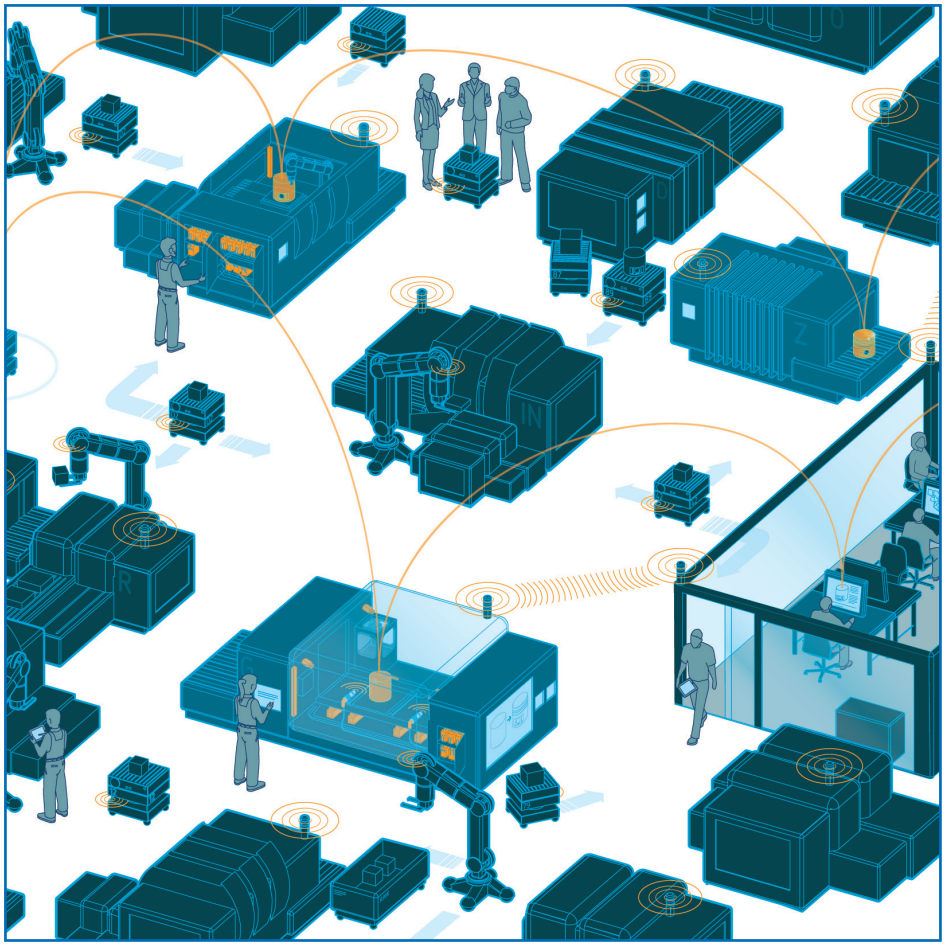
ZVEI:
Die Elektroindustrie

Whitepaper

Schutz der Integrität von Daten, Systemen und Prozessen in der Produktion – Kernelement der Digitalisierung in der Industrie

Teil 2



Zentralverband Elektrotechnik- und Elektronikindustrie

ZVEI:
Die Elektroindustrie

Schutz der Integrität von Daten, Systemen und Prozessen in der Produktion – Kernelement der Digitalisierung in der Industrie

Teil 2 – Version 1.0

Herausgeber:
ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e.V.
Fachverband Automation
Lyoner Straße 9
60528 Frankfurt am Main

Redaktion: Lenkungskreis Industrial Security

Verantwortlich: Stefanie Wiesner
Telefon: +49 69 6302-392
E-Mail: wiesner@zvei.org
www.zvei.org

November 2019

Inhalt

1 Zielsetzung

Dieses Dokument bündelt die technischen Diskussionen des LK Industrial Security des ZVEI hinsichtlich der Anforderungen, Validierung und Umsetzung der Integrität von Daten, Systemen und Prozessen in der Produktion.

Zielsetzung des Dokuments ist, ein gemeinsames Verständnis zum Thema Integrität im Kontext einer Produktion zu entwickeln. Das Papier dient als Diskussionsgrundlage, zur Wissensvertiefung und als Orientierungshilfe für andere Arbeitsgruppen im Bereich Industrial Security und Industrie 4.0.

Das Dokument geht auf die Fragestellung ein, inwiefern zum Beispiel die Korrektheit, Unveränderbarkeit und Vollständigkeit (= Integrität) von Daten, Systemen und Prozessen in der Produktion bereitgestellt, überprüft und diesbezüglichen Störungen begegnet werden kann. Im Fokus stehen technische Daten; das heißt personenbezogene Daten und damit die Aspekte des Datenschutzes werden nicht betrachtet, um einen angemessenen Umfang zu wahren.

Die Ausführungen adressieren insbesondere die Produktionsabläufe von Komponentenherstellern und ihren Verantwortlichen. Im Speziellen sind sowohl die Sicherheitsverantwortlichen in der Fertigung angesprochen, da die hier beschriebenen Bedrohungen und Sicherheitsmechanismen ihre Anlagen und Prozesse betreffen. Ebenso sind Integratoren, die Anlagen oder Anlagenteile zur Verfügung stellen, angesprochen, da die technischen und organisatorischen Voraussetzungen zur Umsetzung der Sicherheitsmaßnahmen durch sie geschaffen werden müssen. Als dritter Adressat dieses Papiers sind die Entwicklungsabteilungen zu nennen, welche die herzustellenden Produkte entwickeln, da diese Produkte ebenfalls Mechanismen zur Sicherstellung ihrer Integrität enthalten müssen. Auch die Übergabeprozesse für Daten und Software zwischen Entwicklung und Fertigung sind für die Integrität des Produkts bedeutend. Die Fragestellungen in diesem Papier sind auch im Kontext von internationalen Zulieferbeziehungen und unternehmensübergreifenden Kooperationen relevant und besitzen damit Bedeutung über die Security-Community hinaus. Das Whitepaper adressiert daher auch Verantwortliche für den Einkauf.

2 Einführung

Digitalisierung und Vernetzung erfordern zwingend ein Vertrauen in die Integrität von eigenen und zunehmend von externen Daten und in die einwandfreie Funktion von Systemen und Prozessen. Dies ist fundamental für alle Geschäftsprozesse innerhalb und außerhalb eines Unternehmens. Zusätzlich betont die Politik auf internationaler, europäischer und nationaler Ebene die Wichtigkeit der Cybersicherheit von Infrastrukturen und Systemen. Infolgedessen sind zum Beispiel mit dem IT-Sicherheitsgesetz[1] und der NIS-Richtlinie[2] für Produkte im Industrie- und Verbraucherbereich bereits Security-Anforderungen entstanden, in denen die Einhaltung des Stands der Technik eingefordert wird. Letzteres wird für den Industriebereich vor allem in IEC 62443 beschrieben. Hierin finden sich Anforderungen unter anderem an die Komponenten und Entwicklungsprozesse. Der Schutz der Integrität von Daten, Systemen und Prozessen ist dabei ein wesentlicher Bestandteil. Das vorliegende zweite Whitepaper soll Industrieunternehmen helfen, diesbezüglich ihre Geschäftsprozesse abzusichern und sich auf die Regulierungsanforderungen einzustellen.

[1] https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/it_sig_node.html
[2] https://www.bsi.bund.de/DE/DasBSI/NIS-Richtlinie/NIS_Richtlinie_node.html

Das erste Whitepaper „Integrität von Daten, Systemen und Prozessen als Kernelement der Digitalisierung“[3] von 2018 stellt bereits eine Grundlage dar, indem es ein gemeinsames Verständnis zum Thema Integrität im Kontext internationaler unternehmensübergreifender Kooperationen sowie der zunehmenden Digitalisierung von Produkten und Systemen (Stichwort: Industrie 4.0) entwickelt. Dabei werden Daten- und Systemintegrität sowie Bestimmung der Gesamtintegrität thematisiert und exemplarische Maßnahmen zur Prüfung und Gewährleistung der Integrität bei bestimmten Bedrohungen dargestellt. Im Hinblick auf die notwendigen Maßnahmen werden insbesondere die Komponentenhersteller, aber auch die nachgeschalteten Integratoren und Betreiber angesprochen.

Das vorliegende Whitepaper behandelt die Integrität der Produktion am Beispiel von Produktionsprozessen von Komponenten in der Fertigung. Integrität ist ein essenzielles Schutzziel und damit ein wesentlicher Bestandteil von Cybersicherheit. Jedoch wird sie häufig nur als technischer Aspekt betrachtet. Ist die Integrität in der Produktion gestört, hat das aber direkte Auswirkungen auf die Wirtschaftlichkeit, die Reputation sowie die Produktqualität oder gefährdet die Einhaltung regulatorischer Vorgaben.

Viele der Inhalte dieses Papiers können analog auch auf die Produktionsprozesse von Maschinen bei einem Maschinenbauer übertragen werden.

