Competence Center Industrial Security

Industrial Security: Mindestempfehlungen zu Security in der Supply Chain

Stand Januar 2022

Vorwort

Die nachfolgenden Empfehlungen sind an Maschinen- und Anlagenbauer gerichtet und beschreiben ein Mindestmaß an technischen, organisatorischen und prozessualen Anforderungen bei der Umsetzung von Security für Produkte (wie z.B. Maschinen, Anlagen, digitale Systeme für Predictive Maintenance & Condition Monitoring, ICS-Steuerungen, ...) und Prozesse. Die Empfehlungen sind als absolutes Minimum zu betrachten und gelten unabhängig von Maschinen- und Anlagentyp, der Komplexität und Industrie.

Je nach Branche und Umfeld kann es gesetzliche oder andere Anforderungen geben, welche diese Mindestempfehlungen übersteigen.

Bei der Erstellung dieses Dokuments boten internationale Security-Normen, Werke von Behörden und Verbänden eine Orientierung:

- IEC 62443
- «ENISA: "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures", November 2017, ISBN: 978-92-9204-236-3»
- Whitepaper BDEW
- EU-NIS Directive

Der Einfachheit halber wird im nachfolgenden Dokument nur von «Maschinen» gesprochen.

Als Unternehmen kann jeder Maschinenbauer mehrere Rollen einnehmen:

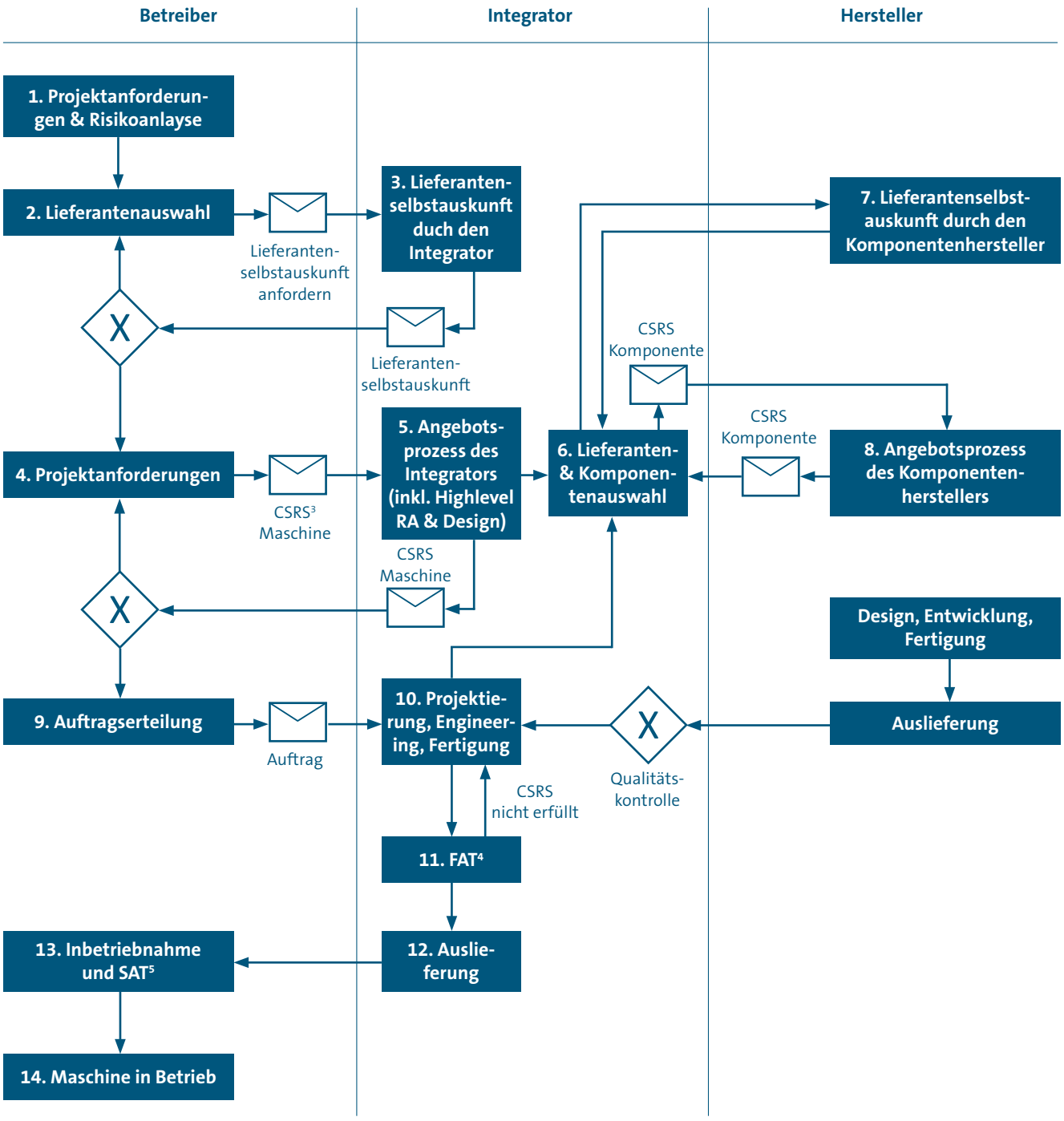
- in erster Linie ist er als Integrator für seinen Kunden tätig
- des Weiteren ist er Betreiber seiner eigenen Fertigungseinrichtung
- wie auch (in selteneren Fällen) als Komponentenhersteller

Durch diese Rollenkombination muss das gegenseitige Verständnis innerhalb der Lieferkette wachsen. Je nach Perspektive / Rolle, die der Maschinenbauer einnimmt, trifft der jeweilige Teil des Dokuments auf ihn zu.

