# CYBERSICHERHEIT- ANFORDERUNGEN AN LIEFERANTEN

## Einleitung

Es ist ein wichtiges Ziel der Endress+Hauser SICK GmbH+Co. KG („EHS), ihren 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 EHS-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 EHS 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 EHS 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 EHS verstehen Cybersicherheit als gemeinsame Verantwortung zum Schutz der Kunden von EHS. Innerhalb dieser Verantwortung ist der Lieferant dafür verantwortlich, die Anforderungen aus diesem Dokument einzuhalten. Darüber hinaus liefert der Lieferant sichere und konforme *Produkte* an EHS, die branchenüblich anerkannten Standards im Bereich Cybersicherheit, regulatorischen Standards im Lieferland sowie den EHS-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.

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

## Reifegradbewertung

EHS behält sich vor, *Produkte* von Lieferanten umfassend auf ihre Anfälligkeit hin zu überprüfen. Für den Fall, dass die Ergebnisse Cyber-Sicherheitsrisiken aufzeigen, benachrichtigt EHS den Lieferanten und fordert Maßnahmen ein.

Endress+Hauser
People for Process Automation

Der Lieferant wird die Maßnahmen umsetzen, soweit ihm dies unter besonderer Berücksichtigung der Interessen von EHS zumutbar ist. Test und Prüfung durch EHS entbinden den Lieferanten nicht von der Verantwortung, selbst sichere *Produkte* zu entwickeln und zu liefern.

EHS 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 EHS-Anforderungen aufdecken, wird der Lieferant auf eigene Kosten alle Anstrengungen unternehmen und allen zumutbaren Anweisungen von EHS folgen, um die Abweichungen unverzüglich zu beheben.

Einverstanden:

_____
Ort Datum

_____
Unterschrift

_____
Name

_____
Funktion

_____
Unternehmen