3 Big Picture

Die IEC 62443-4-1 legt die Anforderungen an den gesicherten Entwicklungsprozess und an den Lebenszyklus für Produkte fest, die in industriellen Automatisierungssystemen eingesetzt werden. Der definierte Security-Development-Lifecycle (SDL) ergänzt bestehende Produktentstehungsprozesse. Die nachfolgende Abbildung 1 illustriert die zu betrachtenden Phasen (hellblau).

Abb. 1: Security-Development-Lifecycle

Quelle: ZVEI (abgeleitet aus Microsoft Security Development Lifecycle)

Diese Anforderungen können für neue oder vorhandene Prozesse der Entwicklung, Instandhaltung und Pflege von Hardware, Software oder Firmware für neue oder vorhandene Produkte angewendet werden.

Zur vollständigen Abdeckung des Security-Lifecycle muss der sichere Entwicklungsprozess noch um eine Phase „Production“ (sichere Fertigung) ergänzt werden (orange).

Die für diese Phase notwendigen Anforderungen und Prüfkriterien sind im Rahmen des sicheren Entwicklungsprozesses zu identifizieren und in einem Anforderungsdokument für die Fertigung zu dokumentieren. Kapitel 5 geht im Detail auf die Produktionsanforderungen ein, die aus den Produktanforderungen abgeleitet wurden und die fertigungsseitig zu berücksichtigen sind, wie zum Beispiel:

[3] https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/hm-2018-integritaet-daten.html

a. Produktanforderung: Produkt soll das Werk mit der aktuellen Software verlassen
   a. Produktionsanforderung: Software kann bei Bedarf (mehrmals) aufgespielt werden
b. Produktanforderung: Produkt hat eine digitale Geräteidentität
   a. Allgemein: Die digitale Geräteidentität unterstützt die Nachverfolgbarkeit über den Lebenszyklus des Produkts
   b. Produktionsanforderung: In der Produktion wird eine digitale Geräteidentität sicher aufgebracht
c. Produktanforderung: Die Integrität des Produkts soll sichergestellt werden
   a. Allgemein: Abweichungen (z. B. Änderungen HW/SW, Konfiguration) von dem definierten Zustand können erkannt werden
   b. Produktionsanforderung: Die Integrität der auf das Gerät aufzuspielenden SW muss geprüft werden, darüber hinaus sollte das Produkt Möglichkeiten zur Integritätsprüfung über den Produktlebenszyklus bieten
d. Produktanforderung: Produkt soll „Secure by default" ausgeliefert werden
   a. Allgemein: Sicherheitsverbesserende Maßnahmen sind in der Entwicklung bereits zu treffen. Die Auslieferungskonfiguration soll „Secure by default" sein, das bedeutet unter anderem, dass alle nicht benötigten, gegebenenfalls unsicheren Dienste ausgeschaltet sind
   b. Produktionsanforderung: In dem Endfunktionstest ist dies sicherzustellen und zu dokumentieren

In Kapitel 5 wird die Phase „Production" aus Abbildung 1 näher betrachtet.

Abb. 2: Phase „Production"

Quelle: ZVEI

Die Phase „Allgemein" (Kapitel 5.1) skizziert die notwendigen Voraussetzungen und Anforderungen an die Produktionsumgebung zur Sicherstellung einer geeigneten Umgebung und zur sicheren Produktion des Produkts.

Übergreifende Aspekte:

Das Supply-Chain- und Qualitätsmanagement sind Schlüsselkomponenten für die Gewährleistung der Integrität. Sie stellen im Sinne des Input-Output-Prinzips sicher, dass integre Vorprodukte als Voraussetzung für die Produktion vorhanden sind, sodass am Ende ein Produkt mit einer Integritätszusicherung an den Kunden übergeben werden kann. So baut ein durchgängiger Integritätsschutz auf folgenden Kernelementen auf:

- Auswahl der Zulieferer: Die Zulieferer sollten auch im Hinblick auf ihre Integritätszusicherungen, -maßnahmen und -prozesse hin bewertet und gegebenenfalls validiert werden.
- Kontrolle der Vorprodukte: Die Korrektheit, Vollständigkeit und Herkunft der Vorprodukte sind bei Anlieferung zu prüfen. Je nach Kontext reicht die Sichtkontrolle der Verpackung und Produkte nicht aus. Es sollten auch die Funktionen und gegebenenfalls Designs überprüft werden (siehe Kapitel Arbeitsvorbereitung). Dies kann Maßnahmen zur Detektion von nicht dokumentierten Funktionen (z. B. Backdoors) einschließen.

- Die Vorprodukte bestimmen maßgeblich die Integrität der Hardware-Produktion. Denn im Regelfall kommen hier gängige – vom Integritätsschutz unabhängige – Methoden zum Einsatz (zum Beispiel Sichtprüfung und Nadeladapter). Wären die Vorprodukte bereits unbemerkt kompromittiert, kann dies bei der Hardware-Produktion schwer erkannt und kaum korrigiert werden.
- Qualitätskontrolle des Endprodukts: Anhand von Testplänen aus der Produktentwicklung muss das Endprodukt gleichermaßen dezidiert auf Korrektheit und Vollständigkeit hin überprüft werden. Nur so kann dem Kunden die durchgängige Qualitäts- und Integritätszusicherung gegeben werden.

4 Entwicklung

Unter der Entwicklung werden hier die Phasen „Requirements" bis „Release" gesehen (siehe Abbildung 1). Produkte haben in der Regel eine Vielfalt späterer Verwendungsmöglichkeiten. Dabei können die Produkte isoliert oder aber auch als Bestandteil größerer Systeme eingesetzt werden. Diese Verwendungsmöglichkeiten unterscheiden sich meist auch hinsichtlich der erforderlichen Security, davon abhängig ergeben sich jeweils unterschiedliche Security-Anforderungen an das Produkt selbst. In der Entwicklungsphase müssen diese Anforderungen identifiziert und festgehalten und im Rahmen von Security by Design die erforderlichen Funktionen zur Erfüllung dieser Anforderungen spezifiziert werden.

Um das Produkt mit den geforderten Security-Eigenschaften entsprechend herstellen zu können, ergeben sich bei der Entwicklung des Produkts darüber hinaus auch weitere Security-Anforderungen für den Fertigungsprozess. Die Erfüllung dieser Anforderungen betreffen dabei sowohl das Produkt selbst als auch die Produktion und können entweder durch entsprechende Funktionen oder aber auch durch die Fertigungsprozesse bei der Herstellung und Auslieferungsvorbereitung sichergestellt werden. Zur besseren Verdeutlichung sind im Folgenden exemplarisch einige Security-Anforderungen an Produkt und Produktion beschrieben, die sich im Rahmen der Entwicklung für die Phase des Fertigungsprozesses ergeben können.

1. Aktuelle freigegebene Software bei Auslieferung

Produkte bestehen oft aus Hardware und Software. Gerade die Software unterliegt meist kontinuierlichen Änderungen und Erweiterungen. Im Rahmen einer Softwarepflege werden Sicherheitslücken, Softwarefehler oder sonstige Softwareschwachstellen entdeckt und durch entsprechende Softwareupdates beseitigt.

Um eine sichere Verwendung des Produkts mit all den erforderlichen Funktionen in den jeweiligen Einsatzszenarien zu gewährleisten, ist es somit eine wichtige Security-Anforderung, dass das Produkt am Ende des Fertigungsprozesses vor der Auslieferung mit der aktuellen Softwareversion versehen wird. Ein Fertigungsprozess kann sich auch über einen längeren Zeitraum erstrecken, beispielsweise kann ein Produkt als eine Art „Halbfabrikat" vorgefertigt und erst vor Auslieferung final gefertigt werden. Dabei kann es durch den Fertigungsprozess erforderlich sein, dass die Software auch in Teilmodulen zu unterschiedlichen Zeitpunkten aufgespielt wird. Dies erfordert von der Produktion, dass ein gegebenenfalls auch mehrmaliges Aufspielen von Software während der Produktion möglich sein sollte.

2. Digitale Geräteidentität

Die Nachverfolgbarkeit von Produkten ist in der Produktion eine wichtige Eigenschaft, die zu unterschiedlichen Zwecken genutzt wird. Zum einen kann sie die Nachverfolgbarkeit vom Hersteller zum Kunden ermöglichen, damit der Hersteller Kenntnis erhalten könnte, wo und von wem seine Produkte eingesetzt werden. Durch diese Kenntnis könnte er beispielsweise weitere Dienstleistungen zum Produkt gezielt den Kunden anbieten und dadurch die Kundenbindung stärken oder aber auch bei erforderlichen Rückrufen gezielt auf die Kunden zugehen. Zum anderen gibt es die Nachverfolgbarkeit vom Kunden zum Hersteller, damit könnten beispielsweise bei auftretenden Problemen in der Verwendung des Produkts (z. B. wenn eine Manipulation am Produkt erkannt wird) gezielt der Hersteller ermittelt und somit entsprechende Maßnahmen eingeleitet werden.

Eine Nachverfolgbarkeit von Produkten ist aber auch während des Fertigungsprozesses von Vorteil: Werden beispielsweise bei der finalen Qualitätskontrolle vor der Auslieferung Mängel im Produkt entdeckt, so lassen sich schnell die einzelnen involvierten Produktionsschritte sowie die verwendeten Komponenten identifizieren, analysieren und somit die Ursache der Mängel lokalisieren und beheben.

