SICK CYBERSICHERHEIT - ANFORDERUNGEN AN LIEFERANTEN

Einleitung

Es ist ein wichtiges Ziel von SICK, seinen Kunden qualitativ hochwertige Produkte und Dienstleistungen anzubieten. Um dies zu erreichen, müssen bestimmte Verfahren für ein kontinuierliches Risikomanagement bezogen auf u.a. die Cybersicherheit der SICK-Produkte implementiert werden. Hierzu muss ein akzeptables Sicherheitsniveau erreicht werden, indem Bedrohungen abgemildert und Best Practices der Branche angewendet werden.

Dieses Dokument enthält Mindestanforderungen an die Cybersicherheit, die für jedes an SICK gelieferte softwarebezogene Produkt (im Folgenden „*Produkt*“) zu erfüllen sind.
Ein Liefergegenstand ist softwarebezogen wenn es irgendeine Art von Software verwendet, teilweise auf Software basiert oder an sich eine Software ist und welches SICK zur Verwendung in eigenen Produkten oder zum Vertrieb an Kunden vorsieht.

Dieses Dokument enthält Anforderungen, die vom Lieferanten einzuhalten sind, in Bezug auf:

- Allgemeine Verantwortlichkeiten
- Organisatorische Verantwortung des Lieferanten
- Produktsicherheit
- Verwundbarkeitsmanagement, Kommunikation, Benachrichtigung und sofortige Maßnahmen bei Sicherheitslücken
- Bewertung des Reifegrads

Allgemeine Verantwortlichkeiten

Der Lieferant und SICK verstehen Cybersicherheit als gemeinsame Verantwortung zum Schutz der Kunden von SICK. Innerhalb dieser Verantwortung ist der Lieferant dafür verantwortlich, die Anforderungen aus diesem Dokument einzuhalten. Darüber hinaus liefert der Lieferant sichere und konforme *Produkte* an SICK, die branchenüblich anerkannten Standards im Bereich Cybersicherheit, regulatorischen Standards im Lieferland sowie den SICK-Sicherheitsanforderungen entsprechen.

Der Lieferant muss für seine *Produkte* eine dem Stand der Technik entsprechende Sicherheit gegen Manipulation, Malware, Abhören, Spionage, Netzwerkangriffe, unbefugten Zugriff auf Endbenutzerdaten oder sonstige böswillige Aktivitäten durch nicht autorisierte Dritten bieten.
Der Lieferant wird insbesondere Sicherheitsgrundsätze und -standards gemäß der Normenreihe der IEC 62443 implementieren und während der Lebensdauer der *Produkte* aufrechterhalten.

Organisatorische Verantwortung des Lieferanten

Der Lieferant ist für die Cybersicherheit seiner *Produkte* verantwortlich. Er ergreift technische und organisatorische Maßnahmen um diese zu gewährleisten. Hierzu zählt die sorgfältige Auswahl, Anleitung und Schulung aller im Geschäftsbetrieb des Lieferanten tätigen (internen und externen) Mitarbeiter im Hinblick auf die Cybersicherheit der *Produkte*.

Produktsicherheit

Der Lieferant muss sichere *Produkte* entwickeln und liefern, um die Auswirkungen potenzieller Sicherheitsrisiken zu minimieren.
Dies beinhaltet, ist aber nicht beschränkt auf

- die Verantwortung, sicherzustellen, dass die *Produkte* keine Schwachstellen oder Verwundbarkeiten aufweisen

- das Ergreifen aller angemessenen Maßnahmen, um sicherzustellen, dass sich in den *Produkten* keine Hintertüren oder anderen Mechanismen befinden, die zu einer Umgehung der Sicherheitsmechanismen, zu unbefugten Zugriff oder Steuerung führen können

Verwundbarkeitsmanagement, Kommunikation, Benachrichtigung und sofortige Maßnahmen bei Sicherheitsvorfällen

Der Lieferant muss einen Prozess entwickeln, dokumentieren und implementieren, um auf Schwachstellen und Sicherheitsprobleme im Zusammenhang mit seinen *Produkten* unverzüglich und in angemessener Weise zu reagieren (sog. Verwundbarkeitsmanagement). Dieser Prozess folgt allgemein anerkannten Industriestandards und –praktiken (einschließlich der Normenreihe IEC 62443) und umfasst auch eine kontinuierliche Überwachung der Sicherheitsempfehlungen und -bewertungen hinsichtlich der *Produkte*. Wo gefordert, sind Sofortmaßnahmen zu ergreifen.

Der Lieferant muss folgende Ansprechpartner benennen:

1. Sofortkontakt für künftige, die Cybersicherheit betreffende Themen:

   _____

2. Key Account Manager, für Eskalationen oder Verstöße gegen die in diesem Dokument vereinbarten Regelungen:

   _____

Der Lieferant wird die Angabe der Ansprechpartner und deren Kontaktdaten stets aktuell halten.

Jegliche Kommunikation im Zusammenhang mit dem Verwundbarkeitsmanagement wird über E-Mail-Korrespondenz so initiiert, dass Vertraulichkeit und Integrität gewahrt bleiben. Hierfür ist die E-Mail-Adresse psirt@sick.de zu verwenden.

Der Lieferant muss SICK unverzüglich über Cyber-Sicherheitsvorfälle in seiner Organisation informieren, die Auswirkungen auf die Sicherheit der *Produkte* haben können, und auf Verlangen von SICK umfassend mit SICK zusammenarbeiten, um Schwachstellen der *Produkte* zu verfolgen.
Der Lieferant liefert unverzüglich eine Lösung, wenn ein Cyber-Sicherheitsvorfall in einem *Produkt* festgestellt wird.

