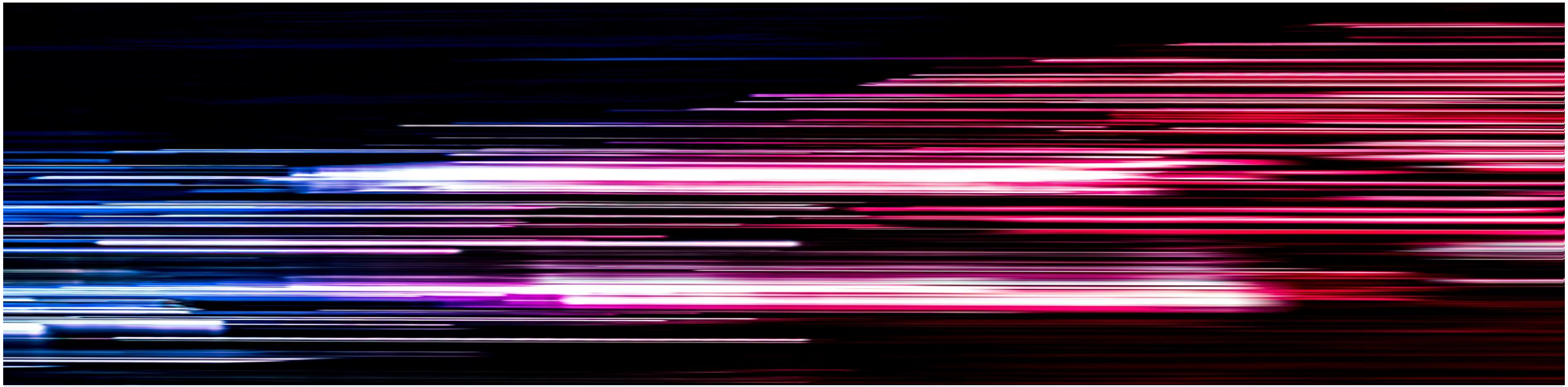
Graf von Westphalen



17.06.2026 I Cybersecurity Region Stuttgart Meetup

Haftungsfallen bei Cyberangriffen

Prävention, Kommunikation und Prozess-Strategien

Dr. Michael Herold | Dr. Martin Strauch

Mehr als 75 Jahre juristische Exzellenz

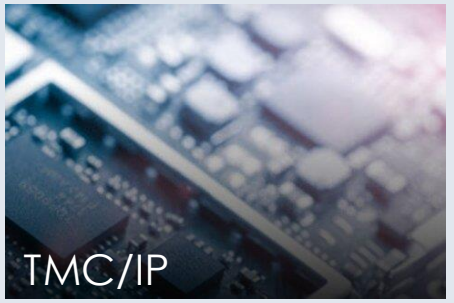
Mehr als 250 Anwältinnen und Anwälte

Standorte in allen Wirtschafts-zentren Deutschlands

Internationale Netzwerke mit mehr als 20.000 Köpfen

Full-Service im Wirtschaftsrecht aus einer Hand

Praxisgruppen



Fokusbereiche

203 Mrd.

EUR Schaden

jährlich durch Cyberangriffe (Bitkom)

72 Std.

Meldefrist bei Datenschutzverletzungen

u.a. 24 Std.

Meldefrist bei erheblichen Sicherheitsvorfällen

4 %

des Jahresumsatzes

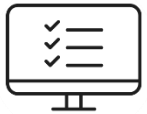
max. Bußgeld nach DSGVO

Quelle: Bitkom-Studie 2024, DSGVO Art. 83

Aktuelle Bedrohungslage in Deutschland

DSGVO

Art. 33/34: Meldepflicht binnen 72h
Bußgelder bis 20 Mio. EUR / 4% Umsatz



NIS2 / IT-SiG 2.0

Erweiterte Pflichten für KRITIS
Risikomanagement & Meldepflichten

GmbHG § 43

Persönliche Haftung des GF
Sorgfalt eines ordentlichen Kaufmanns

AktG §§ 91, 93

Risikofrüherkennungssystem
Business Judgment Rule

BSI-Gesetz

Pflichten gegenüber dem BSI
Meldepflichten bei Sicherheitsvorfällen

D&O-Haftung

Persönliche Haftung des Managements
Regress durch Versicherer möglich

Anonymisierte Beispielsfälle

Aus der Praxis: Was kann schiefgehen und welche Haftungsfolgen drohen?

