SICK Cybersecurity-Anforderungen an Lieferanten

Vorwort

Es ist ein wesentliches Ziel von SICK, seinen Kunden hochwertige Produkte und Dienstleistungen anzubieten. Um dieses Ziel zu erreichen, müssen bestimmte Prozesse für ein kontinuierliches Risikomanagement bezüglich Cybersecurity von SICK-Produkten umgesetzt werden. Darüber hinaus verpflichten gesetzliche Vorgaben (u.a. der EU Cyber Resilience Act) SICK gemeinsam mit seinen Lieferanten, eine angemessene Cybersicherheit über den gesamten Lebenszyklus der Produkte sicherzustellen.

Dieses Dokument legt Anforderungen an die Cybersecurity fest, die von Lieferanten für alle Produkte mit digitalen Elementen (PDE) erfüllt werden müssen, die in oder als Teil einer SICK-Lösung eingesetzt werden. Darüber hinaus werden für einige Anforderungen bevorzugte Implementierungen angegeben.

Folgende Anforderungen müssen vom Lieferanten abgedeckt werden (siehe Kapitel 4):

- Eigenverantwortung für Cybersecurity
- Prozess der Sicherheitsentwicklung
- Lieferantenmanagement für Cybersecurity
- Transparenz und Reaktion auf Cybersecurity
- Cybersecurity-Ausbildung
- Produktionssicherheit

Die “SICK Cybersecurity-Lieferantenanforderungen für Produkte” enthalten Anforderungen für folgende Lieferanten:

- Komponentenhersteller
- Private-Label-Hersteller
- Produktionsdienstleister

Die jeweiligen Anforderungen enthalten Hinweise darauf, für welche Lieferantenart die Anforderung anwendbar sind. Bei der Angabe „Alle Lieferanten“ ist die Anforderung für Komponentenhersteller, Private-Label-Hersteller und Produktionsdienstleister gültig.

Definitionen

Produkte mit digitalen Elementen

Produkte mit digitalen Elementen (PDE) sind so definiert, wie sie im EU-Cyber-Resilienz-Gesetz beschrieben[1] sind.

Recht auf Auditierung

SICK behält sich das Recht vor, jederzeit (höchstens einmal alle zwölf Monate) weitere Unterlagen und Nachweise anzufordern sowie ein Compliance-Audit durchzuführen oder anzuordnen, um festzustellen, ob die aufgeführten Anforderungen erfüllt sind. Jede Partei trägt die im Rahmen der Prüfung entstehenden Kosten jeweils selbst. Der Lieferant ist nicht verpflichtet, Kosten der prüfenden Partei oder von dieser beauftragter Dritter zu übernehmen. Ergeben sich aus der Lieferantendokumentation oder den Auditergebnissen Lücken in der Erfüllung der SICK-Anforderungen, so hat der Lieferant auf eigene Kosten alle Maßnahmen zu ergreifen und allen zumutbaren Weisungen von SICK Folge zu leisten, um identifizierte Lücken unverzüglich zu schließen.

Anforderungen

Verantwortung für Cybersecurity (Ownership for Cybersecurity)

OFC-01

- Gültig für: Alle Lieferanten
- **Anforderung**: Der Lieferant muss Cybersecurity entsprechend organisatorischen, rechtlichen und marktwirtschaftlichen Anforderungen systematisch umsetzen. Die Geschäftsführung des Lieferanten bestätigt Cybersecurity als eine der wichtigen qualitativen Eigenschaften der Liefergegenstände.

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:52022PC0454

- **Bevorzugte Lösung**: Der Lieferant etabliert ein Cybersecurity Management System (CSMS) basierend auf der IEC 62443.

Cybersecurity im Entwicklungsprozess (Security Development Process)

SDP-01

- Gültig für: Alle Lieferanten
- **Anforderung**: Der Lieferant muss den Liefergegenstand mittels eines etablierten Cybersecurity Entwicklungsprozess, im Einklang mit "State of the Art" der Branche, entwickeln.
- **Bevorzugte Lösung**: Der Cybersecurity Entwicklungsprozess des Lieferanten ist zertifiziert (z.B. nach IEC 62443-4-1)

SDP-02

- Gültig für: Alle Lieferanten
- **Anforderung**: Der Cybersecurity Entwicklungsprozess des Lieferanten muss einen risikobasierten Ansatz für Cybersicherheitsmaßnahmen beinhalten. Identifizierte Restrisiken und alle relevanten Annahmen sind zu dokumentieren und dem Liefergegenstand beizulegen.
- **Bevorzugte Lösung**: Die implementierte Risikoanalyse ist in der gesamten Entwicklungsorganisation des Lieferanten standardisiert. Identifizierte verbleibende Risiken müssen im Rahmen des Angebots dokumentiert werden.

