Eine Lösegeldforderung ist keine IT-Frage.

Was vor einer Entscheidung über Verhandlung und Zahlung geklärt sein muss.

DIE ERSTEN STUNDEN

- **Kein Kontakt zu den Angreifern**, *bevor die Geschäftsführung festgelegt hat, wer verhandelt und mit welchem Ziel.*
- **Erpressernachricht sichern.** *Fundort und Zeitpunkt festhalten, Links nicht von Firmensystemen öffnen.*
- **Cyberversicherung informieren**, *bevor externe Dienstleister beauftragt werden.*
- **Anzeige erstatten.** *Sie zählt für Versicherung und spätere Verfahren.*
- **Entscheidungsprotokoll beginnen.** *Wer hat wann welche Information erhalten und was entschieden?*

MELDEPFLICHTEN GELTEN IMMER

Ob gezahlt wird oder nicht. **DSGVO** *Meldung an die Datenschutzbehörde möglichst binnen 72 Stunden.*

NISG 2026 *für wesentliche und wichtige Einrichtungen. Frühwarnung an das zuständige CSIRT binnen 24 Stunden, Meldung binnen 72 Stunden, Abschlussbericht nach einem Monat.*

FÜNF FRAGEN VOR JEDER ZAHLUNG

1 Können wir ohne Zahlung wiederherstellen?
Gibt es Backups, die der Angreifer nicht erreicht hat, und wurde ihre Wiederherstellung realistisch getestet? Auch eine Zahlung garantiert keinen schnellen Wiederanlauf.

2 Was kostet der Stillstand?
Entgangene Umsätze, Vertragsstrafen, Lieferverzug und die Wiederherstellung, die in jedem Fall anfällt.

3 Welche Daten sind abgeflossen?
Das klärt die forensische Analyse. Angaben der Angreifer sind ein Hinweis, kein Beweis, und ihre Löschzusage ist nicht überprüfbar.

4 Darf an diesen Empfänger gezahlt werden?
Sanktionsprüfung nach EU-Recht, etwa VO (EU) 2019/796, dazu die US-Sanktionslisten. Ein Treffer schließt jede Zahlung aus.

5 Was sagt die Versicherung?
Deckung, Zustimmungspflichten und vorgegebene Dienstleister. Eine Zahlung ohne Abstimmung kann den Schutz gefährden.

Verhandeln heißt nicht zahlen.

Eine professionell geführte Verhandlung verschafft Zeit, klärt, welche Daten die Angreifer wirklich besitzen, und macht aus einer Drohung ein geprüftes Angebot. Die Entscheidung bleibt bei der Geschäftsführung, dokumentiert in einem Beschluss.

verhandlung.jetzt
+43 664 144 83 63

Michael Meixner, allgemein beeideter und gerichtlich zertifizierter Sachverständiger für IT-Sicherheit und Computerforensik