# Vom Opfer zum Täter? Strafbarkeitsrisiken und Handlungsempfehlungen bei Ransomware-Angriffen

Dr. Nina Abel

Fachanwältin für Strafrecht

CYBER INSURANCE TALK

04. SEPTEMBER 2026

TAZ online, 01.09.2026

Hacker-Angriff auf Berliner Verwaltung

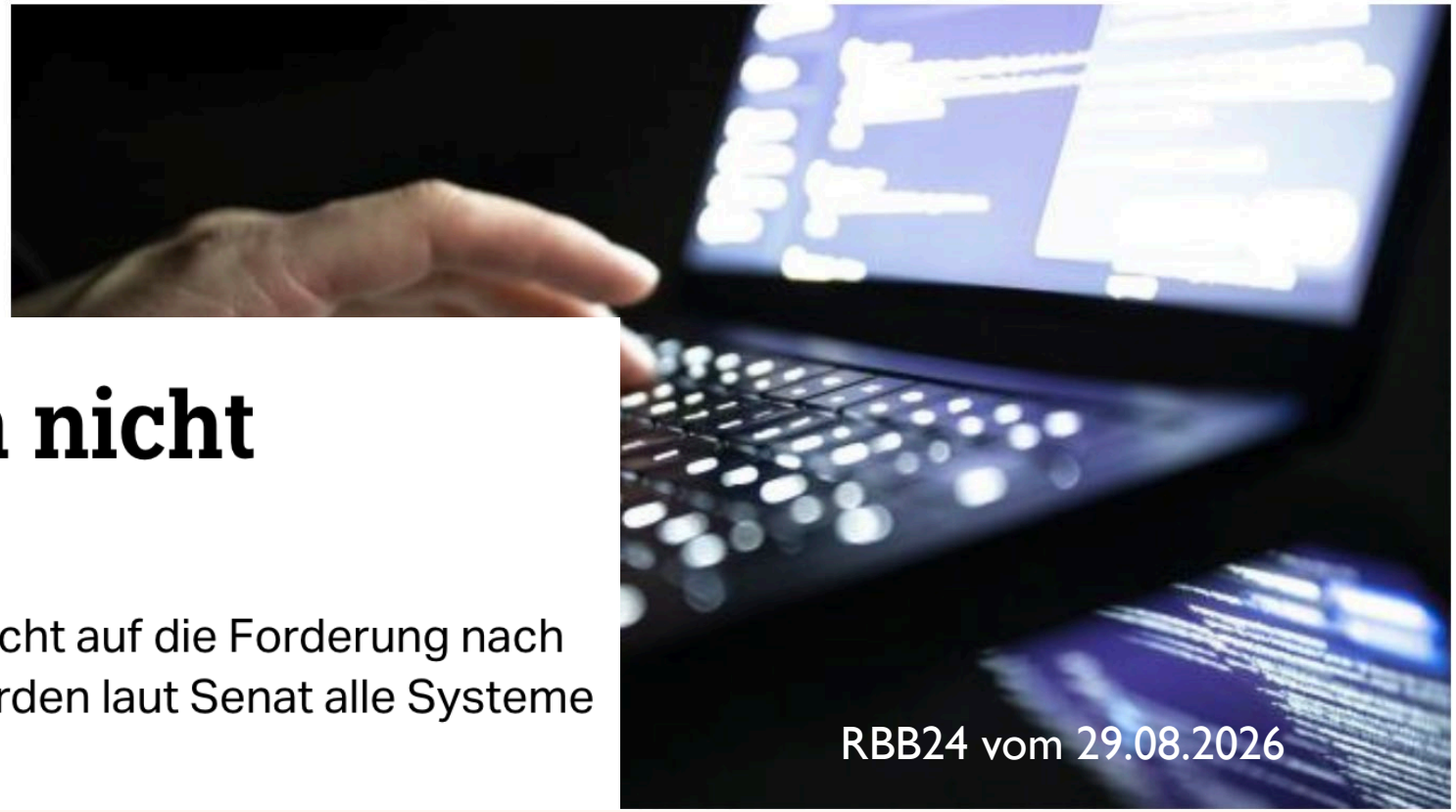
# „Das Land lässt sich nicht erpressen“

Die schwarz-rote Landesregierung will nicht auf die Forderung nach zwei Millionen Euro eingehen. Derzeit werden laut Senat alle Systeme untersucht.

