



Holger Reibold

Supply Chain Security Audit

Handbuch für
prüfungssichere Lieferketten
– NIS-2, DORA und ISO 28000
sicher umsetzen

BRAIN-MEDIA.DE

Audit-Checklisten

Die folgenden Audit-Checklisten dienen als praxisorientiertes Instrument zur strukturierten Bewertung der Supply-Chain-Security. Sie ermöglichen eine systematische Überprüfung zentraler Kontrollen, Prozesse und organisatorischer Maßnahmen entlang der Lieferkette.

Ziel ist es, Auditoren und Verantwortlichen eine klare Orientierung zu geben, welche Anforderungen geprüft werden sollten und wie sich der Reifegrad der eigenen Organisation einschätzen lässt. Die Checklisten sind bewusst risikoorientiert aufgebaut und orientieren sich an regulatorischen Vorgaben wie NIS-2, DORA und dem Cyber Resilience Act. Sie können sowohl für interne Assessments als auch im Rahmen externer Audits eingesetzt und bei Bedarf an organisationsspezifische Anforderungen angepasst werden.

1. Lieferanten & Governance

- Sind alle kritischen Lieferanten identifiziert und klassifiziert?
- Liegt eine Übersicht aller Drittanbieter (inkl. Tier-n) vor?
- Werden Lieferanten regelmäßig risikobasiert bewertet?
- Existiert ein dokumentierter Due-Diligence-Prozess?
- Sind Sicherheitsanforderungen vertraglich definiert?
- Sind Auditrechte gegenüber Drittanbietern eindeutig geregelt?
- Sind Sub-Outsourcing-Beziehungen transparent und bewertet?

- Existieren Prozesse zur Überwachung von Drittparteirisiken?

2. Zugriff & Netzwerksicherheit

- Sind Zugriffskontrollen nach Least-Privilege-Prinzip umgesetzt?
- Ist Multi-Faktor-Authentifizierung für kritische Zugriffe aktiv?
- Sind Netzwerkzugriffe von Dritten segmentiert und überwacht?
- Werden alle Zugriffe protokolliert und regelmäßig ausgewertet?

3. Software Supply Chain / SBOM

- Existiert eine vollständige und aktuelle SBOM?
- Wird die SBOM automatisiert in der CI/CD-Pipeline erzeugt?
- Sind Softwareartefakte signiert und auf Integrität geprüft?
- Erfolgt ein regelmäßiger Abgleich mit bekannten Schwachstellen?
- Ist die Traceability von Komponenten zu Risiken sichergestellt?

4. Monitoring & Schwachstellenmanagement

- Sind Monitoring- und Logging-Prozesse implementiert/wirksam?
- Werden Schwachstellen regelmäßig identifiziert und priorisiert?

- Existieren Prozesse zur Behebung von Sicherheitslücken?

5. Operative Sicherheit

- Ist ein Incident-Response-Prozess definiert und getestet?
- Sind Drittanbieter in Incident-Response-Prozesse eingebunden?
- Existiert ein Business-Continuity-Plan für kritische Lieferanten?
- Werden Notfallpläne regelmäßig getestet und aktualisiert?

6. Prozesse & Organisation

- Gibt es ein strukturiertes Change-Management?
- Bewertung sicherheitsrelevanter Änderungen vor der Umsetzung?
- Ist Awareness für Supply-Chain-Security etabliert?

7. Reporting & Compliance

- Existiert ein regelmäßiges Reporting zu Risiken/Sicherheitsstatus?
- Werden KPIs und KRIs zur Steuerung verwendet?
- Ist die Nachweisbarkeit aller Kontrollen sichergestellt?
- Werden Anforderungen aus NIS-2, DORA und CRA erfüllt?

Mehr zum Thema

Der vollständige Leitfaden „Supply Chain Security Audit“

 [Jetzt bei Amazon bestellen](#)