WICHTIG: Die einzelnen Empfehlungen sind unter Beachtung einer individuellen Risiko- und Bedrohungsanalyse anzuwenden. Auf deren Grundlage könnten einzelne Punkte stärker gewichtet werden oder auch komplett entfallen.

2 Prozessbeschreibungen

Beschaffung (OTO) / Entwicklung (OTC)



[1] OTO = Opportunity-to-Order – Prozess von der Identifikation einer Geschäftsmöglichkeit bis hin zu einer erfolgreichen Bestellung
[2] OTC = Order-to-Cash – Prozess von der Bestellung zur Abwicklung, Auslieferung, Inbetriebnahme und Bezahlung
[3] CSRS = Cybersecurity Requirement Specification – Details siehe Abschnitt 3
[4] FAT = Factory Acceptence Test - Prozess zur Abnahme vor der Auslieferung (Werksabnahme)
[5] SAT = Site Acceptance Test - Prozess zur Abnahme am Aufstellort beim Kunden

Im Folgenden werden die drei zentralen Prozesse beschrieben, die den Lebenszyklus von Maschinen immer wieder begleiten und in Bezug auf die Security eine wichtige Rolle spielen.

2.1 Beschaffung (OTO[1]) und Herstellung (OTC[2])

Bei der Beschaffung einer Maschine sind zwischen Betreiber, Integrator und Hersteller ein Informationsaustausch notwendig. Die Abbildung „Beschaffung (OTO) / Entwicklung (OTC)“ zeigt generisch den Prozess, der zwischen diesen Rollen durchlaufen werden muss, um entsprechend der Mindestempfehlungen die Cybersecurity-Anforderungen zu beachten.

Prozessbeschreibung

1. **Projetanforderungen und Risikoanalyse**

   Der Betreiber ermittelt die allgemeinen Anforderungen an die Maschine. Er führt zudem eine Risikoanalyse durch, um die in seiner Umgebung bestehenden Risiken zu bewerten.

2. **Lieferantenauswahl**
   Der Betreiber beginnt mit einer Auswahl der möglichen Integratoren. Dazu definiert er die Anforderungen an den Integrator und fordert eine Lieferantenselbstauskunft an.

   Hinweis

   - Bei bereits bestehenden Lieferantenbeziehrungen muss eine Selbstauskunft nicht angefordert werden.
   - Die Anforderungen können sich auf das Beantworten einer allgemeinen Lieferantenselbstauskunft beschränken und müssen im ersten Schritt keine projektspezifischen Anforderungen enthalten.

3. **Lieferantenselbstauskunft durch den Integrator**

   Der Integrator beantwortet die Lieferantenselbstauskunft und beschreibt die Security-Fähigkeit der Organisation und der Prozesse.

   Mit diesen Informationen entscheidet der Betreiber, ob die Security-Fähigkeiten seinen Anforderungen entsprechen. Ggf. sind Nachforderungen bei der Beschreibung in der Lieferantenselbstauskunft erforderlich oder ein Lieferant scheidet aus.

4. **Projektanforderungen**

   Der Betreiber beschreibt die maschinenspezifischen Projektanforderungen (incl. der Einsatzbedingungen) und dokumentiert diese in einem Security-Lastenheft für die Maschine (CSRS = Cybersecurity Requirement Specification).

5. **Angebotsprozess**

   Im Rahmen des Angebotsprozesses gleicht der Integrator das Lastenheft mit seinem Security-Konzept für die Maschine (High-Level-Risikoanalyse und Design) ab. Der Umfang des Angebotsprozess unterscheidet sich, je nachdem, ob es sich um eine (kunden-)individuelle Maschine oder um eine Serienmaschine handelt.

   Hinweis

   - Aus dem Security-Lastenheft ergeben sich ggf. neue Security-Anforderungen an den Komponentenlieferanten (→ 6. Lieferanten- & Komponentenauswahl beim Integrator).
   - Ziel ist es, dass im Angebotsprozess die Security-Fähigkeiten der Maschine beschrieben werden.

6. **Lieferanten- und Komponentenauswahl des Integrators**

   Auf Basis der projektspezifischen Anforderungen wählt der Integrator die passenden Komponentenlieferanten und Komponenten für die Maschine aus.

7. **Lieferantenselbstauskunft durch den Komponentenhersteller**

   Der Integrator fordert vom Komponentenhersteller eine Selbstauskunft ein, um eine geeignete Auswahl der Lieferanten vornehmen zu können.

