Reifegradmodell

Das Reifegradmodell dient der strukturierten Bewertung des aktuellen Entwicklungsstands der Supply-Chain-Security innerhalb einer Organisation. Es ermöglicht eine fundierte Einordnung bestehender Maßnahmen, identifiziert gezielt Verbesserungspotenziale und unterstützt die Priorisierung von Weiterentwicklungen. Die Bewertung erfolgt entlang definierter Stufen, die den Grad der Formalisierung, Integration, Messbarkeit und Wirksamkeit von Sicherheitsmaßnahmen widerspiegeln. Neben Prozessen werden auch Governance, Technik, Nachweisfähigkeit und Integration in regulatorische Anforderungen berücksichtigt.

Level 1 – Initial (ad hoc)

Sicherheitsmaßnahmen sind überwiegend reaktiv und werden situativ umgesetzt. Es existieren keine definierten Prozesse oder Richtlinien für den Umgang mit Lieferkettenrisiken. Drittanbieter werden primär aus operativer oder wirtschaftlicher Sicht betrachtet, Sicherheitsaspekte spielen eine untergeordnete Rolle. Transparenz über Lieferketten, insbesondere über Tier-n-Strukturen, ist nicht vorhanden. Nachweise über Sicherheitsmaßnahmen können nicht oder nur eingeschränkt erbracht werden. Audits erfolgen unstrukturiert oder gar nicht.

Level 2 – Wiederholbar (basic)

Erste strukturierte Ansätze sind erkennbar. Einzelne Prozesse, etwa zur Lieferantenbewertung oder Due Diligence, wurden eingeführt, werden

jedoch nicht konsistent angewendet. Sicherheitsanforderungen werden teilweise in Verträgen berücksichtigt, sind jedoch weder standardisiert noch vollständig. Die Transparenz über kritische Lieferanten ist begrenzt, insbesondere in mehrstufigen Lieferketten. Erste Auditaktivitäten finden statt, jedoch ohne klar definierte Methodik oder systematische Nachweisführung. Dokumentation ist vorhanden, aber nicht durchgängig vollständig oder aktuell.

Level 3 – Definiert (standardisiert)

Supply-Chain-Security ist organisatorisch verankert und durch definierte Prozesse, Richtlinien und Rollenstrukturen abgesichert. Drittparteien-Risikomanagement ist etabliert und umfasst strukturierte Klassifikation, Bewertung und Überwachung von Lieferanten. Sicherheitsanforderungen sind standardisiert und werden systematisch in Ausschreibungen und Verträge integriert. Audits folgen definierten Methoden und liefern nachvollziehbare Ergebnisse. Die Dokumentation ist konsistent, und relevante Evidenz wird strukturiert erfasst. Erste regulatorische Anforderungen (z. B. NIS-2, DORA) werden gezielt adressiert.

Level 4 – Gesteuert (gemessen)

Sicherheitsmaßnahmen werden aktiv gesteuert und kontinuierlich überwacht. KPIs und KRIs ermöglichen eine messbare Bewertung von Risiken und Kontrollwirksamkeit. Risiken entlang der Lieferkette sind weitgehend

transparent, einschließlich kritischer Abhängigkeiten und Konzentrationsrisiken. Audits erfolgen risikobasiert und sind eng mit Governance- und Reportingstrukturen verzahnt. Drittanbieter sind aktiv in Sicherheitsprozesse eingebunden, etwa in Incident Response oder Business Continuity. Die Nachweisfähigkeit ist hoch, und regulatorische Anforderungen werden systematisch erfüllt und dokumentiert.

Level 5 – Optimiert (kontinuierlich verbessert)

Supply-Chain-Security ist vollständig in die Unternehmenssteuerung integriert und wird kontinuierlich weiterentwickelt. Prozesse sind weitgehend automatisiert, insbesondere im Bereich Monitoring, SBOM-Analyse und Drittparteienbewertung. Datenbasierte Steuerung und Continuous Compliance ermöglichen eine nahezu Echtzeitbewertung der Sicherheitslage. Zero-Trust-Prinzipien und modellbasierte Kontrollen (z. B. BAM) sind implementiert. Risiken werden proaktiv erkannt und adressiert. Audits sind integraler Bestandteil der operativen Steuerung und liefern kontinuierlich verwertbare Erkenntnisse. Die Organisation ist in der Lage, regulatorische Anforderungen effizient, skalierbar und prüfungssicher zu erfüllen.

Das Modell kann sowohl für Selbstbewertungen als auch im Rahmen interner und externer Audits eingesetzt werden. Es dient als Grundlage für die Ableitung konkreter Maßnahmen und unterstützt Organisationen dabei, ihren Reifegrad systematisch und nachvollziehbar zu erhöhen.

Weitere Downloads

Im Rahmen von Brain-Media KaaS stellen wir unseren Kunden weitere Downloads bereit, beispielsweise folgende:

- Erweiterte Audit-Checklisten (Excel / Tool-Format)
- Reifegrad-Selbsteinschätzung (Self-Assessment-Tool)
- SBOM-Audit-Leitfaden
- KPI/KRI-Dashboard-Vorlage

Mehr zum Thema

Der vollständige Leitfaden „Supply Chain Security Audit“

🛒 Jetzt bei Amazon bestellen