Zur Umsetzung der Nachverfolgbarkeit besteht als Security-Anforderung an das Produkt, dass jedes Produkt identifizierbar ist, das heißt eine entsprechende digitale Identität besitzt. Dies kann beispielsweise bei einem Embedded System eine entsprechende digitale Geräteidentität sein. Im Fertigungsprozess werden diese digitalen Identitäten bei den einzelnen Produktionsschritten verwendet, um zum Beispiel dem Produkt Produktionsparameter wie das eingebaute Netzteil, die vorgesehene Netzspannung, kundenspezifische Ausstattungsmerkmale oder allgemeine Dokumentation hinzuzufügen.

3. Erkennung von Änderungen

Für die Herstellung sicherer Produkte ist es essenziell, dass eine Auslieferung des Produkts genau in dem Zustand und mit der Funktionalität erfolgt, die im Rahmen der Entwicklung festgelegt wurde. Um dies während der Produktion sicherzustellen, müssen die einzelnen Produktionsschritte entsprechend dokumentiert und die im jeweiligen Schritt erfolgten Änderungen am Produkt erfasst werden. Durch eine genaue und lückenlose Dokumentation der einzelnen Produktionsschritte und den dabei erfolgten Änderungen am Produkt kann nachvollzogen werden, dass das ausgelieferte Produkt den entsprechenden Spezifikationen entspricht. Es ist dabei zu berücksichtigen, dass es während der Produktion auch zu unerwünschten Änderungen am Produkt kommen kann. Gründe dafür können fehlerhafte Produktionsprozesse sein oder aber auch eine gezielte Manipulation durch Innentäter oder externe Angreifer.

Damit ergibt sich als Security-Anforderung an das Produkt, dass sich entsprechende Änderungen erkennen lassen. Zudem besteht die Security-Anforderung an die Produktion, dass in den einzelnen Produktionsschritten überprüft wird, ob Änderungen am Produkt vorgenommen wurden und, falls ja, ob diese entsprechend sicher (z. B. unter Verwendung digitaler Signaturen) dokumentiert wurden.

4. „Security by Default"-Auslieferung

Je umfangreicher der Funktionsumfang von Produkten ist, desto vielfältiger sind meist die Einsatzmöglichkeiten, aber auch die Möglichkeiten zum Missbrauch. Gerade im Softwarebereich ist dies leicht nachvollziehbar: Je mehr „Lines of Code" eine Software enthält,

desto höher ist die Wahrscheinlichkeit für Softwarefehler, die wiederum gern von Angreifern ausgenutzt werden. Deshalb ist es aus Security-Gründen eine sinnvolle Maßnahme, die Produkte entsprechend zu härten, das heißt möglichst nur den minimalen, für die Einsatzzwecke des Produkts erforderlichen Funktionsumfang auszuliefern. Verwendet ein Produkt beispielsweise offene Betriebssysteme, so empfiehlt es sich, nur solche Module des Betriebssystems in das ausgelieferte Produkt mitaufzunehmen, welche auch wirklich benötigt werden. Es sind alle Ports zu deaktivieren, die für eine Inbetriebnahme nicht notwendig sind. Das heißt, alle Services sind vom Kunden per Opt-In zuzuschalten. Damit besteht als Security-Anforderung an das Produkt, dass dieses nur in einem entsprechend gehärteten Zustand ausgeliefert wird. Die Härtung muss in den passenden Produktionsschritten konkret vorgenommen beziehungsweise sichergestellt werden. Entsprechend ist dies als Security-Anforderung an die Produktion zu definieren.

Für die Durchführung dieser Härtung gibt es zahlreiche Empfehlungen und Best Practices. Das „Center for Internet Security" (CIS) veröffentlicht beispielsweise derartige Benchmarks für die sichere Konfiguration von Cloud- und Virtualisierungsplattformen, Betriebssystemen, mobilen Geräten oder Browsern.[4] Das Open Web Application Security Project (OWASP) stellt einen „Application Security Verification"-Standard (ASVS) zur Verfügung[5], der den Entwicklern webbasierter Anwendungen Empfehlungen zur sicheren Implementierung gibt.

Diese Empfehlungen lassen sich auch im Kontext der Härtung als eine Art Checkliste verwenden, um die Umsetzung der erforderlichen Sicherheitsfunktionen zu verifizieren beziehungsweise zu testen.

5 Produktion

In der IT-Welt etablierte Security-Mechanismen sind aufgrund der Spezialisierung der Systeme, langen Lebenszyklen und extremen Verfügbarkeitsanforderungen nur bedingt auf Produktionsanlagen übertragbar (z. B. Virenscanner, tägliches Patchen). IT-Sicherheitskonzepte, wie eine „Defense in Depth"-Strategie, sollten auch in der Produktionsumgebung verwendet werden. Hierbei werden durch mehrstufige Sicherheitskonzepte, zum Beispiel Firewalls und Unterteilung in Zonen, Netzwerksegmentierung, Security by Design und „Need to know"-Prinzipien mehrere Barrieren aufgebaut, um die Produktionsanlagen vor Innen- und Außentätern zu schützen. Die eingesetzten Komponenten der Produktionsanlage müssen mit ihren funktionalen und nicht funktionalen Eigenschaften in das Sicherheitskonzept passen und sollten zusätzlich durch einen Security-Komponententest getestet werden. Die Security einer Produktionsanlage ist aber grundsätzlich nicht allein durch Maßnahmen in den Komponenten realisierbar, sondern muss immer durch eine Kombination von Anlagendesign und organisatorischen Maßnahmen erfolgen.

5.1 Allgemein

Allgemein übertragbar gibt es Mechanismen zum Schutz der Integrität, die für mehrere oder alle Fertigungsschritte wichtig sind. Zu den Security-Standards und Richtlinien für die Produktion, die durch Security-Verantwortliche im Sinne eines Informationssicherheitsmanagementsystems (ISMS)[6] erstellt und gepflegt werden, gehören unter anderem

[4] https://learn.cisecurity.org/benchmarks
[5] https://www.owasp.org/images/6/67/OWASPApplicationSecurityVerificationStandard3.0.pdf
[6] https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/leitfaden-it-security-i40.html

1. Sensibilisierungsmaßnahmen für IT-Sicherheitsrisiken

für die Mitarbeiter in der Produktion, zum Beispiel durch regelmäßige Schulungen

2. Regelungen zum Umgang mit Wechseldatenträgern

(USB-Sticks etc.) und externer Hardware (Programmiergeräte und Diagnosesysteme etc.)

3. Sicherheitsvorkehrungen gegenüber Schadsoftware

in der Produktion bei der Beschaffung neuer Maschinen, Anlagen und während deren Betrieb, zum Beispiel durch Antivirusschutz

4. Notfallkonzepte – „Back-up & Restore"-Fähigkeiten

Eine Katastrophe kann schnell eintreten, zum Beispiel durch Ransomware, die eine Festplattenverschlüsselung vornimmt. Daher sollten für „Katastrophen", die sich auf eine Produktionsumgebung auswirken, geeignete Gegenmaßnahmen und Lösungen ergriffen werden. Einige Beispiele:

- Nächtliche Sicherungen aller Systeme inklusive Mechanismen zur Überprüfung der Integrität und der Wiederherstellungsfunktion
- Backup-Bänder / Festplatten außerhalb des Standorts lagern
- Bereithaltung von Ersatzsystemen für Notfallsituationen
- Authentifizierte Kommunikation – siehe Punkt 5
- Bei unautorisiertem Zugriff sollte nachverfolgt werden, von wo dieser erfolgt ist
- Überwachung/Monitoring der Netzwerkaktivitäten – siehe Punkt 10
- Abschaltung von Kommunikationskanälen bei Bedarf

5. Sicherer Zugriff

Berechtigungen sollten so konfiguriert sein, dass sie nur der jeweiligen Aufgabenstellung entsprechen (Least-Privilege-Prinzip). Zum Beispiel sollte der Zugriff auf Datenbanken im Produktionsumfeld nur Personen möglich sein, die diese Datenbank tatsächlich benötigen. Zum anderen sollte ermittelt werden, ob Leseberechtigungen ausreichen, damit die Daten nicht verändert werden können. Berechtigungen sollten nicht standardmäßig erteilt werden, sondern nur nach Bedarf und Genehmigung. Individuelle Benutzerkonten erlauben die individuelle Zuweisung von Rechten. Eine Begrenzung von Rechten reduziert die Risiken eines Integritätsverlusts.

Wenn Mitarbeiter mit Produktionszugang das Unternehmen verlassen beziehungsweise deren Arbeitsumgebung sich ändert, müssen deren Konten angepasst, deaktiviert oder gesperrt werden. Wenn Administratoren mit Produktionszugriff das Unternehmen verlassen, sollten alle betroffenen Gruppenkonten und Kennwörter, zum Beispiel Root- oder Administratorkennwörter, geändert werden.

6. Netzwerksegmentierung und Zonenkonzept

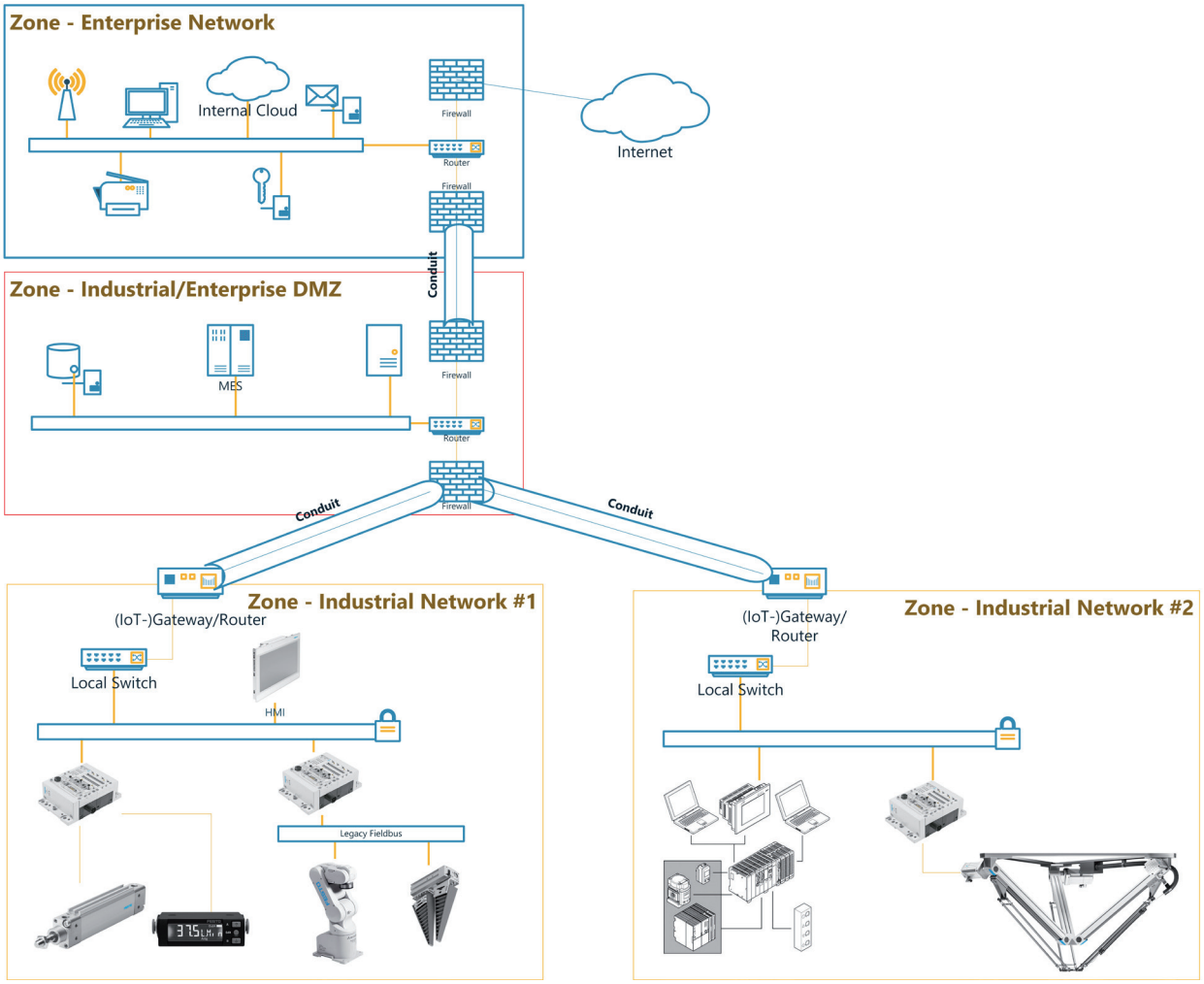
Die Produktionssysteme sollten sich möglichst nicht im selben Netzwerksegment wie andere IT-Systeme befinden. Daher werden diese in ein eigenes dediziertes Subnetz gestellt und der Zugriff und die Verbindung über Firewalls nur den gewünschten Systemen über die erforderlichen Ports ermöglicht. Zudem kann es abhängig vom Sicherheitskonzept (z. B. Altsysteme) sinnvoll sein, Produktionssysteme in weitere Produktionsnetze aufzutrennen. Ein solches Konzept wird auch in der Norm IEC 62443[7] beschrieben (siehe Abbildung 3).

Innerhalb solch einer Fertigungszelle wird die Kommunikation meist über Protokolle stattfinden, die aktuell noch kaum über Sicherheitsmechanismen und Integritätsschutz verfü-

[7] https://www.dke.de/de/themen/cybersecurity/iec-62443

gen und den Fokus auf Safety und Echtzeit legen. Die Verbindung dieser gekapselten Zellen (Zonen) untereinander über die Zellengrenzen hinweg (Conduits) und in übergelagerte Systeme hinaus sollte zur Wahrung der Integrität über gesicherte Protokolle, zum Beispiel TLS oder OPC-UA im Secure Mode, erfolgen.

Abb. 3: Zonenkonzept in Anlehnung an IEC 62443



Quelle: Tobias Pfeiffer, Festo

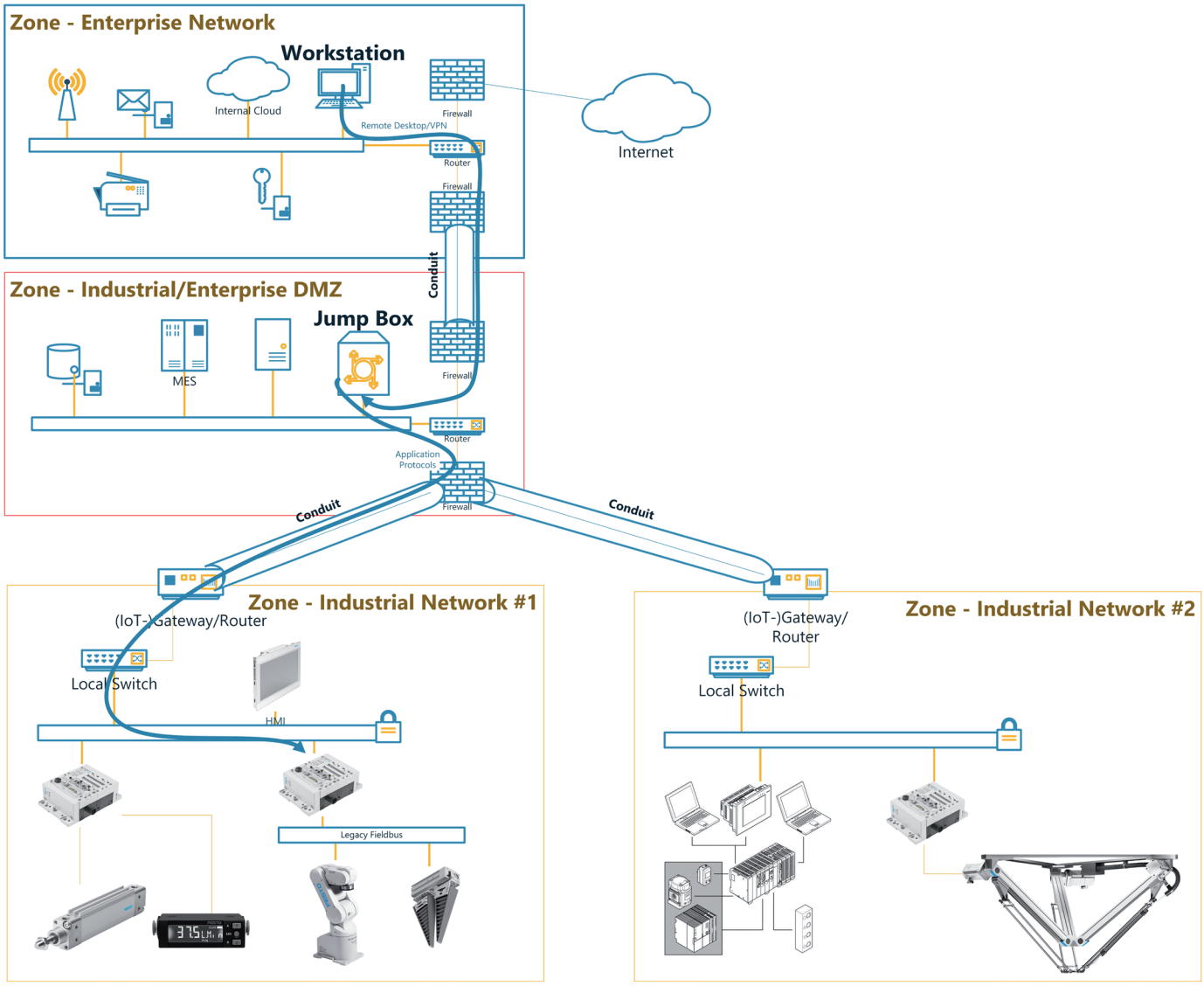
7. Standardisierter Zugang zu Produktionsanlagen und -daten – Fernwartungskonzepte

Es gibt verschiedene Methoden, um auf Produktionsdaten zuzugreifen: über einen Webbrowser, SSH-Konnektivität, Remote-Desktop, sicheres FTP oder verschiedene andere Methoden. Es sollte sichergestellt werden, dass eine im Unternehmen festgelegte Methode zum Zugriff auf die Produktionsanlagen und -daten verwendet wird.

