall
- Patch-Management-Prozess
- ISMS Zertifizierung, Standards/Normen
- Zwei-Faktor Authentifizierung (2FA)
- Sensibilisierung Mitarbeiter
- Datensicherungssysteme

- Informationssicherheitsbeauftragte

Krisenhotline & Krisendienstleister

**und am Ende sollte eine passende Versicherungfür die Absicherung der finanziellen Folgen stehen!**

# Absicherungssphären eines Firmenkunden




- Betriebs-/ Berufshaftpflichtversicherung
- AGG-Versicherung
- Gebäudeversicherung
- Inventar-/ Maschinenbruchversicherung
- Elektronikversicherung
- Betriebsunterbrechungs- o. Betriebsschließungsversicherung
- **Cyberversicherung**
- Rechtsschutzversicherung
- Kautions-/ Kreditversicherung
- Bürgschaftsversicherung
- Transport-/ Ausstellungsversicherung
- Kfz-Flotten Versicherung

- Betriebliche Altersvorsorge
- Betriebliche Krankenversicherung
- Betriebliche Unfallversicherung
- Betriebliche Berufsunfähigkeitsrente
- Betriebliche Erwerbsminderungsrente
- Auslandsreisekrankenversicherung

- Managerhaftung D&O Versicherung
- Straf-Rechtsschutz
- Arbeitsunfähigkeit
- Berufsunfähigkeit
- Invalidität
- Key-Man Police
- Lohn-/ Gehaltsfortzahlung
- Risikoversicherung Todesfall / Erbschaftssteuer

- Privathaftpflichtversicherung
- Wohngebäudeversicherung
- Hausratversicherung
- Kfz-Versicherung
- Unfallversicherung
- Reiseversicherung
- Cyberversicherung
- Sammlungen-/ Kunstversicherungen
- Private Vorsorge
- Krankenversicherung
- Pflegeversicherung

DHS
VERSICHERUNGSMAKLER

## Netzwerksicherheitsverletzungen

## Datenrechtsverletzung, Datenmissbrauch und / oder Datenverlust

## Bedienfehler

## Cyber-Erpressung (auch Lösegelder)

# Absicherungsbausteine

## Prävention

- Aufklärung der Mitarbeiter
- Sensibilisierung für Verhaltensweisen bei der Nutzung moderner Kommunikationstechnologien
- Schulungstools für alle Mitarbeiter
- Notfall-/ Krisenplan

# Absicherungsbausteine

## Assistance

- IT-Forensik zur Analyse, Beweissicherung und Schadenbegrenzung
- Notfallhotline – direkter Zugriff auf Experten
- PR-Spezialisten für Krisenkommunikation
- Anwälte für IT- u. Datenschutzrechte