8. **Angebotsprozess des Komponentenherstellers**

   Der Integrator beschreibt die komponenten-spezifischen Anforderungen und dokumentiert diese in seinem **Security-Lastenheft (CSRS) für die Komponente**.
   Im Rahmen der Angebotsanfrage teilt der Komponentenhersteller dem Integrator die Security-Fähigkeit seiner Komponente mit.

9. **Auftragserteilung**

   Der Betreiber bewertet das Angebot und beauftragt den Integrator mit dem Bau der Maschine (unter Berücksichtigung der CSRS).

10. **Projektanforderungen, Projektierung, Engineering und Fertigung**

    Der Integrator beginnt anhand der Projektanforderungen mit dem Engineering und der Fertigung.

11. **FAT[6]**

    Am Ende des Herstellungsprozesses erfolgt im Rahmen des Factory Acceptance Test (FAT) die Überprüfung der Security-Eigenschaften.

12. **Auslieferung**

    Im Rahmen der Auslieferung wird die Maschine zum Betreiber geliefert.

13. **Inbetriebnahme und SAT[7]**

    Beim Betreiber wird die Maschine aufgebaut und in Betrieb genommen. Danach erfolgt der Site-Acceptance-Test (SAT) und eine abschließende Prüfung der Security-Eigenschaften.

14. **Maschine in Betrieb**

[6] FAT = Factory Acceptence Test - Prozess zur Abnahme vor der Auslieferung (Werksabnahme)
[7] SAT = Site Acceptance Test - Prozess zur Abnahme am Aufstellort beim Kunden

2.2 Betrieb und Service

Im Folgenden beschreiben wir die Abhängigkeit zwischen Betreiber und Service Anbieter im Hinblick auf die Verfügbarkeit der Maschine im Betrieb. Diese entsteht durch Vereinbarung eines Servicevertrages.

Prozessbeschreibung

1a. Wartung auslösen
durch Betreiber

1b. Wartung auslösen
durch Dienstleister

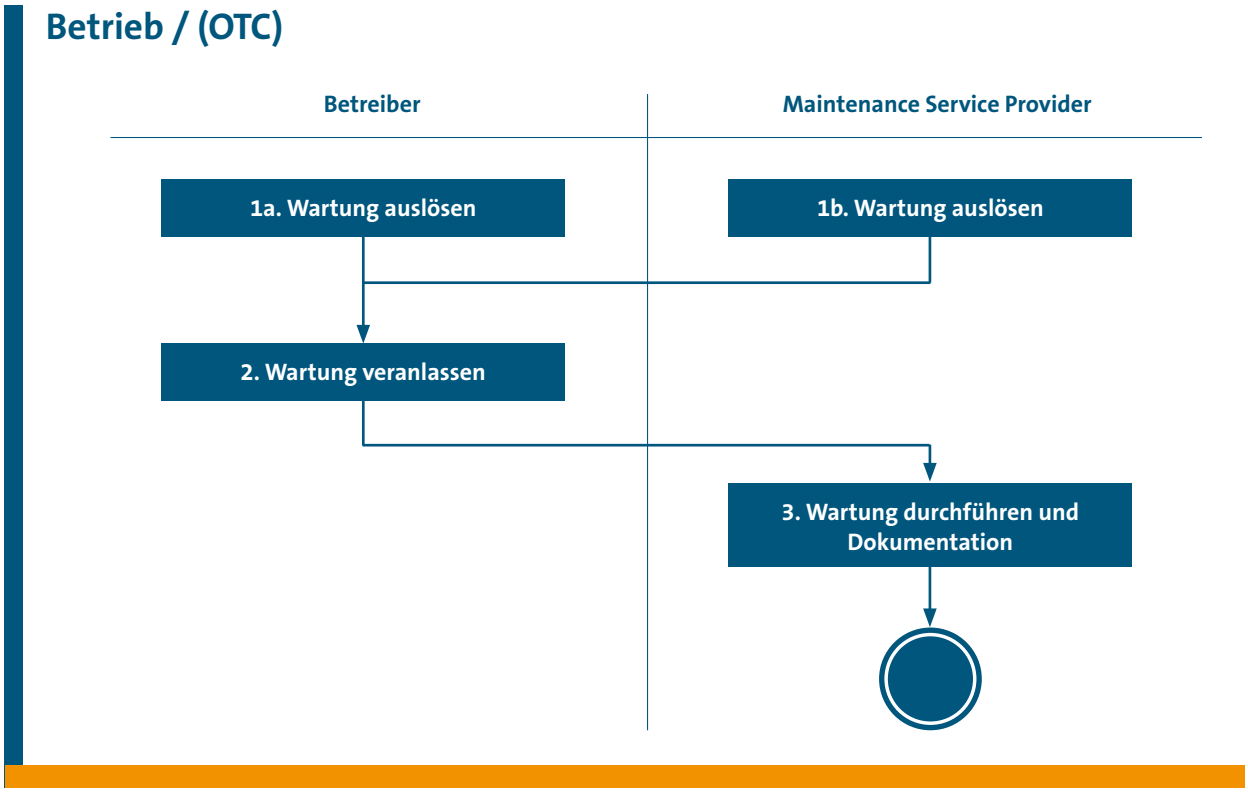
Der Service-Dienstleister informiert den Betreiber über den Wartungsfall.

2. Wartung veranlassen

Daraufhin initiiert der Betreiber einen Fernzugriff (inkl. Autorisierung) oder einen Vor-Ort-Einsatz.

3. Wartung durchführen und dokumentieren

Der Service Dienstleister führt die Wartung durch und dokumentiert dieses.



2.3 Schwachstellen-Management

Ein Schwachstellen-Management ist beim Betreiber, Service Provider, Integrator und Hersteller zu implementieren. Folgende Abbildung soll generisch die Verantwortlichkeiten jeder Rolle darstellen.

Dabei muss mindestens durch den Hersteller, Integrator und ggf. durch den Service Provider kontinuierlich die Überwachung auf Security-Schwachstellen, im Rahmen seiner Produktverantwortung, durchgeführt werden.

Ein besonderes Ereignis tritt auf, wenn eine Schwachstelle identifiziert wird: Dies kann entweder bei dem Hersteller, dem Integrator oder dem Maintenance Service Provider der Fall sein. Die Meldung ist innerhalb des jeweiligen Schwachstellenmanagements zu behandeln.

Prozessbeschreibung

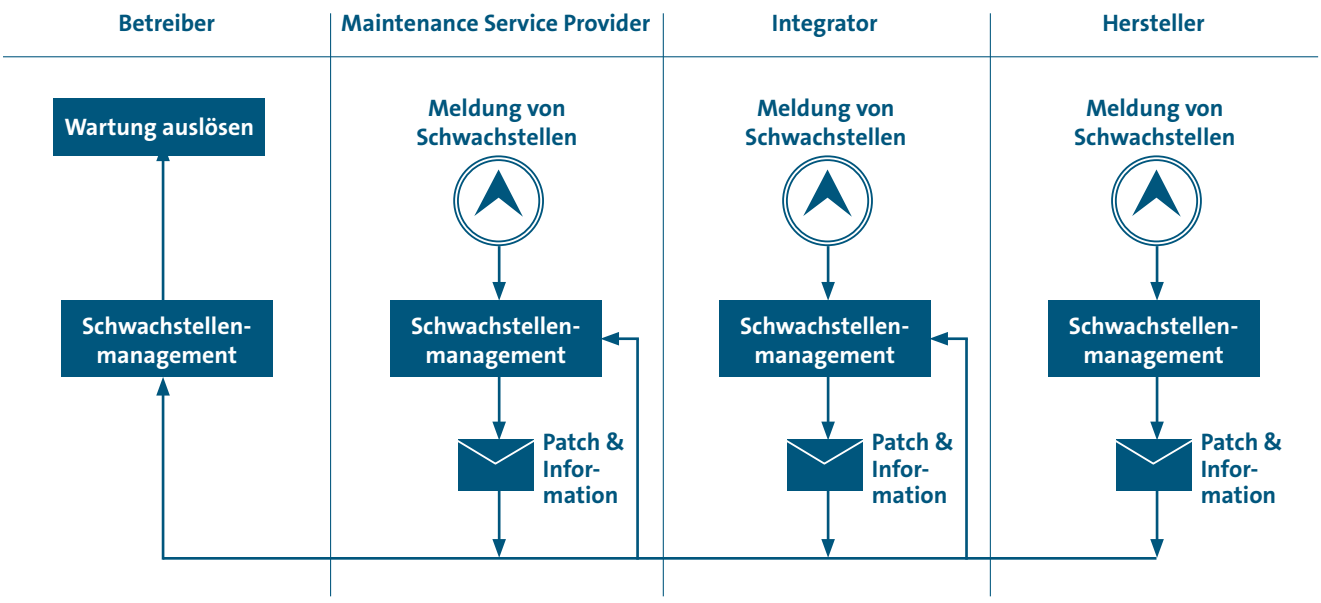
1. Falls eine Schwachstelle vorliegt, ist
   a. durch den Hersteller oder Integrator die Information und der Patch an Integrator, Maintenance Service Provider und Betreiber zu kommunizieren.

   b. durch den Maintenance Service Provider die Information und Patch an den Betreiber zu kommunizieren. Bei vertraglicher Regelung kann durch den Maintenance Service Provider eine Wartung initiiert werden.

2. Der Betreiber muss eingehende Schwachstellenmeldungen ebenfalls in seinem Schwachstellenmanagement behandeln und ggf. eine Wartung veranlassen.

Anmerkung: Die Wartung (inkl. dem Einspielen von Security-Patches) kann ggf. auch durch den Betreiber selbst vorgenommen werden.

Betrieb / (OTC)



3 Mindestempfehlungen für Betreiber

(1) Organisatorisch

Compliance / Governance

- Security-Richtlinien müssen im Unternehmen formuliert, dokumentiert und angewandt werden (von schlanker Policy bis hin zu vollumfänglichem ISMS)
- Die Sicherheitsrichtlinien müssen anwendbar sein auf
  - interne Office-IT (inkl. Service-Rechner)
  - Produktion und
  - externen Dienstleister (z.B. Leistungsbeschreibungen)

Asset-Management der IT-/OT-Devices in der Fertigung, d.h. Sammlung / Übersicht zu

- Technische Informationen
  - IP-Adresse
  - Betriebssystem / Firmware-Version
  - Applikation + Softwareversion
  - Security-Fähigkeiten
- Organisatorische Informationen
  - Lokation, Verantwortlichkeit

Risiko-Management
(z.B. Orientierung an der IEC62443-3-2)

- Risikobeurteilung der bestehenden Produktion und Betrachtung im Sicherheitskonzept
- Risikobeurteilung in der Planungsphase von neuen Maschinen und Festlegung von Security-Anforderungen für die neuen Maschinen.