1 Ransomware – Produktionsunternehmen

2 Datenleck – Online-Händler

3 CEO-Fraud – Finanzabteilung

Ransomware-Angriff

„Firma A“ – Mittelständisches Produktionsunternehmen, ca. 500 Mitarbeiter

Was geschah:

- Ransomware verschlüsselt zentrale Systeme
- Produktion steht 2 Wochen komplett still
- Kein aktueller Notfallplan vorhanden
- Backups veraltet und nicht einsetzbar
- IT-Sicherheitsbudget mehrfach gekürzt

Haftungsfolgen

3 Mio. EUR
Betriebsunterbrechungsschaden

120.000 EUR
Bußgeld (verspätete DSGVO-Meldung)

D&O-Regress
Versicherer prüft Regress gegen die Geschäftsführung

Datenleck durch mangelnde IT-Sicherheit

„Firma B“ – Online-Händler mit 200.000 Kundendaten

Was geschah:

- Veraltete Software mit bekannter Sicherheitslücke
- Patch seit Monaten verfügbar, aber nicht eingespielt
- Angreifer exfiltrieren Kundendaten
- Name, Adresse, Zahlungsdaten betroffen

Haftungsfolgen

800.000 EUR
DSGVO-Bußgeld

Sammelklage
Schadensersatz nach Art. 82 DSGVO durch betroffene Kunden

Reputationsschaden
Massiver Vertrauensverlust, Kundenabwanderung

CEO-Fraud / Phishing-Angriff

„Firma C“ – Finanzabteilung erhält gefälschte CEO-Mail

Was geschah:

- Gefälschte E-Mail gibt sich als CEO aus
- Überweisung von 1,5 Mio. EUR an betrügerisches Konto
- Kein Vier-Augen-Prinzip für hohe Überweisungen
- Geld nicht rückholbar

Haftungsfolgen

1,5 Mio. EUR

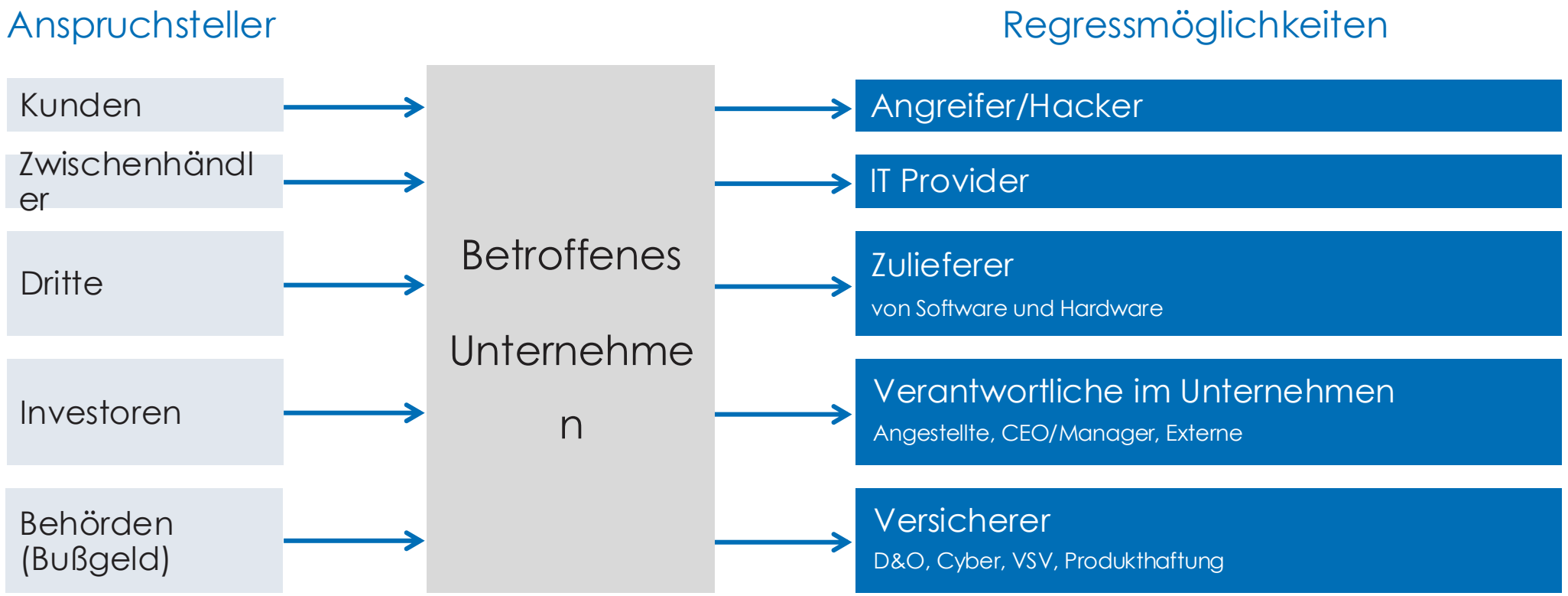
Verlust – nicht rückholbar

Persönliche Haftung

des CFO wegen Organisationsverschulden

Versicherungsschutz fraglich

Fehlende interne Kontrollen können Deckung ausschließen


Anspruchsteller
Kunden
Zwischenhändler
Dritte
Investoren
Behörden (Bußgeld)
Betroffenes Unternehmen
Regressmöglichkeiten
Angreifer/Hacker
IT Provider
Zulieferer
von Software und Hardware
Verantwortliche im Unternehmen
Angestellte, CEO/Manager, Externe
Versicherer
D&O, Cyber, VSV, Produkthaftung

