DAVID ZION · vCISO UND STRATEGISCHE BERATUNG

# vCISO im Vollmandat und im Beirat

Externer CISO · ISMS nach ISO 27001 · NIS2 · Bericht an die Geschäftsführung

davidzion.de · kontakt@davidzion.de · Hamburg (+100 km) und remote

**Informationssicherheit braucht eine Stelle, die entscheidet, priorisiert und der Geschäftsführung berichtet.** Als vCISO übernehme ich diese Rolle auf Zeit, ohne die Kosten einer Vollzeitstelle. Wer im Erstgespräch sitzt, führt auch das Mandat. Vereinbarte Maßnahmen begleite ich bis zur nachvollziehbaren und termingerechten Umsetzung.

## WAS ICH ÜBERNEHME

- **Strategie und Roadmap:** eine Sicherheitsstrategie passend zu Risikoprofil, Branche und Budget, mit priorisierter Roadmap statt einer Sammlung von Einzelmaßnahmen.
- **ISMS und Compliance:** Aufbau und Pflege eines Managementsystems im Einklang mit ISO 27001, NIS2 und BSIG, inklusive Vorbereitung auf Audits und Zertifizierung.
- **Berichtslinie an die Leitung:** fester Berichtsrhythmus, verständliche Lageberichte und Unterstützung der Geschäftsführung bei ihren persönlichen Pflichten aus § 38 BSIG.
- **Lieferanten und Dienstleister:** Bewertung der wesentlichen Dienstleister, Anforderungen im Vertrag und eine dokumentierte Prüfung, wie sie § 30 Abs. 2 Nr. 4 BSIG verlangt.

## PASSEND, WENN

- die Zuständigkeit für Informationssicherheit offen ist oder an einer Person ohne Mandat und Berichtsweg hängt
- NIS2, das KRITIS-Dachgesetz oder Ihre Kunden einen belastbaren Nachweis verlangen
- eine Zertifizierung nach ISO 27001 in absehbarer Zeit ansteht
- eine CISO-Stelle vakant ist und eine Übergangslösung gebraucht wird. Auf Wunsch befähige ich parallel eine interne Kraft, die Rolle später zu übernehmen

## VIER STUFEN, BERATERTAGE IM MONAT

- **Security-Beirat, 1 Tag:** Security-Report an die Geschäftsführung, Rückfragen zwischen den Terminen
- **vCISO Standard, 2 Tage:** zusätzlich Begleitung des ISMS, Risikoregister, fester Berichtsrhythmus
- **vCISO Plus, 3 bis 4 Tage:** Verantwortung für das Managementsystem, Audits, Meldeprozess, Schulungen
- **Vollmandat, 8 bis 12 Tage:** Führung der Sicherheitsorganisation, Kommunikation mit Behörden

## HONORAR UND KONDITIONEN

- **Security-Beirat:** 2.500 € im Monat, Mindestlaufzeit sechs Monate
- **Ab Stufe zwei** hängt das Honorar am Zuschnitt: Geltungsbereich, Standorte und Aufgaben, die im Haus bleiben
- **Wechsel der Stufe** zum Ende eines Vertragsmonats, in beide Richtungen
- **Start** in der Regel binnen zwei Wochen

Zum Vergleich: Ein fest angestellter CISO kostet je nach Markt rund 120.000 bis 180.000 € im Jahr, dazu Suche und Einarbeitung.

Über 40 Jahre in der IT, davon mehr als 30 in Führungsverantwortung
CISM · ISO/IEC 27001 Lead Implementer · ISO/IEC 42001 KI-Manager · AI Compliance nach EU AI Act

**Erstgespräch: 30 Minuten, kostenfrei · Angebot binnen 48 Stunden · davidzion.de**

Stand 19. November 2026. Alle Preise netto zzgl. MwSt. Die Angaben zur Rechtslage ersetzen keine Rechtsberatung.