Sicherheitskonzept
(z.B. Orientierung an der IEC62443-2-4)

- Technische und organisatorische Maßnahmen festlegen.
- Umsetzung des Sicherheitskonzepts.
- Laufenden Durchführung von Assessments (mind. 1 Mal jährl.)

Lieferanten-Management / Engineering-Prozess

- Risikobasierter Ansatz zur Ermittlung der Security-Risiken und Festlegung der erforderlichen Maßnahmen
- Einkaufsbedingungen / Planungsleitfaden
- Konzeption
  - Berücksichtigung des Prinzips «Security by Design»

Erstellen/Aushandeln der CSRS
(cybersecurity requirement specification)

- Bereitstellen von Informationen bezüglich Umgebung, in der die Maschine betrieben werden soll
  - Vorgabe, wo die Maschine, die er bestellt aufgestellt werden soll (Umfeld/Zone)
  - Angaben bzgl. vorhandenen Umsystemen/ Schnittstellen (z.B. Verzeichnisdienst, Log-Server, Zeitsynchronisation, Backupsysteme, Zertifikatsserver, etc.) Was stellt der Betreiber zur Verfügung?
  - Vorgaben für Authentifizierung / Autorisierung
- Bereitstellen und Aushandeln von Security-Anforderungen (SL-T oder Mindestanforderungen).
- Ableitung des «Intended Use» aus den Gegebenheiten seiner eigenen Infrastruktur.
- Maschinenabnahme (SAT): alle in der CSRS definierten Security Maßnahmen müssen überprüft werden
- Serviceverträge: Security Anforderungen (wie z.B. Schwachstellen-Management, Fernzugriff, Monitoring, ...) müssen ggf. ausgehandelt werden.
  - Dienstleister müssen zusichern, dass sein Rechner ordentlich gemanaged ist (aktuelles Betriebssystem, Virenscanner mit aktuellen Signaturen).

Schwachstellen-Management

- für zugekaufte Maschinen und die darin verbauten Komponenten, gemäß Asset Management (inkl. Berücksichtigung von CERT-Meldungen und Meldungen des Herstellers der Maschine)
- ggf. Kommunikation mit dem Integrator/ Lieferanten bzgl. Schwachstellen und Services

Incident Management

- Es muss einen Notfallplan und den entsprechenden Wiederherstellungsprozess geben.

Service Management

- Konzept für eine Service-Unterstützung muss vorhanden sein (evtl. im Rahmen einer internen oder externen Serviceleistung)

Life-Cycle-Management

- Im Rahmen der vertraglichen Vereinbarungen sollten die Partner die Anforderungen an den End-of-Life / End-of-Service festlegen.

Training

- Regelmäßiges Security-Awareness-Training für Mitarbeiter und externe Dienstleister (inkl. Verpflichtungserklärung durch den Mitarbeiter)

(2) Technisch

Infrastruktur

- Physikalischen Schutz (insbes. Zutrittsschutz)
- Vorhalten einer Server-Infrastruktur für generelle Dienste (wie z.B. Verzeichnisdienst, Log-Server, Zeitsynchronisation, Patchmanagement-, Backupsysteme, etc.), sofern dieses für die Erreichung der Security-Anforderungen gemäß seiner CSRS (cybersecurity requirement specification) notwendig wird.
- Netzwerksicherheit (adäquater Schutz des Netzwerks, an welches die Maschine angeschlossen wird). Folgende Ergebnisse kommen typischerweise als technische Anforderungen bei einer Risikobeurteilung heraus:
  - Es muss einen definierten und geschützten Zugang aus dem Produktionsnetz ins Internet geben
  - Produktionsnetz darf nicht direkt mit dem Office-Netz verbunden sein, ggf. weitere Segmentierung der Produktion
  - Netzwerkübergänge müssen geschützt werden durch Einschränkungen in der Kommunikation

Authentifizierung und Autorisierung

- Der Betrieb der Maschine darf nur über Benutzer- oder Gruppenaccounts in Abhängigkeit von Umgebungsrisiken und Betriebsbedingungen erfolgen (der Administrator-User darf im Betrieb nicht verwendet werden)

Netzwerksicherheit (adäquater Schutz des Maschinennetzwerkes):

- Real-Time-Netz («Feldebene») und darüber gelegene Produktionsnetz dürfen nicht direkt miteinander verbunden werden.

