PILS
Cyber Defence

INTEGRIERTES CYBER-, INFORMATIONS- UND GEHEIMSCHUTZ-MANAGEMENT

Für Unternehmen mit Bedarf an Geheimschutzbetreuung
und SUB-Erfordernis gemäß §§ 11 ff Informationssicherheitsgesetz

Unser Mandat

Wir liefern das Know-how für Unternehmen, die in sicherheitskritischen Umgebungen operieren und Anforderungen an Geheimschutz, Informationssicherheit und industrielle Sicherheit erfüllen müssen.

Diese Unternehmen bewegen sich in einem regulatorischen Umfeld, in dem digitale Risiken nicht nur wirtschaftliche Schäden verursachen, sondern nationale Sicherheitsinteressen, Geheimschutzpflichten und behördliche Auflagen berühren. Unser Ansatz basiert auf einem systemischen Sicherheitsverständnis, das technische, personelle, physische und organisatorische Aspekte integriert sowie risikoorientiert, prozessorientiert und behördenfähig dokumentiert.

Leistungsportfolio

1. Geheimschutzbetreuung gemäß §§ 11 ff InfoSiG

Wir übernehmen die strukturierte Betreuung von Unternehmen, die eine Sicherheitsunbedenklichkeitsbescheinigung (SUB) benötigen oder bereits als geheimschutzbetreut geführt werden.

Leistungen:

- Vorbereitung und Begleitung im SUB-Verfahren
- Aufbau einer prüfbaren Geheimschutzorganisation
- Unterstützung des Sicherheitsbeauftragten (SiBe)
- Erstellung von Geheimschutzrichtlinien und Verfahrensanweisungen
- Implementierung von Klassifizierungs- und Berechtigungssystemen
- Schulung von Personal mit VS-Zugang
- Vorbereitung auf behördliche Überprüfungen und Audits

Geheimschutz wird als integraler Bestandteil des unternehmensweiten Sicherheits- und Risikomanagements verankert – nicht als isolierte Compliance-Funktion.

2. Integrierte Risikoanalyse & Sicherheitsarchitektur

Wir führen eine strukturierte, ganzheitliche Risikoanalyse durch, die technische, organisatorische und personelle Gefährdungslagen erfasst:

- Identifikation sicherheitskritischer Assets (VS-Daten, Entwicklungsumgebungen, Kryptomaterial, Schlüsselpersonal, IT-Systeme)
- Bewertung von Cyber-, Betriebs- und Geheimschutzrisiken
- Priorisierung von Maßnahmen nach Eintrittswahrscheinlichkeit und Schadensausmaß
- Abstimmung mit Geschäftsführung, Sicherheitsbeauftragten und Behördenanforderungen

Ziel: Ein integriertes Sicherheitsmanagement, das technische, organisatorische und personelle, infrastrukturelle Maßnahmen kohärent miteinander verzahnt und eine klare Sicherheitsarchitektur für alle Schutzzonen definiert.

3. Herstellung von Zugriffs- und Lagerfähigkeit für Verschlusssachen

Ein zentrales Element der Geheimschutzbetreuung ist die Herstellung und Aufrechterhaltung der Zugriffs- und Lagerfähigkeit für Verschlusssachen.

Schwerpunkte:

- Definition von Sicherheitszonen und Zutrittsregelungen
- Herstellung von Verwaltungs- und Sicherheitsbereichen
- Auswahl zugelassener Sicherheitsbehältnisse
- Einleitung der Sicherheitsüberprüfung gem. MBG oder SPG
- Konzeption von Alarm- und Überwachungssystemen
- Schlüssel- und Dokumentationsmanagement
- Durchsetzung des Need-to-Know-Prinzips
- Rollen- und Berechtigungskonzepte
- Protokollierung und Nachvollziehbarkeit

4. Implementierung von IKT-Systemen nach nationalen, EU- und NATO-Standards

Wir begleiten Unternehmen bei der Konzeption, Implementierung und Härtung von IKT-Systemen, die für die Verarbeitung von Verschlusssachen geeignet und akkreditierungsfähig sind.

Schwerpunkte:

- Architektur von VS-fähigen IT- und OT-Systemen
- Auswahl sicherheitstechnisch geeigneter und zertifizierter Komponenten
- Härtung von Server-, Client- und Netzwerksystemen
- Netzwerksicherheitsarchitekturen (Zoning, DMZ, Air-Gap-Konzepte)
- Kryptokonzeption und Schlüsselmanagement
- Identitäts- und Berechtigungsmanagement (IAM/PAM)
- Vorbereitung technischer Akkreditierungen und Zulassungsverfahren
- Netzwerksegmentierung nach Klassifizierungsstufen
- Strikte Trennung klassifizierter und unklassifizierter Umgebungen
- Zugriffskontrolle und Identitätsmanagement
- Logging-, Monitoring- und SIEM-Strukturen
- Integritäts- und Verfügbarkeitskonzepte (inkl. Backup/Recovery)

Alle Maßnahmen werden so dokumentiert, dass sie behördenfähig, auditierbar und dauerhaft nachvollziehbar sind.

5. Incident-Readiness & Sicherheitssteuerung

Wir befähigen Unternehmen, sicherheitsrelevante Vorfälle strukturiert zu erkennen, zu bewerten und zu bewältigen – insbesondere bei Kompromittierung von Verschlusssachen oder kritischen Systemen.

Schwerpunkte:

- Entwicklung klarer Melde- und Eskalationswege (intern/extern/behördlich)
- Erstellung von Incident-Response-Szenarien für VS-Kompromittierung
- Table-Top-Übungen für Führungskräfte und Sicherheitsfunktionen
- Dokumentierte Entscheidungs- und Due-Diligence-Prozesse
- Einbindung von Lieferkette und externen Partnern in das Sicherheitskonzept
- Forensik-Readiness und Chain-of-Custody-Verfahren
- Durchsetzung des Need-to-Know-Prinzips
- Rollen- und Berechtigungskonzepte
- Protokollierung und Nachvollziehbarkeit

Ihr strategischer Mehrwert

- **Erlangung und Erhalt der Sicherheitsunbedenklichkeitsbescheinigung (SUB) gem. InfoSiG**
- **Rechtssichere, auditfähige Geheimschutzorganisation** – dokumentiert, prozess-orientiert, behördenfähig
- **Nachweisbare Cyber-Resilienz** in sicherheitskritischen Umgebungen
- **Reduzierung regulatorischer, haftungsrechtlicher und Reputationsrisiken**
- **Strukturierte, professionelle Sicherheitsführung** mit klaren Verantwortlichkeiten und Governance-Mechanismen
- **Vertrauen bei Behörden, Auftraggebern und Partnern**

Wenn Ihr Unternehmen...

- eine Sicherheitsunbedenklichkeitsbescheinigung gemäß §§ 11 ff InfoSiG benötigt,
- seine bestehende Geheimschutz- und Cyber-Architektur professionalisieren möchte,
- sicherheitskritische IT-/OT-Systeme betreibt oder
- mit klassifizierten Informationen arbeitet,

...begleiten wir Sie von der Analyse über die Implementierung bis zur nachhaltigen Governance – **strukturiert, behördenfähig und risikoorientiert.**