Reifegradbewertung

SICK behält sich vor, *Produkte* von Lieferanten umfassend auf ihre Anfälligkeit hin zu überprüfen. Für den Fall, dass die Ergebnisse Cyber-Sicherheitsrisiken aufzeigen, benachrichtigt SICK den Lieferanten und fordert Maßnahmen ein. Der Lieferant wird die Maßnahmen umsetzen, soweit ihm dies unter besonderer Berücksichtigung der Interessen von SICK zumutbar ist. Test und Prüfung durch SICK entbinden den Lieferanten nicht von der Verantwortung, selbst sichere *Produkte* zu entwickeln und zu liefern.

SICK behält sich das Recht vor, weitere Unterlagen und Nachweise anzufordern sowie jederzeit ein Compliance-Audit durchzuführen oder durch Dritte durchführen zu lassen, um festzustellen, ob die Anforderungen aus diesem Dokument erfüllt sind. Jede Partei trägt die ihr entstehenden Kosten des Audits.
Falls die Lieferantendokumentation oder die Auditergebnisse Abweichungen bei der Erfüllung der SICK-Anforderungen aufdecken, wird der Lieferant auf eigene Kosten alle Anstrengungen unternehmen und allen zumutbaren Anweisungen von SICK folgen, um die Abweichungen unverzüglich zu beheben.

Einverstanden:

_____
Ort Datum

_____
Unterschrift

_____
Name

_____
Funktion

_____
Unternehmen

SICK CYBER SECURITY - REQUIREMENTS FOR SUPPLIERS

Introduction

It is a vital goal of SICK to offer high quality products and services to its customers. In order to achieve this goal, certain procedures have to be implemented for continual risk management relating, for example, to the cyber security of SICK products. An acceptable security level must be achieved by mitigating threats and following industry best practices.

This document states the minimum cyber security requirements that must be met for every software-related product that is supplied to SICK (hereinafter referred to as "*Product*").
A supplied item is a software-related *Product* if it uses any type of software, is partly software-based or is in itself a type of software and which SICK provides for use in its own products or for distribution to customers.

This document specifies the requirements that the supplier must meet with regard to:

- General responsibilities
- Organizational responsibility of the supplier
- Product security
- Vulnerability management, communication, notification and immediate actions on security related incidents
- Assessment of maturity

General responsibilities

The supplier and SICK view cyber security as their common responsibility to protect the customers of SICK. Within this responsibility, the supplier is responsible for complying with the specifications in this document. Furthermore, the supplier shall deliver to SICK secure and legally compliant *Products* reflecting the industry standards within the cyber security field, other regulatory standards in the country of delivery as well as SICK security requirements.
The supplier shall provide for its *Products* state-of-the art security against tampering, malware, eavesdropping, spying, network attacks, unauthorized access to end user data or any other malicious activity by an unauthorized third party.
The supplier shall in particular implement, and comply with, the security principles and standards of the IEC 62443 series of standards throughout the *Product* lifecycle.

Organizational responsibility of the supplier

The supplier is responsible for the cyber security of its *Products*. The supplier shall implement technical and organizational safeguards to ensure such cyber security. This includes the careful selection, instruction and training with regard to the cyber security of the *Products* of all (internal and external) employees involved in the supplier's business operations.

Product security

The supplier shall develop and deliver secure *Products* to minimize impacts associated with potential security issues.
This includes but is not limited to

- responsibility for ensuring that the *Products* do not contain any weaknesses or vulnerabilities; and
- taking all reasonable steps to ensure that the *Products* are free from of any backdoors or other mechanisms which could result in a circumvention of security mechanisms or unauthorized access or control.

Vulnerability management, communication, notification and immediate action in the event of security related incidents

The supplier shall develop, document, and implement a process to respond adequately and without undue delay to vulnerabilities and security issues associated with its *Products* (so-called vulnerability management). This process shall conform to commonly accepted industry standards and practices (including the IEC 62443 standard series) and include but not be limited to the continuous monitoring of security advisory sources and assessments with regard to the *Products*. Where indicated, the supplier shall take immediate action.

The supplier shall provide the following contacts:

1. Immediate contact for cyber security-related matters to be discussed in the future:

   _____

2. Key account manager to handle escalations or breaches of conditions agreed upon in this document:

   _____

The supplier shall keep the contacts up-to-date at all times.

All communication related to vulnerability management shall be initiated via email correspondence in such a manner that confidentiality and integrity are maintained. Please use the e-mail address psirt@sick.de for this purpose.

The supplier shall notify SICK without undue delay about any cyber security incidents within its organization that may affect the security of the *Products* and, upon the request of SICK, cooperate closely with SICK to address the *Products'* vulnerabilities.

The supplier shall promptly deliver a solution if a cyber security incident is identified in a *Product*.

Assessment of maturity

SICK reserves the right to thoroughly test and inspect the supplier's *Products* regarding their vulnerability. In the event that the test and inspection results reveal security risks, SICK will notify the supplier and request remedial action. The supplier shall take remedial action to the extent that this is possible in particular consideration of the interests of SICK. Test and inspection by SICK will not release the supplier from its responsibility to develop and deliver secure *Products*.

SICK reserves the right to request further documentation and evidence as well as to perform or order a compliance audit at any time in order to determine whether the listed requirements have been met.
Each Party shall bear the costs it incurs in connection with the audit.
If the supplier documentation or audit results reveal gaps in the fulfilment of the SICK requirements, the supplier shall, at its own expense, take all steps and follow all reasonable instructions of SICK to close such security gaps without undue delay.

Signed in acceptance of the above

_____
Place, Date

_____
Signature

_____
Name

_____
Function

_____
Company