Systemwiederherstellung

- Technische Fähigkeit zur Erstellung und Vorhaltung von Backups (inkl. Tests und Virenscan)

Fernzugriff

- Verschlüsselte Verbindung durch das Internet
- Zugang nur in den Bereich (zu der Maschine), der für die Remote-Verbindung notwendig/vorgesehen ist.
- Fernzugriff explizit von Betreiberseite freigegeben
- Protokollierung der Fernzugriffe
- Beim Betrieb von Lösungen, die für den Remote-Zugang vorgesehen sind, müssen vorhandene Good-Practices (z.B. Vorgaben des BSI) berücksichtigt sein

4 Mindestempfehlungen für Integratoren

(1) Organisatorisch

Compliance / Governance

- Security-Richtlinien müssen im Unternehmen formuliert, dokumentiert und angewandt werden (von schlanker Policy bis hin zu vollumfänglichem ISMS)

- Die Security-Richtlinien müssen anwendbar sein auf
  - interne Office-IT (inkl. Service-Rechner)
  - Produktentwicklung / Engineering (z.B. Quality-Gates)
  - Produktion und
  - externen Dienstleister (z.B. Leistungsbeschreibungen)

Asset-Management

- Technische Dokumentation aller in einer Maschine verbauten IT-Komponenten
  - IP-Adresse
  - Betriebssystem / Firmware-Version
  - Applikation + Softwareversion
  - Security-Fähigkeiten

Risiko-Management
(z.B. Orientierung an der IEC62443-3-2)

- Risikobasierter Ansatz zur Ermittlung der Security-Risiken und Festlegung der erforderlichen Maßnahmen (z.B. Systemhärtung zum Schutz der Komponenten) in der Planungsphase von neuen Maschinen.

Sicherheitskonzept
(z.B. Orientierung an der IEC62443-2-4) für das Engineering (sichere Systemintegration) der jeweiligen Maschine

- Technische und organisatorische Massnahmen festlegen.

- Umsetzung und Dokumentation des Sicherheitskonzepts.

- Laufenden Durchführung von Assessments (mind. 1 Mal jährl.)

Lieferanten-Management

- Integrator muss sich mit den Komponentenlieferanten abstimmen bzgl.
  - Informationen zum «Intended Use» (bestimmungsgemäßer Gebrauch) einer Komponente abholen
  - Nachweis der Security-Fähigkeit von Produkt/Prozess des Komponentenlieferanten (z.B. externe Zertifizierung, Selbsterklärung oder vertragliche Einkaufsbedingungen)
  - Lifecycle der Produkte für den Gewährleistungszeitraum und darüber hinaus
  - Berücksichtigung des Prinzips «Security by Design»

- Serviceverträge: Security Anforderungen (wie z.B. Schwachstellen-Management, Fernzugriff, Monitoring, ...) müssen ggf. ausgehandelt werden.
  - Dienstleister müssen zusichern, dass sein Rechner ordentlich gemanaged ist (aktuelles Betriebssystem, Virenscanner mit aktuellen Signaturen).

Engineering-Prozess

- Sicherstellen einer sicheren Umgebung für die System-Integration.
- Richtlinien, welche die Berücksichtigung von Security bei der System-Integration fordern.
- Integrator muss sich mit dem Betreiber abstimmen bzgl.
  - Informationen zum «Intended Use» (bestimmungsgemäßer Gebrauch) einer Maschine liefern
  - Abgleich der Security-Anforderungen des Betreibers mit den Security-Fähigkeiten der spezifischen Maschine (CSRS)
- Abgleich zwischen gefordertem (SL-T oder Mindestanforderung) und erreichtem (SL-A oder umgesetzten Maßnahmen) Security-Level
  - Dokumentation des bestimmungsgemäßen Gebrauchs, was betreiberseitig vorausgesetzt wird («Intended Use»).
- Dokumentation einer sicheren Konfiguration und deren Betrieb (z.B. Patch-Management)

Schwachstellen-Management

- für eigene und zugekaufte Komponenten (Berücksichtigung von CERT-Meldungen)
  - Berücksichtigung der Security-Patches mit hoher Kritikalität (z.B. CVSS-Score > 7)
- Kunden-Kommunikation (verantwortliche Person benennen; Meldungen von Kunden aufnehmen und Informationen über neue Schwachstellen für Kunden bereitstellen – Aufbau PSIRT)
- Festlegung des freigegebenen Softwarestandes ("Baseline"), der beim Bau einer Maschine berücksichtigt werden soll.
  - Bei der Festlegung sollen Security-Patches beachtet werden.

Serviceverträge

- Security-Fähigkeiten (wie z.B. Patch-Management, Fernzugriff, Monitoring, ...) können angeboten werden

Systemwiederherstellung

- Erstellung und Vorhaltung von Backups (inkl. Tests)
- Bereitstellung sämtlicher, zur Wiederherstellung benötigter Daten (Konfigurationsdaten, Software/Applikationen, Daten)

Life-Cycle-Management

- Im Rahmen der vertraglichen Vereinbarungen sollten die Partner die Anforderungen an den End-of-Life / End-of-Service festlegen. Abgekündigte Komponenten sollten im Engineering nicht mehr verwendet werden.

Training

- Regelmäßiges Security-Awareness-Training für Mitarbeiter (z.B. Inbetriebnehmer, Entwickler) und externe Dienstleister (inkl. Verpflichtungserklärung durch den Mitarbeiter)

(2)Technisch

Infrastruktur

- [Anm.: Für Integrator nur in der Rolle als Betreiber seiner eigenen Fertigung notwendig.]