Cyberangriff auf Berliner Landesnetz

# Hacker fordern rund zwei Millionen Euro in Bitcoin für gestohlene Daten

Sa 29.08.2026, 11:33 Uhr



RBB24 vom 29.08.2026

# AGENDA

1. Ransomware & der ökonomische Zwang hinter der Zahlung
2. Strafrechtliche Fallstricke der Lösegeldzahlung
3. Meldepflichten
4. Wen trifft welches Risiko?
5. Handlungsempfehlungen

# RANSOMWARE

- Massenphänomen mit steigendem Schadenspotenzial
- Double Extortion
- Triple Extortion
- Ransomware as a service (RaaS)

- Betriebsausfall
- Produktionsausfall
- Reputationsschaden

# ZAHLUNG

# = DIE GÜNSTIGSTE VON MEHREREN SCHLECHTEN OPTIONEN?

# STRAFRECHTLICHE FALLSTRICKE

- Beteiligung an einer (versuchten) Erpressung?
- Geldwäsche?
- Terrorismusfinanzierung?
- Untreue?

- Sanktionsverstoß, § 18 AWG
- Unterstützung einer kriminellen Vereinigung
- Steuerdelikte

# **Exkurs**: US-Recht → bußgeld- und strafbewehrter OFAC-Verstoß

- Geldstrafen bis 1 Mio. USD
- auch ohne Wissen um Listung
- Bezug: Abwicklung Lösegeldzahlung in USD über US-Banken und/oder Dienstleistungskette

# **Exkurs**: Verschärfte Geldwäsche Aufsicht durch AMLR, VO (EU) 2024/1624

- Erhöhte Sorgfaltspflichten für EU-Kryptobörsen (Art. 40 AMLR)

- Verbot anonymitätsverstärkender Kryptowerte (Art. 79 AMLR)

# ERMITTLUNGS-MAßNAHMEN


Anhaltspunkte
Amtsermittlung
Beweiserhebung

- Auskunftsersuchen an Unternehmen
- Zeugenschaftliche Befragungen
- Durchsuchung & Beschlagnahme (§ 103 StPO!)

# MELDEPFLICHTEN

# DSGVO

- Art. 33 DSGVO: binnen 72 h an Aufsichtsbehörde
  → Bußgeld bis 20 Mio. / 4 % weltweiter Jahresumsatz

- Art. 34 DSGVO: unverzüglich gegenüber Betroffenen
  → Bußgeld bis 10 Mio. / 2 % weltweiter Jahresumsatz
  → Schadensersatz

# Seit 01/2025: DORA (Meldung an BaFin)

- Ca. 22.000 EU-Unternehmen in Finanzsektor
- Gestufte Meldepflicht
- Bußgelder bis 10 Mio. Euro / 5 % weltweiter Jahresumsatz

## Seit 12/2025: NIS2 / BSIG (Meldung an BSI)

- Ca. 30.000 Unternehmen aus 18 Sektoren
- (besonders) wichtige Einrichtungen
- Gestufte Meldepflicht, Frühwarnung binnen 24 h
- Bußgelder bis 7 Mio. / 10 Mio. Euro

# OPTIONAL: STRAFANZEIGE

→ GRUNDLAGE FÜR STEUERUNG & KOOPERATION

# WEN TRIFFT DAS RISIKO?

# Unternehmen / juristische Person

- Bußgeld wegen Sanktionsverstoß, § 19 Abs. 7 AWG
- Bußgeld wegen unzureichender Sicherheitsmaßnahmen, Art. 5, Art. 32 DSGVO
- Bußgeld wegen verspäteter/unterbliebener Meldung, Art. 33 DSGVO

# Geschäftsführung

- Ggf. Innenhaftung ggü. Gesellschaft bei Sorgfaltspflichtverletzung
- Bußgeld wegen unzureichender Sicherheitsmaßnahmen, Art. 5, Art. 32 DSGVO
- Persönl. Verantwortlichkeit, § 38 BSIG
- Div. Straftatbestände, insb. Untreue

# Weitere Mitarbeiter

- Zivilrechtlich nur in Ausnahmefällen
- Selten: Untreue, § 266 StGB
- Zu anderen Straftatbeständen Beihilfe bei aktiver Mitwirkung unter Vorsatz

