Schwachstellen- und Lieferkettenmanagement

Abhängigkeiten, sichere Entwicklung, Updates, Offenlegung und Dienstleisterrisiken.

Version 1.0 | Stand 18.08.2026 | Prüfgrundlage

Versorgia - Schwachstellen- und Lieferkettenmanagement
Version: 1.0
Stand: 18.08.2026
Status: Prüfgrundlage
Zielgruppen: Entwicklung, Informationssicherheit, Einkauf

Prüfziel
Abhängigkeiten, sichere Entwicklung, Updates, Offenlegung und Dienstleisterrisiken.

1. Software und Abhängigkeiten
- Komponenten, Versionen, Herkunft, Lizenz, Supportende und bekannte Schwachstellen nachvollziehbar führen.
- Codeprüfung, Tests, Geheimnisprüfung, Build- und Freigabeverfahren vor Änderungen anwenden.

2. Bewertung und Behebung
- Meldung, Triage, Kritikalität, Exponierung, Behebungsfrist, Ausnahme und Wirksamkeitsprüfung dokumentieren.
- Verantwortung für Sicherheitsupdates und Kundeninformation vertraglich abgrenzen.

3. Lieferkette
- Hosting, Bibliotheken, Zertifikatsstellen, Versand-, Support- und Monitoringdienste in die Risikobewertung aufnehmen.
- Austauschbarkeit, Konzentrationsrisiko, Vorfallpflichten und Exit je kritischem Anbieter bewerten.

4. Quellen und Prüfmaßstab

- § 30 BSIG: Risikomanagementmaßnahmen: https://www.gesetze-im-internet.de/bsig_2025/__30.html
- BSI C5:2020 für Cloud-Kontrollen und Kundentransparenz: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/C5_2020.pdf?__blob=publicationFile&v=3

Einordnung

Dieses Dokument ist eine strukturierte Prüf- und Abstimmungsgrundlage. Es ist kein Zertifikat, kein Prüfbericht einer unabhängigen Stelle und keine Rechtsberatung. Offene Betreiber-, Hosting-, Vertrags- und Abnahmeangaben müssen vor Produktivfreigabe mit Nachweisen ergänzt und von den zuständigen Stellen freigegeben werden.

Öffentliche Prüfgrundlage von Versorgia. Kein Zertifikat, kein unabhängiges Testat und keine Rechtsberatung.