Authentifizierung und Autorisierung

- Authentifizierung von Benutzern oder Benutzergruppen in Abhängigkeit von Umgebungsrisiken und Betriebsbedingungen, z.B. zwingende Authentifizierung für Konfigurationsänderungen.
- Bei der Inbetriebnahme müssen individuelle Passwörter für den Einzel-User und Admin eingerichtet werden, dies gilt insbesondere für die Konfiguration und den Zugang zu Schnittstellen wie z.B. ext. Netzwerk oder HMI.
- Für Maschinenanwender, die als Nutzer nur auf eingeschränkte Funktionen zugreifen können, sollten Benutzer oder Gruppenaccounts in Abhängigkeit von Umgebungsrisiken und Betriebsbedingungen erstellt werden.
- Nicht notwendige Accounts sollen gelöscht oder deaktiviert werden.

Netzwerksicherheit

(adäquater Schutz des Maschinennetzwerkes):

- Safety- und Produktionsnetz sind getrennt (gem. IEC 62443-3-3 SR5.1)
- Real-Time-Netz («Feldebene») und darüber gelegene Produktionsnetz sind getrennt

Systemhärtung

- Umsetzung des definierten Patch-Levels (Baseline) für die zusammengehörigen Komponenten (mind. 1 Mal jährlich)
- Keine Verwendung von Legacy-Systemen, die von Herstellern nicht mehr supportet werden
- Nicht benötigte Ports schließen
- Nicht benötigte Dienste deaktivieren
- Umsetzen der vom Komponentenhersteller empfohlenen Härtungsmaßnahmen, z.B. aktivieren der Windows-Features UWF & AppLocker (Whitelisting)

Systemwiederherstellung

- Technische Fähigkeit zur Erstellung und Widerherstellung von Backups (inkl. Tests)
- Möglichkeit zur Wiederherstellung der Werkseinstellungen

Fernzugriff

- Risikoanalyse zur Ermittlung, auf welche Systeme/Komponenten zugegriffen werden darf
- Verschlüsselte Verbindung
- Fernzugriff explizit von Betreiberseite freigegeben
- Technische Fähigkeit Protokollierung der Fernzugriffe
- Bei der Auswahl von Komponenten, die für den Remote-Zugang vorgesehen sind, müssen vorhandene Good-Practices (z.B. Vorgaben des BSI) berücksichtigt sein.

5 Mindestempfehlungen für Komponentenlieferanten

(1) Organisatorisch

Compliance / Governance

- IT-Security-Richtlinien müssen im Unternehmen formuliert, dokumentiert und angewandt werden (von schlanker Policy bis hin zu vollumfänglichem ISMS)
- Die Sicherheitsrichtlinien müssen anwendbar sein auf
  - interne Office-IT (inkl. Service-Rechner)
  - Produktentwicklung / Engineering (z.B. Quality-Gates)
  - Produktion und
  - externen Dienstleister (z.B. Leistungsbeschreibungen)

Risiko-Management
(z.B. Orientierung an der IEC62443-3-2)

- Risikobasierter Ansatz zur Ermittlung der Security-Risiken und Festlegung der erforderlichen Maßnahmen in der Planungsphase von neuen Komponenten.

Sicherheitskonzept
(z.B. Orientierung an der IEC62443-2-4) für das Engineering

- Technische und organisatorische Massnahmen festlegen.
- Umsetzung und Dokumentation des Sicherheitskonzepts.
- Laufenden Durchführung von Assessments (mind. 1 Mal jährl.) zur Kontrolle, ob das Sicherheitskonzept korrekt umgesetzt ist.

Engineering-Prozess
(z.B. Orientierung an der IEC62443-4-1)

- Sicherstellen einer sicheren Umgebung für die Produktentwicklung.
- Richtlinien, welche die Berücksichtigung von Security bei der Produktentwicklung fordern.
- Berücksichtigung des Prinzips «Security by Design» in der Softwareentwicklung basierend auf «Best Practices» (z.B. OWASP Top 10), inkl. entsprechendem Nachweis.
- Möglichkeit zur Integritätsprüfung von Software (inkl. Dokumentation).
- Abgleich zwischen markterforderlichem (SL-T oder Mindestanforderung) und erreichtem (SL-C oder umgesetzten Maßnahmen) Security-Level
  - Dokumentation des bestimmungsgemäßen Gebrauchs («Intended use»)
  - Dokumentation einer sicheren Konfiguration und dessen Betrieb (z.B. Patch-Management)
- Komponentenlieferant sollte sich regelmäßig mit den interessierten Integratoren abstimmen bzgl.
  - Nachweis der Security-Fähigkeit der Komponenten (z.B. externe Zertifizierung, Selbsterklärung oder vertragliche Einkaufsbedingungen)

Schwachstellen-Management

- Für eigene und zugekaufte Komponenten (Berücksichtigung von CERT-Meldungen)
- Kunden-Kommunikation (verantwortliche Person benennen; Meldungen von Kunden aufnehmen und Informationen über neue Schwachstellen für Kunden bereitstellen – Aufbau PSIRT)
- Berücksichtigung der Security-Patches mit hoher Kritikalität (z.B. CVSS-Score > 7)
- Festlegung des Softwarestandes, für die Aufbringung in die Hardware-Komponente, bei dem die freigegebenen Security-Patches mit eingeschlossen sind – min. 1 Mal jährlich.