SDP-03

- Gültig für: Komponentenlieferanten
- **Anforderung**: Der Lieferant muss für den Liefergegenstand eine SBOM mit den direkten Abhängigkeiten dokumentieren. Für den Fall, dass SICK wiederum verpflichtet ist die SBOM für ein SICK PDE, die den Liefergegenstand integrieren, an zuständige Behörden weiterzugeben, muss der Lieferant die SBOM für den Liefergegenstand zur Verfügung stellen.

- **Bevorzugte Lösung**: Die SBOM ist im “CycloneDX”-Format oder alternativ in einem anderen weithin verbreiteten maschinenlesbaren Format (z.B. SPDX) erhältlich. Die SBOM enthält Unterkomponenten (transitive Abhängigkeiten). Die Einträge in der SBOM für kommerzielle Softwarekomponenten enthalten eine Kontaktmöglichkeit für die Komponente. Die SBOM ist Teil der Auslieferung oder wird über einen Endpunkt bereitgestellt, von dem SICK die SBOM herunterladen kann.

SDP-04

- Gültig für: Private-Label-Lieferanten
- **Anforderung**: Der Lieferant hat für den Liefergegenstand eine SBOM zu liefern, die die direkten Abhängigkeiten enthält.
- **Bevorzugte Lösung**: Die SBOM ist im “CycloneDX”-Format[2] oder alternativ in einem anderen weithin verbreiteten maschinenlesbaren Format (z.B. SPDX) erhältlich. Die Stückliste enthält Unterkomponenten (transitive Abhängigkeiten). Die Einträge in der Stückliste für kommerzielle Softwarekomponenten enthalten eine Kontaktmöglichkeit für die Komponente. Die SBOM ist Teil der Auslieferung oder wird über einen Endpunkt bereitgestellt, von dem SICK die SBOM herunterladen kann.

SDP-05

- Gültig für: Private-Label-Lieferanten, Komponentenlieferanten
- **Anforderung**: Der Lieferant muss den Liefergegenstand ohne bekannte ausnutzbare Schwachstellen liefern. Der Lieferant muss mit geeigneten Mitteln nach ausnutzbaren Schwachstellen suchen.
- **Bevorzugte Lösung**: Der Lieferant setzt Methoden wie statische Codeanalysen, Sicherheitstests und kontinuierliche Prüfungen auf öffentlich bekannte Schwachstellen bei der Entwicklung des Liefergegenstandes ein.

[2] https://cyclonedx.org/docs/1.6/json/

Lieferantenmanagement für Cybersecurity (Supplier Management for Cybersecurity)

SMC-01

- Gültig für: Private-Label-Lieferanten, Komponentenlieferanten
- **Anforderung**: Der Lieferant verlangt und stellt sicher, dass seine Lieferanten die Cybersicherheit auf der Grundlage etablierter Industriestandards berücksichtigen.

Transparenz und Reaktion auf Cybersecurity (Transparency and Reaction Requirements)

TRR-01

- Gültig für: Alle Lieferanten
- **Anforderung**: Der Lieferant muss eine dedizierte, SICK zugängliche Kontaktmöglichkeit für die Meldung von Schwachstellen einrichten.
- **Bevorzugte Lösung**: Der Kontakt wird in der security.txt gemäß RFC 9116 angegeben[3].

TRR-02

- Gültig für: Alle Lieferanten
- **Anforderung**: Der Lieferant muss SICK unverzüglich über Cybersecurity-Vorfälle innerhalb seiner Organisation informieren, die die Sicherheit der gelieferten PDEs beeinträchtigen können, und auf Verlangen von SICK eng mit SICK zusammenarbeiten, um Schwachstellen zu beheben.
- **Bevorzugte Lösung**: Der Lieferant benachrichtigt SICK innerhalb von 24 Stunden per E-Mail an psirt@sick.de (unter der Nutzung von PGP-Verschlüsselung), nach Entdeckung der Schwachstellen.