Zum Beispiel einen sicheren kontrollierten Zugangspunkt (siehe „Jump-Box“ in Abbildung 4), zu dem eine Verbindung hergestellt wird und über den dann dediziert durch das Netzwerk auf den freigegebenen Teil der Produktionsanlage geschaltet und nur mittels freigegebener und überprüfter Systeme/Software auf die Produktionsanlage zugegriffen werden kann. Gleichzeitig sollten alle Aktivitäten aufgezeichnet und bei Unstimmigkeiten jederzeit die Verbindung unterbrochen werden können.

Ungewollte Änderungen und Manipulationen können damit verhindert oder nachvollzogen werden.

Abb. 4: Möglichkeiten für Fernzugriffe in Anlehnung an IEC 62443



Quelle: Tobias Pfeiffer, Festo

8. Minimalismus – Security by Default

Produktionssysteme sollten nur notwendige Dienste/Anwendungen enthalten. Dies bedeutet, dass weniger Fehler behoben und gepatcht werden müssen. Die Einfachheit sorgt für eine besser vorhersehbare und verwaltbare Umgebung. Diese Strategie reduziert auch eine potenzielle Angriffsoberfläche. Eingesetzte Komponenten sollten daher nach dem „Security by Default"-Prinzip in einem gehärteten Zustand verwendet werden, zum Beispiel ein Webserver sollte nur einen Webserverdienst in sichererer, gehärteter Konfiguration ausführen und keine weiteren Dienste bereitstellen, da dies die Angriffsfläche erhöht. Zudem sollten nicht erforderliche Anwendungen oder Dienste entfernt werden.

9. Patch-Strategie

Es sollte eine Patch-Strategie definiert und umgesetzt werden, die sicherstellt, dass auf Basis regelmäßiger Überprüfung auf neue Sicherheitsupdates der eingesetzten Soft- und Firmware diese bewertet und entsprechend eingeplant werden. Dabei ist darauf zu achten, dass die neuen Sicherheitsupdates die Funktionalität des bestehenden Produktionssystems nicht gefährden und die Anpassung der Bedrohung angemessen ist. Durch das Einspielen

von Patches werden die Prozesse in einer Anlage gegebenenfalls kurzzeitig unterbrochen, was zu einer Beeinträchtigung des Schutzziels Verfügbarkeit führen und durch den Einsatz von Clustern minimiert werden kann. Sofern eine temporäre Reduktion der Verfügbarkeit akzeptabel ist, kann, abhängig von der Anwendung, auch erst ein Teil des Clusters aktualisiert werden, um entsprechende Tests durchzuführen. Idealerweise stehen hierfür jedoch entsprechende Testsysteme zur Verfügung. Auch die Integrität der Produktionssysteme muss gewahrt bleiben, was zu einem integren Produktionsprozess und damit Produkt führt.

10. Überwachung, Protokollierung und Alarmierung

Viele der oben genannten Schritte werden weniger effektiv oder bedeutungslos, wenn keine Überwachung, Protokollierung und Alarmierung verwendet wird. Jede in einem Produktionssystem durchgeführte Aktion, welche die Safety oder Security betrifft, sollte aufgezeichnet werden und, je nach Schweregrad, gegebenenfalls eine Warnmeldung auslösen. Wenn man sich als Administrator anmeldet, sollte beispielsweise eine Benachrichtigung an das IT-Personal und/oder die Sicherheitsgruppe gesendet werden, damit diese beurteilen können, was passiert und ob eine unautorisierte Handlung vorliegt.

Weiter ist der Einsatz von Intrusion-Detection- und -Prevention-Systemen (IDS/IPS), die in der IT üblich sind, in den Enterprise Networks und DMZs sinnvoll. Innerhalb einer Fertigungszelle sind Intrusion-Detection- und/oder -Prevention-Systeme jedoch schwer einzusetzen. Zum einen gibt es meist solche Systeme für (proprietäre) Feldbusse kaum. Zum anderen arbeiten die meisten Feldbusprotokolle derart, dass kein neuer Teilnehmer ohne eine Änderung der kompletten Anlagenkonfiguration eingefügt werden kann. Dennoch sollte auch regelmäßig, zum Beispiel im Rahmen einer Wartung, das Netz einer Zelle nach neuen Teilnehmern, geöffneten Ports und Netzwerkschnittstellen gescannt und eventuell gefundene Auffälligkeiten untersucht werden.

11. Public-Key-Infrastruktur (PKI) in der Produktion

Eine Möglichkeit zur Sicherstellung der Integrität von Produktionssystemen und -parametern und damit auch den zu produzierenden Produkten ist die Nutzung von digitalen Zertifikaten. In der Regel kommen hierfür digitale Zertifikate im X509v3-Format zum Einsatz. Die Ausstellung dieser Zertifikate erfordert eine Public-Key-Infrastruktur und die zugehörigen Systeme und Prozesse, die eine entsprechende Certificate-Authority-Struktur (CA-Struktur) und die damit verbundenen Dienste abbilden.

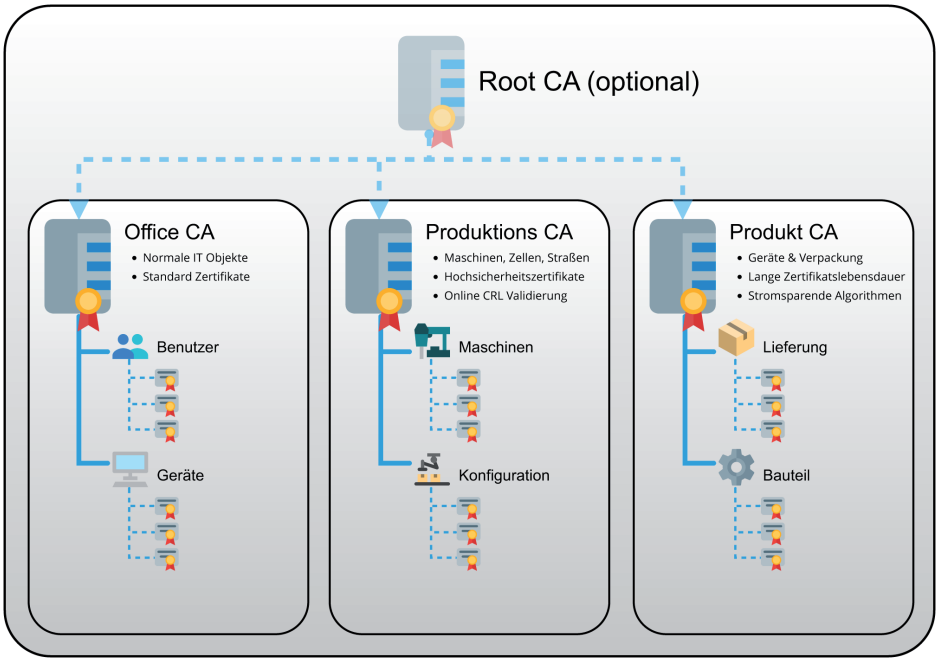
Eine mögliche CA-Struktur ist in Abbildung 5 dargestellt. Diese zeigt eine Unterteilung in verschiedene CAs. Abhängig vom CA-Design nutzen die CAs eine eigene oder eine gemeinsame Root-CA. Die Root-CA sollte dabei, egal ob in einfacher oder mehrfacher Ausführung, als Offline-Root-CA ausgelegt werden.

Die unten aufgeführte exemplarische Trennung in die Bereiche „Office/Enterprise", „interne Produktion" und „Produkte" ist auf unterschiedliche Anforderungen der jeweiligen Anwendungsfälle in Bezug auf Parameter wie Zertifikatslaufzeit, Verfügbarkeit, Schlüsselalgorithmen und -längen, Validierungsdienste und Zertifikatsrückruf, Zertifikatserneuerung, Verwendungszwecke usw. zurückzuführen

- Die Office-CA bildet dabei eher klassische Anwendungsfälle wie zum Beispiel Benutzer-, Computerzertifikate ab.
- Die Produktions-CA stellt Identitätszertifikate aus, die für die Kommunikation zwischen Maschinen, Zellen und Linien genutzt werden können. Protokolle wie TLS helfen hier bei der Erreichung der Schutzziele Integrität und Vertraulichkeit auf der Transportschicht.

- Des Weiteren könnte die Produktions-CA Zertifikate zur Erstellung digitaler Signaturen erzeugen. Diese können zum Beispiel zur Signatur von Fertigungsaufträgen oder Prüfprogrammen verwendet werden, um die Integrität der Produktionsparameter und Aufträge zu belegen.
- Die Produkt-CA stellt zum Beispiel Identitätszertifikate für die Produkte aus, aber auch Zertifikate für die Erstellung digitaler Signaturen für Firm- oder Software, die durch die entsprechenden Entwicklungsbereiche im Rahmen des Releaseprozesses für die Signatur von Firm- und Software genutzt werden und eine Verifikation der Integrität und Vertraulichkeit durch Produktion und Produkt ermöglichen sowie die Urheberschaft regeln.

