SICK CYBERSICHERHEIT - Anforderungen für Lieferanten

Einleitung

Es ist ein wichtiges Ziel von SICK, seinen Kunden qualitativ hochwertige *Produkte* und Dienstleistungen (im Folgenden „*Produkte*“) anzubieten. Um dies zu erreichen, müssen bestimmte Verfahren für ein kontinuierliches Risikomanagement im Umfeld von Cybersicherheits-*Produkten* implementiert werden. Hierzu muss ein akzeptables Sicherheitsniveau erreicht werden, indem Bedrohungen abgemildert werden und Best Practices der Branche angewendet werden.

Dieses Dokument enthält Mindestanforderungen an die Cybersicherheit, die für jedes an SICK gelieferte softwarebezogene *Produkt* zu erfüllen sind.
Ein softwarebezogenes Produkt ist ein *Produkt*, das jegliche Art von Software verwendet, teilweise auf Software basiert oder an sich eine Software ist.

Der Umfang dieses Dokuments umfasst die untenstehenden Ziele, die vom Lieferanten mit Bezug auf Ressourcen, Prozesse und Informationen zu erfüllen und aufrecht zu erhalten sind:

- Allgemeine Verantwortlichkeiten
- Verantwortung des Managements
- *Produkt*-Sicherheit
- Verwaltung, 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. 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* die bestmögliche Sicherheit gegen Manipulation, Malware, Abhören, Spionage, Netzwerkangriffe, unbefugten Zugriff auf Endbenutzerdaten oder sonstige böswillige Aktivitäten durch nicht autorisierte Dritten bieten.

Verantwortung des Managements

Die Verantwortung für die Sicherheit der an SICK gelieferten *Produkte* liegt beim obersten Management des Lieferanten. Diese beinhaltet die Definition von Zielen und die Zuweisung von Ressourcen für deren Erreichung. Aufgaben, die zur Erfüllung erforderlich sind, können an qualifizierte Mitarbeitern übertragen werden.
Das Management stellt sicher, dass alle Mitarbeiter in der Organisation über Cybersicherheit angemessen informiert und geschult werden. Das Management stellt sicher, dass Schulungen und Informationen effektiv sind.

Produktsicherheit

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

- Die Sicherstellung, 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, der auf Schwachstellen und Sicherheitsprobleme im Zusammenhang mit seinen *Produkten* reagiert. Dieser Prozess folgt allgemein anerkannten Industriestandards und Praktiken und umfasst auch eine kontinuierliche Überwachung der Sicherheitsempfehlungen und -bewertungen hinsichtlich der *Produkte* sowie der installierten Software auf *Produkten* für SICK. Wo gefordert, sind Sofortmaßnahmen zu ergreifen.
SICK fordert, dass beim Lieferanten ein Sofortkontakt für künftige sicherheitsrelevante Themen benannt wird. Darüber hinaus muss ein Key Account Manager benannt werden, um Eskalationen oder Verstöße gegen die in diesem Dokument vereinbarten Regelungen zu behandeln.

Sofortkontakt für sicherheitsrelevante Angelegenheiten: _____

Key Account für weitere Informationen: _____

Wo erforderlich muss der Lieferant die Kontakte ohne Aufforderung aktualisieren.

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 Sicherheitsvorfälle in seiner Organisation informieren, die Auswirkungen auf die Sicherheit der an SICK gelieferten *Produkte* haben können, und den Prozess einer koordinierten Offenlegung von Schwachstellen gemeinsam mit SICK verfolgen.
Der Lieferant liefert unverzüglich eine Lösung, wenn ein Sicherheitsvorfall in einem an SICK gelieferten *Produkt* festgestellt wird.

Reifegradbewertung

SICK behält sich vor, *Produkte* von Lieferanten umfassend auf ihre Anfälligkeit hin zu überprüfen. Für den Fall, dass die Ergebnisse Sicherheitsrisiken aufzeigen, benachrichtigt SICK den Lieferanten und fordert Maßnahmen ein. Test und Prüfung durch SICK entbinden den Lieferanten nicht von der Entwicklung und Lieferung sicherer *Produkte*.

