Checkliste

Vorkehrungen gegen Informationsabfluss

1. Welche Sicherheitsvorkehrungen haben Sie im IT-Bereich getroffen, um sich gegen Spionage/Informationsabfluss zu schützen?

- ❑ Firewall
- ❑ Passwortschutz auf allen Geräten
- ❑ Hohe Standards bei der IT-Sicherheit
- ❑ Kontinuierliches Monitoring sämtlicher Daten in der Unternehmens-EDV
- ❑ Brenner, USB-Ports o.Ä. nur an ausgewählten Desktop-PCs bzw. Laptops
- ❑ Verschlüsselter E-Mail-Verkehr
- ❑ Internetzugang nur für ausgewählte Mitarbeiter
- ❑ Zertifizierung nach BSI-Standard
- ❑ Intrusion-Detection-Systeme zur Prüfung der Anfälligkeit
- ❑ Nur ausgewählter Einsatz von Head-Sets, Funktastaturen oder Funkmäusen
- ❑ Weitere Sicherheitsmaßnahmen:

2. Welche Sicherheitsvorkehrungen haben Sie im Bereich Personal getroffen?

- ❑ Geheimhaltungsverpflichtungen in Arbeitsverträgen
- ❑ Personalfördernde Maßnahmen zur Steigerung der Verbundenheit mit den Unternehmen
- ❑ Sensibilisierung der Mitarbeiter zu den Gefahren von Spionage
- ❑ Background-Checks vor der Besetzung von sensiblen Positionen
- ❑ Moderne Personaldiagnostiken bei der Einstellung von neuen Mitarbeitern
- ❑ Integritätstest für neue Bewerber
- ❑ Pre-Employment-Screening

- ❑ Whistle-Blowing-System für Hinweise auf verdächtiges Verhalten
- ❑ Weitere Sicherheitsmaßnahmen:

3. Welche prozesstechnischen Vorkehrungen haben Sie getroffen, um sich gegen Industriespionage zu schützen?

- ❑ Klare Regeln über den Umgang mit schützenswerten Informationen
- ❑ Geheimhaltungsverpflichtungen für Geschäftspartner
- ❑ Bestellung eines Sicherheitsverantwortlichen
- ❑ Sorgfältige Auswahl der Geschäftspartner (Background-Check)
- ❑ Eindeutige Kennzeichnung und Klassifizierung von Firmen- oder Betriebsgeheimnissen
- ❑ Regelmäßige Prüfung der Prozessabläufe durch externe Spezialisten
- ❑ Clean-Desk-Policy
- ❑ Informationsschutzkonzept
- ❑ Abhörsichere Kommunikation (Telefon, Fax, E-Mail)
- ❑ Weitere Sicherheitsmaßnahmen:

4. Welche Sicherheitsvorkehrungen haben Sie im Bereich Objektsicherheit getroffen?

- ❑ Zugangskontrollen zum Firmenareal (technisch oder personell)
- ❑ Überwachung besonders sensibler Bereiche (Videoüberwachung, Zugangskontrollen etc.)
- ❑ Besonders gesicherter Serverbereich (Sicherheitsvorkehrungen gegen HPM-Waffen)
- ❑ Regelmäßige Untersuchung auf Wanzen durch Spezialisten
- ❑ Vorhandensein von abhörsicheren Räumen
- ❑ Weitere Sicherheitsmaßnahmen: