Sichere Lieferketten für die Verteidigungs- und Rüstungsindustrie

Produktblatt CADIS

Mit steigender technischer Komplexität, internationalen Abhängigkeiten und wachsenden Cyberrisiken stehen Unternehmen der Verteidigungs- und Rüstungsindustrie vor neuen Anforderungen: Lieferketten müssen nicht nur effizient, sondern auch nachweislich sicher, resilient und vertrauenswürdig sein.

CADIS ist das erste europäische Prüfverfahren, das speziell auf Zulieferer dieser Branche zugeschnitten ist. Es schafft eine einheitliche, objektive und messbare Grundlage, um Cyber- und Informationssicherheit entlang der gesamten Lieferkette zu bewerten – modular, nachvollziehbar und risikoorientiert.

Ihre Vorteile mit CADIS

- **Stärker im Wettbewerb –** Nachweisbar geprüfte Sicherheit erhöht das Vertrauen von Auftraggebern und stärkt Ihre Position in Ausschreibungen.
- **Erleichterter Marktzugang –** Erhöht die Chance, in sicherheitskritischen Beschaffungsprozessen berücksichtigt zu werden.
- **Planungssicherheit –** Klare Anforderungen ermöglichen eine strukturierte Vorbereitung und reduzieren Unsicherheiten.
- **Effizienz durch Modularität –** Nur relevante Module werden geprüft; Aufwand und Kosten bleiben beherrschbar.
- **Ganzheitliche Sicherheit –** IT, OT, physische Sicherheit und organisatorische Prozesse werden integriert betrachtet.
- **Lieferkettenrisiken minimieren –** Frühzeitige Erkennung von Schwachstellen verhindert spätere Störungen.
- **Glaubwürdigkeit stärken –** Unternehmen positionieren sich als verantwortungsbewusster Partner mit hoher Sicherheitskultur.

Warum CADIS?

Cybersicherheit und Widerstandsfähigkeit werden zur Grundvoraussetzung. Organisationen in der Verteidigungsindustrie tragen besondere Verantwortung: Geheimschutz, kritische Informationen und komplexe Technologien müssen gegenüber externen und internen Risiken geschützt werden – und zwar über die gesamte Lieferkette hinweg.

CADIS wurde genau hierfür entwickelt:
Es bietet einen klar strukturierten, standardisierten Prüfrahmen, der speziell an die Sicherheitsanforderungen in diesem sensiblen Sektor angepasst ist.

Der modulare Aufbau umfasst 14 Prüfmodule, die abhängig von Rolle, Sensibilität und Risikoprofil flexibel kombiniert werden können. Unternehmen müssen nur das erfüllen, was für ihre Position in der Lieferkette wirklich relevant ist.

Die Bewertung der Lieferanten erfolgt durch den Systemhersteller. Zur Unterstützung dieses Prozesses stellt DEKRA das Tool „Supplier-Criticality-Evaluation“ bereit – ein standardisiertes Bewertungsschema, das eine einheitliche und nachvollziehbare Festlegung des individuellen Prüfscopes je Lieferant sicherstellt.

Die Anforderungen sind klar formuliert, aber bieten gleichzeitig technische Umsetzungsspielräume – ideal für Unternehmen mit unterschiedlichem Reifegrad.

Der Prüfprozess – Schritt für Schritt

1. Kick-Off
Zu Beginn des Prüfprozesses findet ein gemeinsames Kick-Off-Meeting statt. Dabei werden alle relevanten Rahmenbedingungen besprochen, Erwartungen geklärt und der Ablauf der Prüfung gemeinsam abgestimmt. Gleichzeitig werden die erforderlichen Unterlagen und Ansprechpartner festgelegt.

2. Phase 1 – Remote-Vorprüfung
In der ersten Phase erfolgt eine formale und inhaltliche Vorabprüfung auf Basis bereitgestellter Unterlagen. Ziel ist es, ein erstes Bild des Lieferanten zu gewinnen, mögliche Risikobereiche zu identifizieren und die Hauptprüfung gezielt vorzubereiten.