[3] https://www.rfc-editor.org/rfc/rfc9116.txt

TRR-03

- Gültig für: Private Label Lieferanten, Komponentenlieferanten
- **Anforderung**: Der Lieferant muss einen Incident-Response-Prozess einrichten, geeignete Ressourcen bereitstellen und die Wirksamkeit des Prozesses gewährleisten. Der Incident-Response-Prozess muss ein für SICK zugängliches Verfahren zur Meldung von Schwachstellen bereitstellen. Der Lieferant muss angemessen und unverzüglich auf Schwachstellen und Cybersecurity-Vorfälle im Zusammenhang mit allen gelieferten PDEs reagieren.
- **Bevorzugte Lösung**: Es wurde ein Prozess zur koordinierten Offenlegung von Schwachstellen etabliert. Der Lieferant unterstützt die Benachrichtigung über Schwachstellen über das maschinenlesbare CSAF-Format[4]. Für vertrauliche Informationen ist eine Benachrichtigung von SICK per E-Mail an psirt@sick.de mit PGP-Verschlüsselung bevorzugt.

TRR-04

- Gültig für: Private-Label-Lieferanten, Komponentenlieferanten
- **Anforderung**: Wenn ausnutzbare Sicherheitslücken in dem Liefergegenstand dem Lieferanten bekannt werden, muss der Lieferant unverzüglich, in der Regel innerhalb von 30 Tagen, Sicherheitsupdates für den Liefergegenstand bereitstellen.
- **Bevorzugte Lösung**: Die Benachrichtigung über das Update wird über das maschinenlesbare CSAF-Format kommuniziert. Bei vertraulichen Informationen ist es vorzuziehen, SICK per E-Mail an psirt@sick.de mit PGP-Verschlüsselung zu informieren.

Cybersecurity-Ausbildung (Cybersecurity Education)

CED-01

- Gültig für: Private-Label-Lieferanten, Komponentenlieferanten

[4] https://www.csaf.io/specification/

- **Anforderung**: Der Lieferant muss ein Cybersecurity Schulungsprogramm zur Verfügung stellen, das dem zur Produktentwicklung beitragenden Personal zur Verfügung steht und von diesem nachweisbar genutzt wird.

Lieferketten- und Produktionssicherheit (Supplychain and Production Security)

PRD-01

- Gültig für: Alle Lieferanten
- **Anforderung**: Der Lieferant muss die Produktionsbereiche des Liefergegenstandes vor dem physischen Zugriff durch Personen (z.B. Dritte oder Mitarbeiter), die nicht vom Lieferanten autorisiert sind, angemessen schützen.
- **Bevorzugte Lösung**: Der physische Schutz wurde durch physische Penetrationstests getestet.

PRD-02

- Gültig für: Alle Lieferanten
- **Anforderung**: Der Lieferant muss die Produktionsbereiche des Liefergegenstandes vor dem digitalen Zugriff (z.B. Netzwerkzugriff) durch Personen (z.B. Dritte oder Mitarbeiter), die nicht vom Lieferanten autorisiert sind, schützen.
- **Bevorzugte Lösung**: Es existieren Lösungen zur Netzwerkseparierung. Die Netzwerke werden überwacht. Der digitale Schutz wurde durch Penetrationstests getestet. Die relevanten Prozesse, IT-Assets und Netzwerke in der Produktion sind nach ISO 27001, IEC 62443 oder anderen etablierten IT-Sicherheitsstandards zertifiziert.

PRD-03

- Gültig für: Alle Lieferanten
- **Anforderung**: Der Lieferant muss die Herstellung, Lagerung und Auslieferung des Liefergegenstandes angemessen vor Cyberbedrohungen schützen.

- **Bevorzugte Lösung**: Die relevanten Prozesse, IT-Assets und Netzwerke in der Produktion sind nach ISO 27001, IEC 62443 oder anderen etablierten IT-Sicherheitsstandards zertifiziert.

PRD-04

- Gültig für: Alle Lieferanten
- **Anforderung**: Werden digitale Daten zwischen dem Lieferanten und SICK zum Zwecke der Entwicklung, Produktion, Herstellung oder Lieferung des Liefergegenstandes ausgetauscht, muss der Sender dies über einen sicheren Übertragungsweg vornehmen.
- **Bevorzugte Lösung**: Von SICK zur Verfügung gestellte Möglichkeiten (z.B., https://ftp.sick.com) werden zum Datenaustausch genutzt.

Unterzeichnet in Bestätigung der Anforderungen

Ort, Datum

Unterschrift

Name

Funktion

Unternehmen