Abb. 5: Beispielhafte Public-Key-Infrastruktur mit drei Certificate Authorities (CA) innerhalb eines Industrieunternehmens



Quelle: Udo Schneider, Trend Micro Deutschland

5.2 Produktion: Auftragsbearbeitung und Produktionsvorbereitung

Der Fertigungsauftrag aus dem ERP-System ist die Grundlage für die auftragsbezogene Produktion und damit ein sehr wichtiger zu schützender Bestandteil. Der Input für das ERP-System kommt in der Regel nicht von dem Fertigungsunternehmen selbst, sondern wird von externen Auftraggebern und Kunden übergeben beziehungsweise in das Unternehmensnetzwerk oder Portal eingespielt. Da der Auftrag sozusagen von außen kommt, sind mehrere Punkte zu betrachten:

- Gültigkeit der Daten, auf deren Basis der Fertigungsauftrag erstellt wird (z. B. ERP/MES/MOMS)
- Inhaltliche Validierung des Auftrags
- Sicherung der Übertragung des Auftrags in die Produktion
- Verifizierung der Gültigkeit des Auftrags

Insbesondere wenn der Fertigungsauftrag nicht nur Metadaten (Produktart, Seriennummer, Kunde …), sondern auch Produktionsanweisungen enthält, ist die Sicherstellung der Inte-

grität auf dem Transportweg entscheidend. Das betrifft zum Beispiel Bestückungsanweisungen (EU- vs. US-Netzteil), Zertifikate, Konfigurationseinstellungen oder Ähnliches. Darüber hinaus ist auch die Authentizität, zum Beispiel über digitale Signaturen, nachzuweisen.

Die Quelldaten werden gültig und valide durch ein ERP/MES/MOMS der Produktion zur Verfügung gestellt. Zum Erkennen von Veränderungen und der Gültigkeit des Fertigungsauftrags können digitale Signaturen eingesetzt werden.

Aufträge der Produktion werden digital signiert übertragen. Die Integritätsprüfung dieser Produktionsaufträge könnte durch Hash-Werte erfolgen. Um jedoch den Nachweis der Urheberschaft eindeutig zu validieren, sind digitale Signaturen notwendig, da diese den Nachweis der Authentizität erlauben.

Die Bereitstellung der zur Bestückung erforderlichen Elemente umfasst in der Regel den Wareneingang (externe Zulieferung) beziehungsweise die Zulieferung von Elementen aus internen Quellen. Dabei gilt es sicherzustellen, dass die richtigen Elemente bereitgestellt werden.

Bereitstellung benötigter Elemente

Fehlende Elemente können aufgrund von Liefer- oder Lagerengpässen entstehen. Dabei stellen diese an sich keine Verletzung der Integrität dar, jedoch können resultierende Gegenmaßnahmen zu einer Verletzung führen. Ein Beispiel ist die Beschaffung von fehlenden Bauteilen aus Kanälen, die eventuell falsche oder nicht funktionsgleiche Bauteile liefern.

Falsche Elemente (abweichende Bauform oder Funktion)

Neben fehlenden Elementen sind eindeutig falsche Elemente am einfachsten festzustellen. Dies kann zum Beispiel bei der Wareneingangsprüfung optisch oder anhand von Lieferinformationen festgestellt werden. Beispiele sind verschiedene Bauformen (z. B. DIP vs. SMD), Betriebsspannungen (z. B. TTL vs. CMOS) oder Einsatzgebiete (Max.-/Min.-Temperatur).

Defekte Elemente

Auch aus vertrauenswürdigen Kanälen können Elemente mit Defekten geliefert werden. Hier gilt es, mit geeigneten Maßnahmen die zu erwartende Funktionalität zu prüfen. Beispielhaft sei hier eine qualitative Messung im analogen und ein Funktionstest im digitalen Segment genannt.

Gefälschte Elemente

Vorsätzlich gefälschte Elemente können in jede der oben genannten Kategorien fallen. Dementsprechend ist deren Erkennung und Vermeidung mit entsprechenden Überprüfungsmechanismen durchzuführen.

Integritätsprüfung von Fertigungselementen

Das Prüfen der Integrität von Elementen kann eine große Herausforderung darstellen. Hier empfiehlt es sich, Komponenten von bekannten und vertrauenswürdigen Lieferanten zu beziehen. Bei Wareneingang ist die Verpackung und Etikettierung auf Beschädigung oder Manipulation zu prüfen. Die Lieferung sollte identifizierbar und nachvollziehbar sein. Die Bauteile sind nicht nur einer optischen Prüfung auf Manipulation zu unterziehen. Vielmehr sollte die Integrität dieser Elemente mit weiteren geeigneten Maßnahmen überprüft werden.

5.3 Produktion: Firmware-Installation

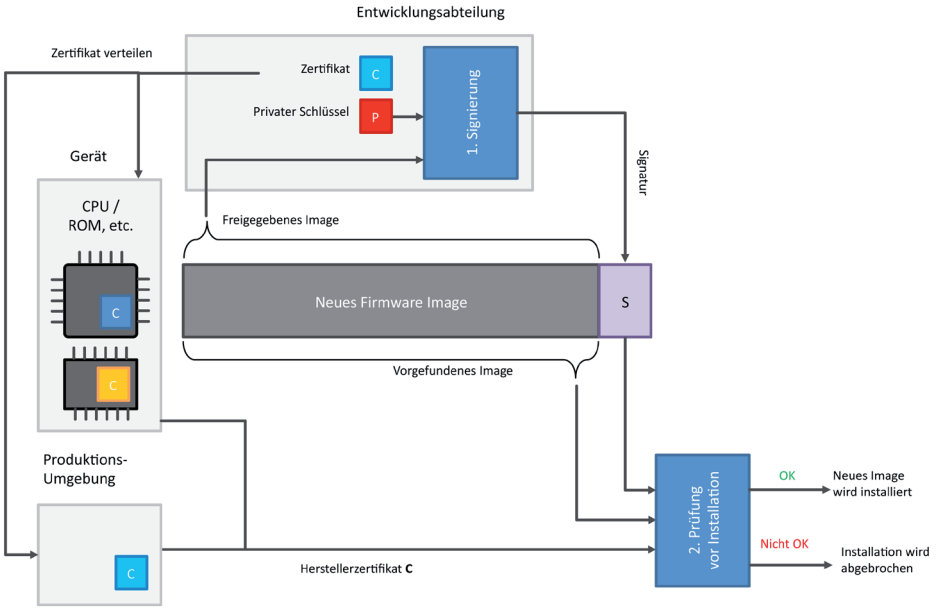
Grundsatz:
Die Integrität der Software oder Firmware eines Geräts ist für den späteren sicheren Betrieb unerlässlich. Da spätere Integritätssicherungsmaßnahmen nur greifen können, wenn zuerst ein vertrauenswürdiger und integrer Zustand hergestellt wird, ist die Erstinstallation der Gerätesoftware ein kritischer Schritt bei der Sicherung der Integrität des Produkts.

Während der Installation der Software muss zum einen die Integrität der zu installierenden Software sichergestellt werden. Dies geschieht in der Regel durch die Validierung einer Signatur über die zu installierende Software. Zum anderen müssen die Voraussetzungen für die spätere Integritätsprüfung des Geräts beim Gerätestart und im Gerätebetrieb geschaffen werden. Dies basiert auf zwei Schritten: erstens auf dem Setzen eines Vertrauensankers in der Produktionsphase; zweitens durch die spätere Prüfung der Software gegenüber diesem Vertrauensanker während des Gerätestarts (Boot Prozess). Des Weiteren wird während der Produktion des Geräts oftmals eine eindeutige sichere Systemidentität erzeugt. Diese kann später im Betrieb zur eindeutigen Identifikation des Geräts und seiner Herkunft genutzt werden. Auf alle drei Phasen und deren Vorbedingungen wird im Folgenden eingegangen.

5.3.1 Prüfung der Integrität der neuen Gerätesoftware vor dem Aufspielen

Wenn eine neue Gerätesoftware durch die Entwicklungsabteilung zur Verfügung gestellt wird, muss diese während des Produktionsprozesses auf das zu produzierende Gerät aufgespielt werden. Aus Sicht der Geräteintegrität ist es jedoch möglich, dass ein Angreifer die Gerätesoftware bei der Übergabe an die Produktionsstätte verändert oder die am Produktionsort lagernde Gerätesoftware manipuliert beziehungsweise durch eine veränderte Gerätesoftware ersetzt. Daher ist es notwendig, die Gerätesoftware vor dem Aufspielen auf das neue Gerät hinsichtlich ihrer Integrität zu prüfen. Diese Prüfung kann entweder durch das Produktionssystem oder durch das neue Gerät selbst geschehen. Abbildung 6 zeigt beide Varianten.

Abb. 6: Prüfung der Integrität des Firmware-Images vor der Installation durch das Produktionssystem oder das Gerät selbst



Quelle: Prof. Tobias Heer, Hirschmann Automation and Control

Im Produktionssystem kann ein digitales Herstellerzertifikat C (Certificate) hinterlegt werden, auf dessen privaten Schlüssel die Produktionsstätte keinen Zugriff hat. Durch den öffentlichen Schlüssel sowie die hinterlegte Zertifikatskette kann die Produktionsstätte beziehungsweise das Produktionssystem die Integrität und Authentizität der neuen Gerätesoftware direkt vor dem Aufspielen prüfen, insofern die Software mit dem Herstellerzertifikat in der Entwicklungsabteilung signiert wurde. So kann sichergestellt werden, dass die Gerätesoftware nicht während der Lagerung oder während der Übertragung verändert wurde.

Eine wichtige Voraussetzung für eine aussagekräftige Prüfung ist die Integrität des Prüfsystems und die Vertraulichkeit des geheimen Schlüssels für das Zertifikat C. Nur wenn das prüfende System selbst nicht manipuliert wurde, kann sichergestellt werden, dass auch die produzierten Geräte die korrekte Software enthalten. Daher ist es unabdingbar, dass alle vertretbaren Maßnahmen der IT-Sicherheit (z. B. aktuelle Geräte- und Anwendungssoftware, sichere Passwörter, Benutzerauthentifizierung, Netzwerksegmentierung, Ereignisdatenüberwachung etc.) zum Schutz des Produktionssystems getroffen werden. Ebenso muss der Zugriff auf den privaten Schlüssel des Herstellerzertifikats C geschützt werden, da ansonsten eine manipulierte Gerätesoftware damit signiert und dies nicht vor dem Aufspielen und Betrieb der Software festgestellt werden könnte. Der Zugriff auf den privaten Schlüssel muss durch technische und organisatorische Maßnahmen so eingeschränkt werden, dass nur prozessgemäß freigegebene Gerätesoftware damit signiert werden kann.

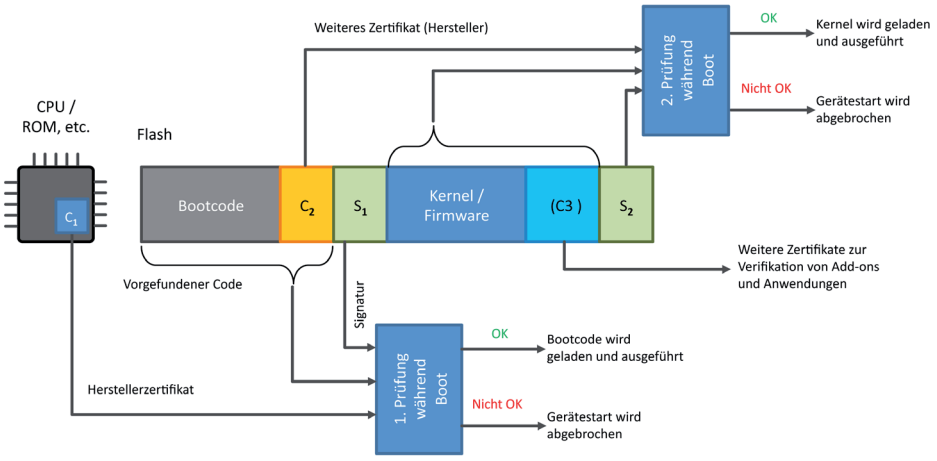
Auch das Gerät selbst kann die Integrität der aufzuspielenden Software prüfen. Dazu muss jedoch in einem vorbereitenden Schritt das Herstellerzertifikat C im Gerät hinterlegt werden. Auch das zu hinterlegende Herstellerzertifikat muss geprüft werden. In der Regel wird dieses Zertifikat (oder Hashs des Zertifikats) in einem speziell geschützten Speicherbereich hinterlegt, sodass ein Angreifer dieses Zertifikat nach dem ersten Aufspielen nicht mehr oder nicht einfach verändern kann. Während dieses vorbereitenden Schritts muss sichergestellt werden, dass das Zertifikat beziehungsweise die Hashs tatsächlich dem Herstellerzertifikat entsprechen. Auch dies bedingt ein integres Produktionssystem, das nach dem Stand der Technik vor Veränderungen geschützt wird. Nach dem initialen Setzen des Herstellerzertifikats auf dem Gerät kann nun das Gerät die Firmware anhand der angehängten Signatur prüfen und eigenständig die Installation einer fehlerhaft signierten, also nicht integren, Gerätesoftware verweigern.

5.3.2 Prüfung der Integrität der installierten Gerätesoftware während des Systemstarts

Falls auch Manipulationen am Gerät nach der Auslieferung durch Maßnahmen wie zum Beispiel Secure-Boot erkannt werden sollen, so muss dies während des Produktionsprozesses vorbereitet werden. Secure-Boot ist eine Technik, bei der sämtliche Teile der Gerätesoftware durch digitale Signaturen vor Veränderungen geschützt werden. Sollte eine unautorisierte Änderung an der Gerätesoftware erkannt werden, so bricht das Gerät den Startvorgang ab. Bei einem Gerät, das ordnungsgemäß startet, kann also angenommen werden, dass die geladene Software der tatsächlich durch den Hersteller freigegebenen Software entspricht. Abbildung 7 zeigt den schematischen Ablauf des sicheren Boot-Prozesses. Im Gerät wurde bereits ein Zertifikat C1 in einem speziell gesicherten Speicherbereich hinterlegt. Dieser Speicherbereich ist hardwaretechnisch so geschützt, dass ein Angreifer ihn selbst dann nicht verändern kann, wenn er physischen Zugriff zum Gerät und seinen Schaltkreisen erlangt. Mithilfe dieses Herstellerzertifikats (Root of Trust) kann das Gerät den initialen Bootcode verifizieren, bevor er ausgeführt wird. Nur wenn die Signatur S1 des Bootcodes

mit dem Herstellerzertifikat C1 verifiziert werden kann, ist das Gerät bereit, den Bootcode auszuführen. Ansonsten bricht das Gerät den Boot-Vorgang ab. Der Bootcode kann weitere Zertifikate C2 enthalten, die zum Beispiel mit einem Firmware-Update einfacher austauschbar sind als die fest gespeicherten Herstellerzertifikate C1. Bevor der verifizierte und nachweislich integre Bootcode das eigentliche Betriebssystem des Geräts lädt, überprüft der Bootcode die Signatur des Betriebssystems mit dem Herstellerzertifikat C1 oder C2. Erneut wird der Startprozess des Geräts abgebrochen, falls die Software des Geräts keine gültige Signatur S2 aufweist. Das Betriebssystem C3 kann wiederum weitere Zertifikate enthalten, mit denen später zu ladende Software-Erweiterungen oder -Anwendungen verifiziert werden können. Die hier beschriebene und in Abbildung 7 dargestellte Abfolge stellt nur einen einfachen sicheren Boot-Vorgang exemplarisch dar. Andere Mechanismen und der Einsatz von weiteren Hardware-Einheiten, wie zum Beispiel einem Trusted Platform Module (TPM), sind ebenso möglich.

Abbildung 7: Prüfung der Integrität der auf dem Gerät aufgespielten Firmware/Software beim Systemstart durch das Gerät



Quelle: Prof. Tobias Heer, Hirschmann Automation and Control GmbH

Um den oben beschriebenen sicheren Boot-Prozess durchführen zu können, müssen die Voraussetzungen dafür in der Entwicklung der Gerätesoftware und der Geräteproduktion geschaffen werden. Zum einen müssen die Herstellerzertifikate C1 im Gerät hinterlegt werden. Zum anderen müssen freigegebene Bootcodes sowie Betriebssystemversionen (meist durch die Entwicklungsabteilung) digital signiert werden, bevor sie in die Produktion übergeben werden oder den Kunden per Download zur Verfügung gestellt werden. Sowohl das Aufspielen der Herstellerzertifikate als auch die Signierung der Bootloader- und Firmware-Teile müssen in einer sicheren Umgebung stattfinden, da während dieser Phasen sonst eine unbemerkte Veränderung der Software möglich ist. Auch hier sind die Grundregeln für den sicheren Betrieb aller beteiligten Geräte zu beachten.

5.3.3 Erzeugung einer sicheren Systemidentität für die Verwendung im Betrieb

Für die Integrität eines Gesamtsystems aus kommunizierenden Einzelsystemen ist die Feststellung der Identitäten der Einzelsysteme von großer Bedeutung. In der Vergangenheit gab es wiederholt Sicherheitsprobleme[8], da Geräte keine oder keine eindeutige Identität

[8] https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final228.pdf

besaßen. So sind Fälle bekannt, in denen alle Geräte eines Herstellers ein fest in der Firmware codiertes Zertifikat und den ebenfalls fest in der Firmware hinterlegten Private-Key zur Authentifizierung verwendeten. In solch einem Fall kann ein Angreifer die Identität eines einzelnen Geräts auslesen (z. B. über direkten physischen Zugriff auf die Speicherchips eines Geräts oder über eine Analyse beziehungsweise ein Reverse-Engineering einer Firmware-Datei) und die Kommunikation abhören oder fälschen.