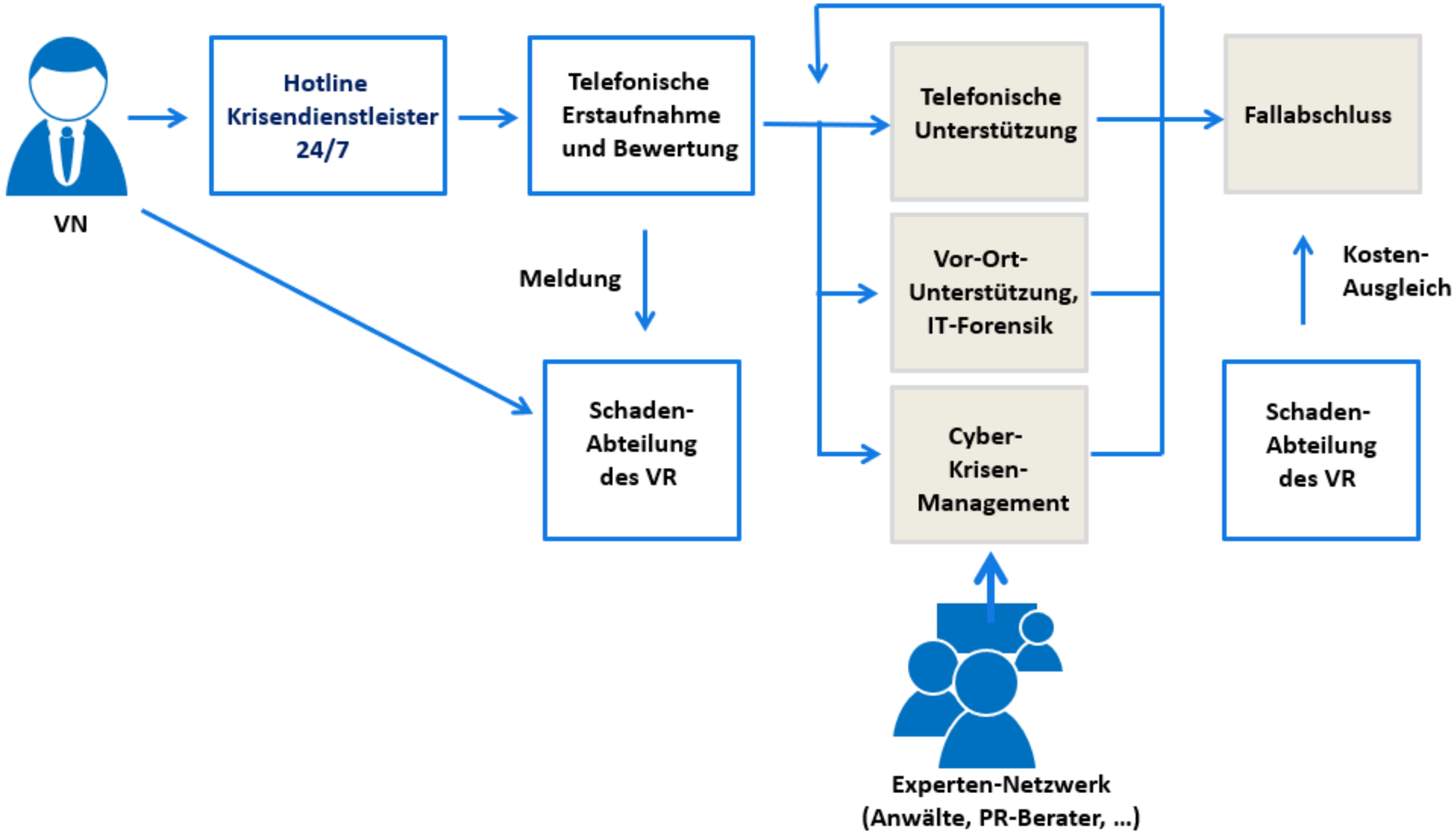
# Absicherungsbausteine

## Versicherung

- Kostenübernahme:
- Eigenschäden – wirtschaftlicher Schaden
- Betriebsunterbrechung
- Daten- u. Systemwiederherstellung
- Lösegeldzahlungen
- Drittschäden
- Schadenersatzforderungen durch Datenmissbrauch und/oder Lieferverzug

# Soforthilfe im Notfall

## (Feuerwehr/Versicherung)



DHS
VERSICHERUNGSMAKLER

# Ist eine Absicherung unverzichtbar?

- Schutz vor finanziellen Verlusten
- Schutz der Reputation
- Erfüllung von Compliance Anforderungen
- Unterstützung bei der Incident-Response
- Schutz vor menschlichen Versagens

- Optimismus
- Akzeptanz
- Lösungsorientierung
- positive Zukunftsplanung
- ein Erfolgsnetzwerk
- das Verlassen der Opferrolle
- und Selbstreflexion

DHS
VERSICHERUNGSMAKLER

# Kontakt zu uns:


**Christian Gerstung**

Direktor Kundenmanagement

Office: 0531 - 24 25 444
Mobil: 0175 - 77 69 927

E-Mail c.gerstung@dhs-makler.de

Haus der Versicherungen
Bankplatz 7a
D-38100 Braunschweig

# Dankeschön.

DHS
VERSICHERUNGSMAKLER