# Externe Dienstleister

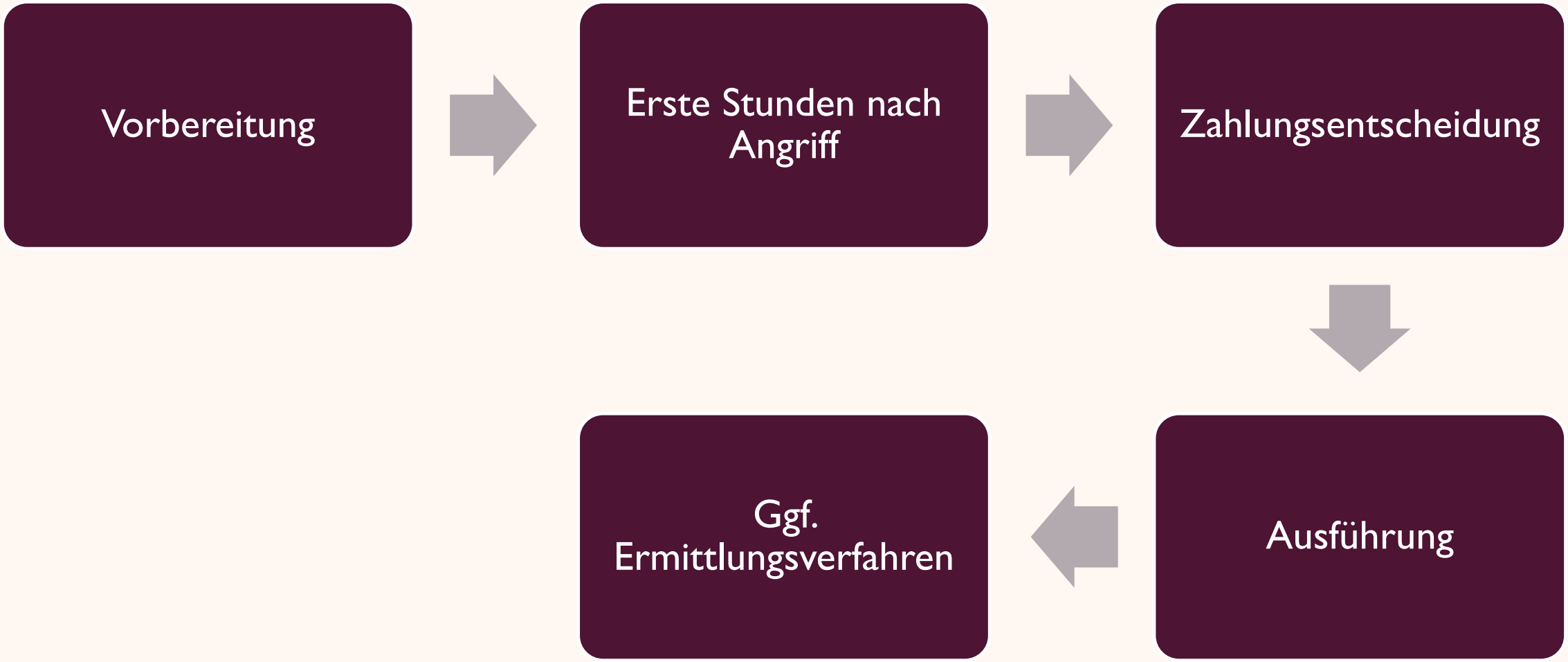
- Zivilrechtlich für Beratungsfehler
- Strafrechtliche Beihilfehandlung denkbar

# Cyber-Versicherer und Makler

- Zivilrechtlich aus Versicherungsvertrag bzw. Beratungshaftung

- Ggf. Beihilfe zu div. Straftatbeständen

# TO DO


Vorbereitung
Erste Stunden nach Angriff
Zahlungsentscheidung
Ausführung
Ggf. Ermittlungsverfahren

# Phase 0 - Vor dem Angriff

- Panel vorab kuratieren
- Eskalations- und Entscheidungswege festlegen
- Cyberversicherung kennen
- Durchsuchungsszenario durchspielen

# Phase 1 – Erste Stunden nach Entdeckung

- Forensische Sicherung; Attributionsversuche
- IR-Plan aktivieren
- One-Voice-Prinzip sofort etablieren
- Meldepflichten! DSGVO, BSIG/NIS2 u.a.

# Phase 2 – Zahlungsentscheidung

- Sanktions- und Attributionsprüfung
- Alternativenprüfung dokumentieren (Wiederherstellung aus Backups?)
- Ggf. Einbindung von Strafverfolungsbehörden (ZAC/BKA)