Organisations-verschulden

Fehlende IT-Sicherheitsorganisation, keine klaren Verantwortlichkeiten, unzureichende Ressourcen

Compliance-Verletzung

Keine Risikoanalyse durchgeführt, keine regelmäßigen Audits, gesetzliche Pflichten nicht erfüllt

Mangelnde Dokumentation

Fehlende Nachweise über getroffene Maßnahmen, kein Compliance-Nachweis möglich

Verspätete Meldung

24-/72-Stunden-Frist versäumt, keine Benachrichtigung Betroffener, Bußgelder und Schadensersatz

Fehlende Cyber-Versicherung	Ohne angemessene Versicherung tragen Unternehmen und Geschäftsführer das volle Risiko selbst.
Keine Mitarbeiterschulungen	Ungeschulte Mitarbeiter sind das größte Einfallstor – ohne Schulungsnachweis droht Organisationsverschulden.
Unzureichendes Patch-Management	Bekannte Sicherheitslücken nicht zu schließen ist grob fahrlässig und führt fast immer zur Haftung.

Merke: Die Beweislast liegt beim Unternehmen – wer nicht dokumentiert, haftet.

Best Practices

Wie Sie Haftungsrisiken minimieren können.

I Prävention – Technisch & organisatorisch

II Kommunikation – Intern & extern

III Prozess-Strategie – Incident Response

I Prävention

— Regelmäßige Risikoanalysen

— Multi-Faktor-Authentifizierung

— Notfallpläne erstellen & testen

— Aktuelles Patch-Management

— Mitarbeiterschulungen

— Cyber-Versicherung

II Kommunikation

Intern:

— Mitarbeiter frühzeitig informieren
— Klare Anweisungen geben
— Kommunikationskette festlegen
— Vertraulichkeit sicherstellen

Extern:

— Behörden fristgerecht melden
— Betroffene benachrichtigen
— Proaktive Medienarbeit
— Juristisch abgestimmte Aussagen

III Prozess-Strategie

1 Incident-Response-Plan aktivieren

2 IT-Forensik & Anwälte einbinden

3 Beweissicherung durchführen

4 Versicherer & Behörden informieren

5 Lessons Learned

Checkliste zur Haftungsvermeidung

Die wichtigsten Schritte für Ihr Unternehmen

- Risikoanalyse durchführen – Regelmäßig IT-Risiken identifizieren und bewerten
- IT-Sicherheitsmaßnahmen implementieren – Firewalls, MFA, Patch-Management, Verschlüsselung
- Mitarbeiter schulen – Regelmäßige Phishing-Awareness-Trainings dokumentieren
- Notfallplan erstellen und testen – Incident-Response mit klaren Verantwortlichkeiten

Checkliste (Fortsetzung)

Meldeprozesse etablieren
72-Stunden-Frist DSGVO bzw. 24-/74-Stunden-Frist BSIG kennen und einhalten können

Cyber-Versicherung abschließen
Deckungsumfang regelmäßig prüfen und anpassen

Dokumentation pflegen
Alle Maßnahmen nachweisbar dokumentieren

Externe Experten benennen
IT-Forensik, spezialisierte Anwälte, PR-Berater vorab identifizieren

Key Takeaways

Cyberangriffe sind Chefsache
Geschäftsführer und Vorstände haften persönlich bei Pflichtverletzung.

Prävention schlägt Reaktion
Investitionen in IT-Sicherheit sind günstiger als Haftungsfolgen.

Dokumentation ist Pflicht
Ohne Nachweis keine Entlastung – dokumentieren Sie alle Maßnahmen.

Handeln Sie jetzt – bevor der Ernstfall eintritt.

Die beste Verteidigung gegen Haftung ist eine nachweisbar gute Vorbereitung.

Dr. Michael Herold, M.C.L.

m.herold@gvw.com
T +49 69 707970-169

Ulmenstraße 23-25
60325 Frankfurt a. M.

Dr. Martin Strauch, LL.M. (Edinburgh)

m.strauch@gvw.com
T +49 711 25087-130

Theodor-Heuss-Straße 21
70174 Stuttgart