SICK behält sich das Recht vor, weitere Unterlagen und Nachweise anzufordern sowie ein Compliance-Audit durchzuführen oder in Auftrag zu geben, um festzustellen, ob die Anforderungen aus diesem Dokument erfüllt sind. Im Falle eines Audits werden Umfang, Dauer und Organisation jeweils in guter Absicht vereinbart. Falls die Lieferantendokumentation oder die Auditergebnisse Abweichungen bei der Erfüllung der SICK-Anforderungen aufdecken, muss der Lieferant den zumutbaren Anweisungen von SICK folgen, um die Abweichungen unverzüglich zu beheben.

Unterzeichnet zur Annahme der obigen Ausführungen

_____
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 (in the following "*Products*") to its customers. To achieve this goal, certain procedures have to be implemented for continuous risk management associated with *Products* related to cyber security. Therefore, an acceptable security level must be achieved by mitigating threats and by following industry best practices.
This document states the minimum cyber security requirements, which shall be fulfilled for any software-related *Product* that is supplied to SICK.
A software-related product is a *Product*, which uses any type of software, is partly based on any type of software or is in itself a type of software.

The scope of this document includes the following objectives to be delivered and maintained by the supplier in the scope of resources, processes and information:

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

General responsibilities

The supplier and SICK understand cyber security as a common responsibility to protect customers. Within those, it is the supplier's responsibility to adhere to the conditions of this document. Furthermore, the supplier shall deliver secure and compliant *Products* to SICK reflecting the industry recognized standards within the cyber security field, other regulatory standards in the country of delivery as well as SICK security requirements.
The supplier shall include the best possible security of the *Products* against tampering, malware, eavesdropping, spying, network attacks, unauthorized access to end user data or any other malicious activity by an unauthorized 3rd party.

Management responsibility

The responsibility for security of *Products* delivered to SICK is assigned to the supplier's top management. This includes definition of objectives and the assignment of resources to enable their fulfilment. Tasks required for fulfilment may be assigned to qualified employees.
Management assures that all employees in the organization are informed and trained adequately on information security. Management assures that training and information are effective.

Product security

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

- ensuring that the *Products* do not contain any weaknesses or vulnerabilities
- taking any reasonable steps to ensure the *Products* are clear 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 actions on security related incidents

The supplier shall establish, document, and implement a process to react to vulnerabilities and security issues associated with his *Products*. This process shall follow commonly accepted industry standards and practices and includes but shall not be limited to continuous monitoring of security advisory sources and assessments with respect to the *Products* and the software installed on the *Products* delivered to SICK. Where indicated, immediate action shall be taken.

SICK requires an instant contact to be nominated at the supplier for security related matters to be discussed in the future. A key-account manager must additionally be appointed to handle escalations or breaches of conditions agreed upon in this document.

Immediate contact for security related matters: _____

Key account t.b. informed additionally: _____

If so, the supplier shall update the contacts without request.

Any communication related to vulnerability management shall be initiated via email correspondence in such a matter that confidentiality and integrity are maintained. Please use the email address given psirt@sick.de .

The supplier shall notify SICK immediately about any security incidents within its organization which may impact the security of the *Products* delivered to SICK and follow the process of a coordinated vulnerability disclosure together with SICK.

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

Assessment of maturity

SICK reserves the right to thoroughly test and inspect supplier *Products* regarding their vulnerability. In the event that the test and inspection results will reveal security risks, SICK will notify the supplier and request measures. Test and inspection by SICK will not release the supplier from the development and delivery of secure *Products*.

SICK reserves the right to ask for further documentation and evidence, as well as to perform or order a compliance audit, in order to determine whether the listed requirements are fulfilled.
In case of an audit the exact audit scope, duration and organization will be mutually agreed in each case and in good faith.
In the event that the supplier documentation or audit results reveal gaps in the fulfilment of the SICK requirements, the supplier shall follow SICK's reasonable directions to close such security gaps without undue delay.

Signed in acceptance of the above

_____
Place, Date

_____
Signature

_____
Name

_____
Function

_____
Company