Erweiterter Fragebogen

(für kritische Lieferanten)

Anwendungsfälle:

- Softwarelieferanten
- Cloud-Anbieter
- Fernwartungsdienstleister
- SPS-/Steuerungslieferanten
- Entwicklungsdienstleister
- Anbieter mit Zugriff auf Produktionssysteme

Bearbeitungszeit typischerweise 30–60 Minuten.

---

1. Governance

Existiert ein Informationssicherheitsmanagementsystem?

◯ Ja ◯ Nein

Wird das ISMS regelmäßig auditiert?

◯ Intern ◯ Extern ◯ Beides ◯ Nein

---

2. Asset- und Risikomanagement

Werden IT-Assets inventarisiert?

◯ Ja ◯ Nein

Werden Cyber-Risiken regelmäßig bewertet?

◯ Jährlich ◯ Ad hoc ◯ Nein

Existiert ein dokumentierter Risikomanagementprozess?

◯ Ja ◯ Nein

---

3. Zugriffsschutz

Ist MFA für privilegierte Konten verpflichtend?

◯ Ja ◯ Nein

Werden Administratorrechte regelmäßig überprüft?

◯ Ja ◯ Nein

Werden Zugriffe protokolliert?

◯ Ja ◯ Nein

---

4. Schwachstellenmanagement

Werden Schwachstellenscans durchgeführt?

◯ Monatlic ◯ Quartalsweise ◯ Seltener

Werden Penetrationstests durchgeführt?

◯ Jährlich ◯ Gelegentlich ◯ Nein

Frist zur Behebung kritischer Schwachstellen:

◯ < 7 Tage ◯ < 30 Tage ◯ > 30 Tag

---

5. Incident Response

Existiert ein dokumentierter Incident-Response-Plan?

◯ Ja ◯ Nein

Werden Übungen durchgeführt?

◯ Jährlich ◯ Unregelmäßig ◯ Nein

Verpflichten Sie sich zur Meldung von Sicherheitsvorfällen innerhalb von 24 Stunden?

◯ Ja ◯ Nein

---

6. Business Continuity

Existiert ein Business-Continuity-Plan?

◯ Ja ◯ Nein

Werden Backups regelmäßig getestet?

◯ Ja ◯ Nein

Gibt es definierte Wiederanlaufzeiten?

◯ Ja ◯ Nein

---

7. Sichere Softwareentwicklung (CRA relevant)

Existiert ein Secure Development Lifecycle?

◯ Ja ◯ Nein

Werden Entwickler in Secure Coding geschult?

◯ Ja ◯ Nein

Werden Code Reviews durchgeführt?

◯ Ja ◯ Nein

Werden folgende Verfahren eingesetzt?

- ☐ SAST
- ☐ DAST
- ☐ Dependency Scanning
- ☐ Container Scanning

Werden Open-Source-Komponenten überwacht?

◯ Ja ◯ Nein

Können Sie eine SBOM bereitstellen?

◯ Ja ◯ Nein

Werden Software-Updates digital signiert?

◯ Ja ◯ Nein

---

8. Produkt- und Schwachstellenmanagement

Existiert ein Verfahren zur Annahme externer Schwachstellenmeldungen?

◯ Ja ◯ Nein

Existiert eine veröffentlichte Vulnerability Disclosure Policy?

◯ Ja ◯ Nein

Werden Kunden über kritische Schwachstellen informiert?

◯ Ja ◯ Nein

---

9. Fernzugriff und OT-Sicherheit

Besteht Fernzugriff auf Kundenanlagen?

◯ Ja ◯ Nein

Falls ja:

Wird MFA eingesetzt?

◯ Ja ◯ Nein

Werden Sitzungen protokolliert?

◯ Ja ◯ Nein

Kann der Kunde den Fernzugriff aktiv freigeben oder sperren?

◯ Ja ◯ Nein

Werden Standardpasswörter vermieden?

◯ Ja ◯ Nein

---

10. Unterauftragnehmer

Werden Unterauftragnehmer bewertet?

◯ Ja ◯ Nein

Werden Sicherheitsanforderungen vertraglich weitergegeben?

◯ Ja ◯ Nein

Werden kritische Unterauftragnehmer regelmäßig überprüft?

◯ Ja ◯ Nein

Bewertungsvorschlag

Eine einfache Bewertung könnte so aussehen:

Ergebnis	Bewertung
≥ 85 %	Niedriges Risiko
70–84 %	Mittleres Risiko
50–69 %	Erhöhtes Risiko
< 50 %	Hohes Risiko

Zusätzlich sollten einige **K.-o.-Kriterien** definiert werden, z. B.:

- kein Verfahren zur Behandlung von Sicherheitsvorfällen,
- keine MFA bei Fernzugriffen,
- keine Kontrolle privilegierter Konten,
- keine Prozesse für Schwachstellenmanagement,

- keine Möglichkeit zur Bereitstellung von Sicherheitsupdates bei Softwarelieferanten.

Die Kombination aus Basis- und erweitertem Fragebogen wird in der Praxis häufig als ausreichend angesehen, um die Lieferanten-bewertung im Kontext von C-SCRM sowie die lieferkettenbezogenen Erwartungen von NIS2 und CRA strukturiert nachzuweisen.