Um solchen Angriffen vorzubeugen, ist die Generierung einer gerätespezifischen sicheren Identität unabdingbar. Eine solche sichere Identität besteht in der Regel aus einem asymmetrischen Schlüsselpaar sowie einem damit oder darüber erzeugten digitalen Zertifikat. Dieses Schlüsselpaar kann entweder beim ersten Start des Geräts durch das Gerät selbst generiert werden oder es kann durch das Produktionssystem generiert und an das Gerät übertragen werden. Beide Alternativen bieten Vor- und Nachteile:

Bei der Erzeugung eines Schlüssels durch das Gerät selbst muss sichergestellt werden, dass genug Entropie vorhanden ist, um hinreichend unvorhersehbare Zufallszahlen für die Generierung des asymmetrischen Schlüsselpaars gewinnen zu können. Die Entropie ist ein Maß für die Zufälligkeit von Quellen, aus denen der geräteeigene Zufallsgenerator sichere Zufallswerte erzeugen kann. Zur Steigerung der Entropie verwenden Computersysteme nicht vorhersagbare Eingaben wie Zeiten von zufällig auftretenden Ereignissen, Benutzerinteraktionen oder thermisches Rauschen von Funkschnittstellen. Manche Geräte haben sogar die Möglichkeit, zufällige Werte durch spezielle Hardwarekomponenten erzeugen zu lassen, um sie als zufällige Eingaben für den Zufallsgenerator des Systems zu verwenden. Entsprechende Zufallsquellen werden zum Beispiel von Secure-Elements wie TPMs bereitgestellt oder können direkt in Prozessoren integriert sein. Bei einer zu geringen Zufälligkeit von Zufallszahlen, also bei einer zu geringen Entropie der Quellen des Zufallszahlengenerators, werden die mithilfe dieser Zufallszahlen erzeugten asymmetrischen Schlüsselpaare vorhersagbar und Angreifer können die privaten Schlüssel effizienter errechnen. Gerade beim identischen Start von neuen Geräten unter identischen Produktionsbedingungen können gegebenenfalls nicht genügend unterschiedliche Umgebungswerte gewonnen werden, um eine hinreichende Unvorhersehbarkeit zu erreichen. Daher muss dieser Punkt hinreichend berücksichtigt und untersucht werden, wenn die sicheren Identitäten durch die Geräte selbst im Produktionsprozess erzeugt werden sollen. Ein Vorteil bei der Generierung der Identitäten auf dem Gerät selbst ist jedoch, dass der private Schlüssel des Schlüsselpaars das Gerät niemals verlässt und daher auch selbst bei einem kompromittierten Produktionssystem nicht von einem Angreifer gelernt werden kann.

Die Vorteile und Nachteile der Schlüsselgenerierung auf dem Gerät stehen in einem Spannungsverhältnis zu den Vorteilen und Nachteilen der Schlüsselgenerierung auf der Produktionsumgebung. Die Verwendung sicherer Quellen von Zufallszahlen, etwa in Prozessoren oder Secure-Elements, sollte hier keine finanzielle Hürde darstellen. Jedoch sind die privaten Schlüssel auch der Produktionsumgebung bekannt (da es diese ja erzeugt hat), was einem Angreifer mit Zugriff auf die Produktionsumgebung das Aushorchen der privaten Schlüssel erlaubt.

Welche Art der Schlüsselerzeugung vorzuziehen ist, lässt sich nicht pauschal beantworten und bedarf einer Einzelfallbetrachtung. Jedoch ist es zwingend notwendig, dass sich Hersteller von Geräten mit sicheren Identitäten mit den oben beschriebenen Problemstellungen befassen.

5.4 Produktion: Endfunktionstest

Nachdem die Firmware installiert wurde, sollte das Produkt gemäß der in der Designphase erstellten Prüf- und Testszenarien getestet werden. Dazu sollten die schon mehrfach beschriebenen Standardmaßnahmen zur Sicherstellung der Integrität für Prüfdokumente und der Test- und Produktionsgeräte berücksichtigt werden, um die Integrität und die Funktion des Endprodukts sicherzustellen. Während bis zu diesem Schritt die meisten Komponenten getrennt/autark verifiziert wurden, wird im Funktionstest des Endprodukts die übergreifende Integrität geprüft beziehungsweise sichergestellt.

Hierbei sind automatische und teilautomatisierte Tests vorzuziehen, weil dadurch die Daten automatisch gespeichert und weitergeleitet werden können. Manuelle Prüfungen sind durch organisatorische Anweisungen, wie zum Beispiel die Nutzung eines automatischen Logbuchs mit signierten Einträgen, vorzusehen. Die Dokumentation der Tests kann auch durch Foto- und Videoaufzeichnungen unterstützt werden.

5.5 Produktion: Konfiguration Endprodukt

Nachdem sichergestellt ist, dass das Endprodukt korrekt funktioniert, kann nun das Produkt in den Auslieferungszustand versetzt werden. Hierzu werden alle zu Testzwecken auf das Endprodukt geladenen Daten und Programme sicher gelöscht, eventuell angelegte Nutzeraccounts zurückgesetzt, Systemdienste, bis auf die Inbetriebnahmeschnittstellen, deaktiviert usw. sowie die Werkseinstellungen appliziert. Die notwendigen Mechanismen für diese Systembereinigung wurden im Rahmen des Security by Designs bereits während der Entwicklungsphase geplant, um sicherzustellen, dass die Auslieferung nach dem Konzept Security by Default erfolgt.

Werden im Rahmen einer individuellen Produktion bereits Daten des Kunden übernommen beziehungsweise sind diese bereits installiert/konfiguriert, sind die Schutzziele Integrität der Kundenparametrierung und Vertraulichkeit der Parametrierung zu betrachten.

Die Integrität der Parametrierung ist sicherzustellen, damit dem Kunden das Gerät im gewünschten Zustand ausgeliefert wird. Dies betrifft insbesondere die Security-Konfiguration, da der Kunde sich darauf verlässt, dass keine ungeplanten Zugänge zum System aktiviert sind, die als Backdoor benutzt werden könnten. Eine effektive Überprüfung könnte durch Prüfsummen ermöglicht werden, die nach Auslieferung über die Parametrierung erstellt und vom Kunden abgefragt und verglichen werden können.

Enthält die Kundenparametrierung vertrauliche Informationen, sollte sie, je nach Schutzbedarf, auf einem sicheren System abgelegt und mithilfe einer sicheren Kommunikationsverbindung übertragen werden. Dabei ist die Echtheit des Endprodukts zum Schutz der Information nachzuweisen, was über die vorher ausgestellte sichere Identität des Endprodukts erfolgen kann.

5.6 Produktion: Verpackung

Um die Integrität des Produkts nach der Konfiguration des Endprodukts sicherzustellen, sollte es direkt verpackt und beschriftet werden und durch Maßnahmen, wie zum Beispiel ein Siegel oder andere, vor Manipulation geschützt werden. Dadurch wird die Integrität während der Lagerung und des Versands, die ein inhärenter Bestandteil der Integrität der Lieferkette sind, sichergestellt. Dabei gilt es, unter Umständen auch ein Szenario der Auslagerung, des Updates, der Verpackung und der Wiedereinlagerung zu berücksichtigen.

Bei einem Update sollten zur Sicherstellung der Integrität die Beschriftung und das Siegel geprüft und das Update unter Berücksichtigung der Punkte Firmware, Installation bis zur Verpackung durchgeführt werden. Dabei müssen Siegel und Beschriftung erneuert/upgedatet werden.

6 Ausblick und Umsetzung

Das Whitepaper macht deutlich, dass der Schutz der Integrität, insbesondere in der Produktion, elementare Bedeutung für digitale und vernetzte Geschäftsprozesse hat. Industrieunternehmen sollten dies in ihre Zukunftsstrategie und das Risikomanagement integrieren. Denn die gesetzlichen Anforderungen an die Integrität von Daten steigen in Deutschland und Europa.[9] Schrittweise sollten Maßnahmen zur Gewährleistung der Integrität im Unternehmen sowie in der gesamten Supply-Chain umgesetzt werden.

Diese Maßnahmen entstehen dabei nicht im luftleeren Raum. Das Produktmanagement und die Produktentwicklung stellen die Anforderungen, aus denen sich die Maßnahmen ableiten. Dem Verantwortlichen für die Produktion obliegt es, sicherzustellen, dass diese Maßnahmen umgesetzt werden. Sicherlich sind hierin mehrere Rollen und Unternehmenseinheiten involviert.

Eine gute Orientierung bietet die beschriebene IEC 62443, die Anforderungen für eine übergreifende IT- und Cybersicherheit formuliert. Diese lässt sich nicht ohne Integritätsschutz in Entwicklung, Produktion, Integration und Betrieb herstellen. Die Beschäftigung mit der Norm und den hier skizzierten Orientierungshilfen unterstützen Unternehmen dabei, Cybersicherheit als (selbstverständlichen) Bestandteil ihrer Prozess- und Produktqualität für sich und ihre Kunden umzusetzen.

[9] https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_de

ZVEI:
Die Elektroindustrie

ZVEI - Zentralverband Elektrotechnik-
und Elektronikindustrie e.V.
Lyoner Straße 9
60528 Frankfurt am Main

Telefon: +49 69 6302-0
Fax: +49 69 6302-317
E-Mail: zvei@zvei.org
www.zvei.org

Bildnachweis Titelseite: ZVEI