Asset-Management

- Technische Dokumentation bezüglich Komponenten-Eigenschaften
  - S/N, MAC, Betriebssystem / Firmware-Version
  - Applikation + Softwareversion
  - Security-Fähigkeiten

Service-Management

- Security-Fähigkeiten (wie z.B. Patch-Management) sollen ggf. im Rahmen von Serviceverträgen angeboten werden
- Serviceverträge: Security Anforderungen (wie z.B. Schwachstellen-Management, Fernzugriff, Monitoring, ...) müssen ggf. ausgehandelt werden.
  - Dienstleister müssen zusichern, dass sein Rechner ordentlich gemanaged ist (aktuelles Betriebssystem, Virenscanner mit aktuellen Signaturen).

Life-Cycle-Management

- Im Rahmen der vertraglichen Vereinbarungen sollten die Partner die Anforderungen an den End-of-Life / End-of-Service festlegen. Abgekündigte Komponenten sollten im Engineering nicht mehr verwendet werden.

Training

- Regelmäßiges Security-Awareness-Training für Mitarbeiter, die in der Produktentwicklung arbeiten und externe Dienstleister (inkl. Verpflichtungserklärung durch den Mitarbeiter)

(2) Technisch

Infrastruktur

- [Anm.: Für Komponentenhersteller nur in der Rolle als Betreiber seiner eigenen Fertigung notwendig.]

Authentifizierung und Autorisierung

- Technische Fähigkeit eine Authentifizierung zu erzwingen.
- Eine Userverwaltung für Einzel-User, User-Gruppen und Admins muss vorhanden sein
  - universelle Standardpasswörter bei der Auslieferung sind zulässig; über eine begleitende Dokumentation muss der Integrator auf eine notwendige Änderung der Passwörter vor der Erstinbetriebnahme hingewiesen werden.
- Der Betrieb der Komponente muss über Einzel-User oder User-Gruppen erfolgen (der Betrieb über Admin-User ist im Standardbetrieb nicht gestattet)

Systemhärtung

- Grundhärtung der Komponente (Security by Design)
  - Nicht benötigte Ports schließen
  - Nicht benötigte Dienste deaktivieren
  - Widerstandsfähigkeit der Komponente (z.B. gegenüber OpenVAS oder Nessus)
- Dokumentation von Härtungsmaßnahmen, Empfehlungen an den Integrator
- Keine Verwendung von Zukauf-Komponenten, die von Herstellern nicht mehr supportet werden oder bei denen eine Abkündigung des Supports absehbar ist.
- Zum Zeitpunkt der Aufbringung der Software in die Hardware-Komponente muss ein aktueller Softwarestand dafür verwendet werden, bei dem die freigegebenen Security-Patches mit eingeschlossen sind.

Systemwiederherstellung

- Möglichkeit zur Wiederherstellung der Werkseinstellungen
- Backup-Möglichkeit für sämtliche relevante Daten (inkl. Dokumentation)

Mindestfähigkeiten
(abhängig vom Komponententyp)

- Anforderungen gemäss SL-T1 aus IEC62443-4-2 als Minimum (ist dies nicht möglich, müssen Ausgleichsmaßnahmen umgesetzt und dokumentiert werden)

Fernzugriff

- Bei Komponenten, die für den Remote-Zugang vorgesehen sind, müssen vorhandene Good-Practices (z.B. Vorgaben des BSI) umgesetzt sein.

Mitarbeitende an den Mindestempfehlungen

Florian Buschor	Syntegon Technology GmbH
Jens Cordt	Bundesamt für Sicherheit in der IT
Bernd Gehring	J.M. Voith SE & Co. KG
Martin Holtmannspötter	Robert Bosch GmbH
Marcel Hug	ZVEI e.V.
Maximilian Korff	Siemens AG
Thomas Lantermann	Mitsubishi Electric Europe B.V.
Jochen Müller	Bizerba SE & Co. KG
Rainer Traub	Balluff GmbH
Alexander Wahl	Festo SE & Co. KG
Bernd-Ulrich Wittwer	Weidmüller Interface GmbH & Co. KG
Steffen Zimmermann	VDMA e.V.

Impressum

VDMA
Competence Center Industrial Security

Lyoner Straße 18
60528 Frankfurt am Main

Kontakt
Telefon 069 6603-1978
E-Mail steffen.zimmermann@vdma.org
Internet www.vdma.org/cybersecurity

Layout
VDMA DesignStudio

VDMA
Competence Center Industrial Security

Lyoner Straße 18
60528 Frankfurt am Main

Steffen Zimmermann
Telefon 069 6603 1978
E-Mail steffen.zimmermann@vdma.org
Internet www.vdma.org/cybersecurity

www.vdma.org/cybersecurity

VDMA DesignStudio