3. Phase 2 – Hauptprüfung
Die Durchführung der Hauptprüfung orientiert sich am Level of Examination (LoE):
- LoE 1: Plausibilitätsprüfung der Gesamtumsetzung je Prüfpunkt (nicht anforderungsbezogen im Detail). Keine Prüfung der Nachweisdokumentation.
- LoE 2: Strukturiertes Remote-Interview mit risikobasierter Auswahl von Prüfpunkten. Vertiefende Verifizierung über Plausibilität hinaus.
- LoE 3: Vor-Ort-Audit mit Interviews, Einsichtnahmen, Stichproben und Standortbegehung. Evidenzbasierte Verifizierung.

4. Abschlussgespräch
Im Anschluss an die Hauptprüfung werden die Ergebnisse in einem Abschlussgespräch mit dem Kunden besprochen. Dazu zählt auch die Abstimmung von Maßnahmenplan, Follow-Up (sofern notwendig) und den Termin für risikobasierte Überwachungsprüfung im Folgejahr.

5. Maßnahmenplan
Auf Basis der identifizierten Abweichungen erarbeitet der Kunde einen verbindlichen Maßnahmenplan. Dieser definiert konkrete Korrekturmaßnahmen, Verantwortlichkeiten sowie realistische Umsetzungsfristen.

6. Follow-Up
Im Rahmen des Follow-Ups wird die Umsetzung der vereinbarten Maßnahmen überprüft und dokumentiert. So wird sichergestellt, dass identifizierte Schwachstellen nachhaltig behoben wurden.

7. Risikobasierte Überwachungsprüfung
Bestandteil des zweijährigen Prüfzyklus und wird im Jahr nach der Erstprüfung durchgeführt. Die Planung orientiert sich am Ergebnis der Vorprüfung sowie an einem risikobasierten Ansatz, der die Kritikalität und das Risikoprofil des Unternehmens, offene Feststellungen und Abweichungen aus der Vorprüfung sowie relevante Änderungen – etwa organisatorischer oder standortbezogener Art sowie etwaige Sicherheitsvorfälle – berücksichtigt.

8. Neuer Prüfzyklus
Nach Abschluss aller Schritte beginnt der Prüfprozess erneut – angepasst an aktuelle Gegebenheiten und das weiterentwickelte Risikoprofil des Lieferanten. So wird eine lückenlose und dynamische Lieferantenüberwachung gewährleistet.

Die 14 Module von CADIS

1. Physische Sicherheit am Standort
2. Organisation der Informationssicherheit
3. IT-Security
4. OT-Security
5. Einsatz cloudbasierter und externer Serviceleistungen
6. Kontinuitätsmanagement
7. Incident- und Krisenmanagement
8. Identität- und Zugriffsmanagement
9. Sicherheit in der Softwareentwicklung
10. Informationssicherheit im Projektmanagement / Personalwesen / Einkauf
11. Datenschutz
12. Compliance Management System
13. Einsatz künstlicher Intelligenz
14. Transport und Umschlag

Warum DEKRA?

- Exklusives Prüfverfahren – CADIS wurde von DEKRA entwickelt und wird ausschließlich durch DEKRA durchgeführt.
- Tiefe Branchenexpertise – jahrzehntelange Erfahrung in Cybersecurity, Industrieprüfungen und sicherheitskritischen Sektoren.
- Unabhängigkeit & Glaubwürdigkeit – neutral, international anerkannt, mit hoher Reputation in der Sicherheitsbewertung von Lieferketten.

Als Teil des DEKRA Leistungsportfolios ergänzt CADIS unsere Zertifizierungsleistungen um ein strukturiertes Prüfverfahren zur einheitlichen Bewertung der Cyber- und Informationssicherheit in der Verteidigungs- und Rüstungslieferkette..

Darüber hinaus bietet Ihnen die DEKRA Gruppe folgende Dienstleistungen:

- Bewertungen zur Einhaltung eigener Regeln
- Personen-Zertifizierungen
- Produktprüfungen und -zertifizierungen

Sie möchten mehr über CADIS erfahren? Dann informieren Sie sich jetzt!

Kontaktieren Sie uns!

Mehr erfahren!

Wünschen Sie weitere Informationen?
Besuchen Sie unsere Website:

dekra-certification.de