# Phase 3 – Ausführung der Zahlung

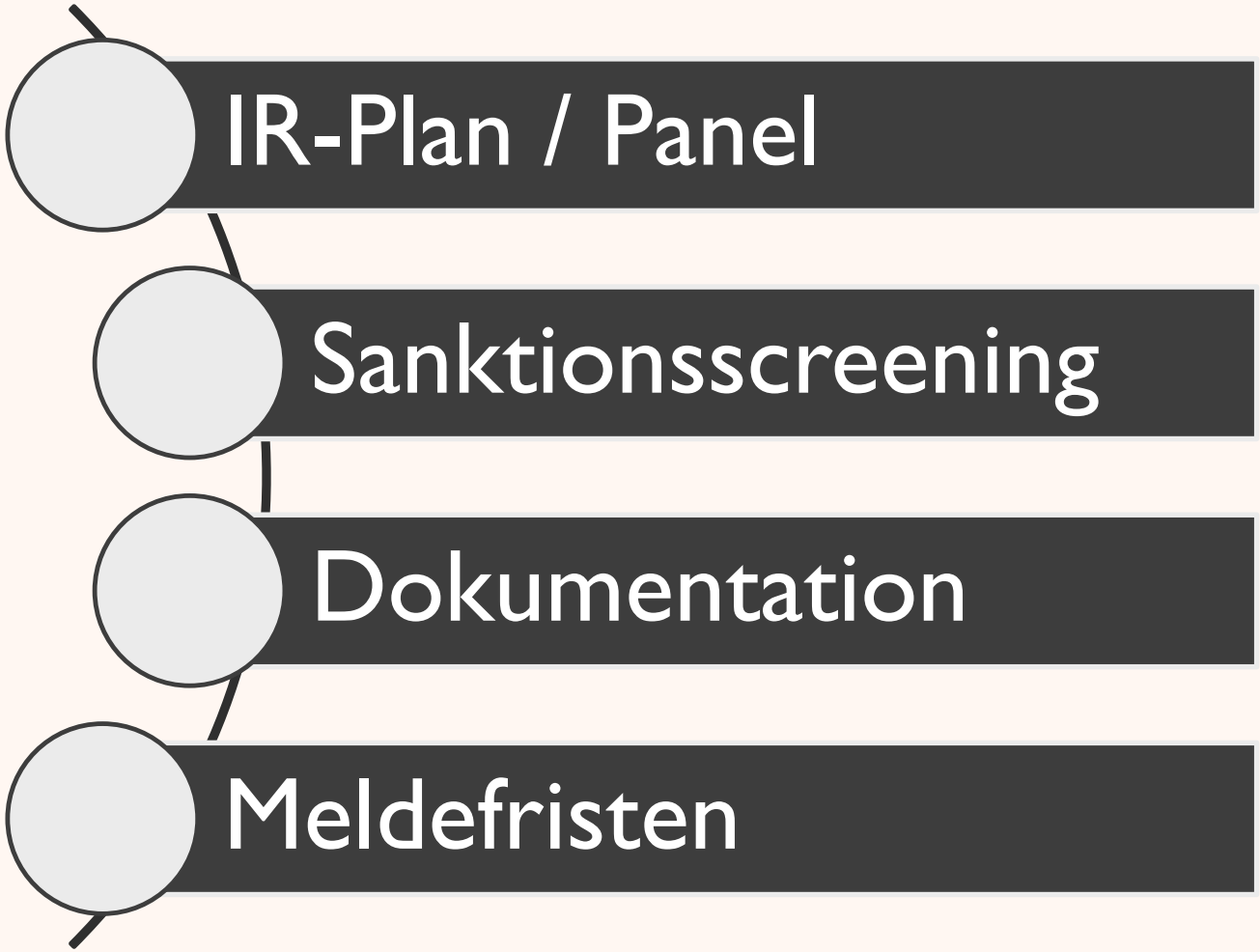
- Lizenzierte AMLR-/GwG-konformer Kryptowerte-Dienstleister
- Zeitpuffer für Verdachtsmeldung / Durchführungsverbot einplanen
- Ggf. zusätzliche OFAC-Prüfung

# Phase 4 – Ermittlungsverfahren

- Durchsuchung: Forensische Spiegelung statt Mitnahme
- Zeugenbefragungen: Anwaltlicher Beistand, keine Einflussnahme
- Auskunftsersuchen: anwaltliche Beratung (Selbstbelastung)

# Phase 5 – Nachbereitung

- Lessons Learned
- Ggf. Regressprüfung ggü. Versicherer und Dienstleistern
- Kooperative Verfahrensbeendigung anstreben (§§ 153, 153a StPO?)


IR-Plan / Panel
Sanktionsscreening
Dokumentation
Meldefristen

# Ausblick

Ransomware made in Switzerland

# International gesuchter Hacker in Zürich vor Gericht

Aus seiner Wohnung heraus soll ein Softwareentwickler Hunderte Firmen gehackt und erpresst haben. Nun steht er vor Gericht. Auf dem Prüfstand steht aber auch die Schweizer Strafverfolgung: Sind wir für moderne digitale Kriminalität gerüstet?

SRF online, 19.08.2026

# FRAGEN?

**Dr. Nina Abel**

Rechtsanwältin
Fachanwältin für Strafrecht

**E-Mail:** abel@abel-strafrecht.de
**Web:** abel-strafrecht.de

KANZLEI | ABEL
WIRTSCHAFTSSTRAFRECHT