Positionspapier

CYBER-SICHERHEITS-CHECK IN INDUSTRIELLEN ANLAGEN

ISACA
Trust in, and value from, information systems
Germany Chapter

Einführung / Präambel / Motivation

Das 21. Jahrhundert steht im Zeichen der Digitalisierung. Die erste Generation der *Digital Natives* steht im Berufsleben: die Personen, die im Umgang mit digitalen Medien aufgewachsen sind und nicht erst als Erwachsene mit der Informationstechnologie in Berührung kamen. Vor allem die Arbeitswelt erfährt dadurch einen enormen Wandel. Die Digitalisierung der gesamten Wertschöpfungskette verändert nicht nur Produkte und deren Fertigung, sondern auch ganze Geschäftsmodelle. Deshalb spricht man bereits von der 4. industriellen Revolution, die durch den Begriff »Industrie 4.0« geprägt ist. Speziell die Produktionsumgebung wird zunehmend digitaler und intelligenter. So werden vor allem Automatisierung, Mobilität, Flexibilität sowie Individualität forciert.

Die Nutzung von eingebetteten Systemen, Industrie-PCs und industrieller Netzwerktechnik zur Steuerung von Produktionsanlagen und -straßen ist nicht neu und seit Jahren fester Bestandteil der betrieblichen Aktivitäten in den Unternehmen. Im Produktionsumfeld hat sich entsprechend der Begriff *Operational Technology* (OT) etabliert, wenn von Betriebstechnik die Rede ist, die zur Steuerung, Kontrolle und Überwachung von Geräten, Prozessen und Events verwendet wird.

Neu ist, dass aus industriellen Anlagen, Maschinen und Sensoren mittels vernetzter Kommunikation und Datenwolken im Internet nun sogenannte »smarte Maschinen« oder »Cyber-physische Systeme« werden, die somit Bestandteil des »Internets der Dinge« (IoT) sind. Ein wesentlicher Aspekt ist die hieraus gewachsene Verbindung zur klassischen *Informationstechnik* (IT) in der Unternehmensorganisation und -verwaltung und zu den dort integrierten Geschäftsprozessen. Daten aus Verkaufsgesprächen durchlaufen nach Eingabe verschiedenste Schritte von Einkauf über Produktionsplanung und -steuerung bis zur logistischen Auslieferung an den Kunden – CRM-, ERP- oder MFS-Systeme.

Auf Seiten der OT können heute – dank direkter Internetanbindung – industrielle Anlagen bei Bedarf ganz oder teilweise via Smartphone aus der Ferne vom Management abgefragt und gesteuert werden. Eine intelligente Überwachung von Verschleißteilen einer Maschine löst bei Bedarf eine automatische Bestellung beim Hersteller aus – Condition-Based Monitoring. Kundenbestellungen werden bei Bedarf automatisch individuell hergestellt und ausgeliefert. Schon heute ist es Alltag, dass Dienstleister Maschinen in der Produktion via Internet fernwarten – Predictive Analytics & Maintenance.

Doch mit den Chancen, die sich durch die zunehmende Vernetzung und Verschmelzung von Produktion und IT ergeben, wachsen auch die Risiken. Historisch bedingt spielte das Thema Cyber-Sicherheit im Produktionsbereich nur eine untergeordnete Rolle und Produktionsnetze weisen bisher nur ein geringes Schutzniveau auf. Denn in den vergangenen Jahren lag der Fokus lediglich auf Verfügbarkeit und Betriebssicherheit (Safety). Mit dem steigenden Grad der Digitalisierung und Vernetzung werden zunehmend analoge Bussysteme durch digitale Kommunikationsschnittstellen ersetzt, die auf Internettechnologie basieren. Der Vorteil ist, dass die Kommunikation deutlich einfacher und transparenter wird, aber auf der anderen Seite steigt das potenzielle Risiko von Cyberangriffen.

Unter Digitalisierung ist in diesem Zusammenhang der Sachverhalt zu verstehen, Dinge im Cyberspace adressierbar, sichtbar und dadurch nutzbar zu machen. Vergleichbar mit der realen Welt muss hierbei auch in der digitalen Welt Vertrauen durch Cyber-Sicherheit geschaffen werden. Cyber-Sicherheit ist somit die Basis, damit die Digitalisierung überhaupt gelingen kann. Die aktuellen Angriffe durch *WannaCry* und *NotPetya* zeigten, wie drastisch die Auswirkungen auf die gesamte Wertschöpfungskette sein können, wenn Cyber-Security-Maßnahmen nicht berücksichtigt werden. Insbesondere, wenn kritische Infrastrukturen und somit überlebenswichtige Bereiche betroffen sind.

Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) hängen heute die meisten Geschäftsprozesse von verlässlicher und fehlerfreier IT ab. Viele Unternehmen, vor allem kleine und mittelständische Unternehmen, sind sich aber der Gefahren nicht bewusst. Enorme wirtschaftliche Schäden durch Produktionsausfälle, Imageverlust, Daten- bzw. Ideenklau, Datenschutzverstöße und Rechtsfolgen sind nur einige der Auswirkungen, die Unternehmen treffen können. Hauptgrund dafür ist eine digitale Sorglosigkeit, die sich in mangelndem Sicherheitsbewusstsein, fehlender Sicherheitsexpertise und nur rudimentärer Kenntnisse der eingesetzten Produkte widerspiegelt.

Es gilt nun eine Brücke zwischen IT und OT zu bauen, die die technischen sowie die organisatorischen Maßnahmen in der OT berücksichtigt. Dies ist nur zu schaffen, wenn hierbei IT- und OT-Verantwortliche zusammenarbeiten. Die Einführung klassischer Sicherheitsmaßnahmen und -prozesse aus der Office-IT können nicht einfach übernommen werden, da die Voraussetzungen oft andere sind. In der Regel werden in der Produktion Maschinen angeschafft, die über viele Jahrzehnte ohne jegliches Aktualisieren der Software betrieben werden und deshalb gravierende Sicherheitslücken enthalten können.

Der grundlegende interne Produktionsprozess steht hier im Vordergrund und nicht die möglichen Einwirkungen auf Serviceleistungen. Allein das Aktualisieren der Produktionsanlagen kann hier zu einer Herausforderung werden. Testsysteme werden aus Kostengründen nicht vorgehalten und so bedeutet das Einspielen von Updates ein hohes Risiko. Oft existieren nicht einmal Updates bzw. kann das Aktualisieren sogar zum Verlust von Zertifizierungen führen. Ein weiteres Problem stellen die Schnittstellen der Anlagen dar, da diese meist herstellerspezifisch oder nicht im Detail bekannt sind. Auch die Einstellung zur Sicherheit ist bei den OT-Verantwortlichen häufig eine andere. Zugangs- und Zugriffsschutz werden oft aus Effizienzgründen vernachlässigt oder bewusst umgangen, um im Bedarfsfall schnell in den Produktionsprozess eingreifen zu können. Passwörter sind eher hinderlich und werden daher in der Voreinstellung belassen oder ganz weggelassen. Die Funktion und einfachste Nutzung der Anlagen stehen klar im Vordergrund. Es gibt viele offene Punkte, die angegangen werden müssen und für die es ggf. neuer Prozesse, Methoden und Ansätze bedarf.

Ziel des Leitfadens zum ICS-Check

In Ergänzung zum Leitfaden Cyber-Sicherheits-Check (CSC) mit dem Fokus auf IT, der vom ISACA Germany Chapter e.V. im Rahmen der Allianz für Cyber-Sicherheit gemeinsam mit Experten des BSI erstellt wurde, soll ein weiterer Leitfaden für OT entwickelt werden, der sich auf Cyber-Sicherheit in industriellen Anlagen (ICS) fokussiert. Dieser lehnt sich im Vorgehen an die sechs Stufen des CSC IT an, ist aber in den Schritten 2 bis 5 an die Gegebenheiten in der Industrie (Anlagen- und Maschinenbetreiber) angepasst. Das Vorgehen im CSC ICS ist wie folgt strukturiert:

Nach Schritt 1, der Auftragserteilung, erfolgt:

- **Schritt 2 - Ist-Erfassung**
  Befragung der Produktionsleitung zu relevanten Bedrohungen und Werten der Industrieanlage. Was muss hoch verfügbar sein? Welche Teile der Anlage stehen im Fokus? Wie ist der Schutz umgesetzt?
- **Schritt 3 - Vor-Ort-Analyse**
  Begehung der Anlage zur Vertiefung, Einsicht in Dokumente, Hinzuziehen von externen Dienstleistern.
- **Schritt 4 - Ist-Soll-Abgleich**
  Die im Schritt 3 gewonnenen Erkenntnisse werden mit den Anforderungen der Normenreihe IEC 62443 abgeglichen.
- **Schritt 5 - Ergebnisvalidierung**
  Soll-Darstellung für ein angemessenes Cyber-Sicherheitsniveau. Präsentation der Ergebnisse an Produktionsleitung, Aufzeigen von Soll-Maßnahmen, weitergehender Abgleich der Maßnahmen mit Bedrohungen und Werten.

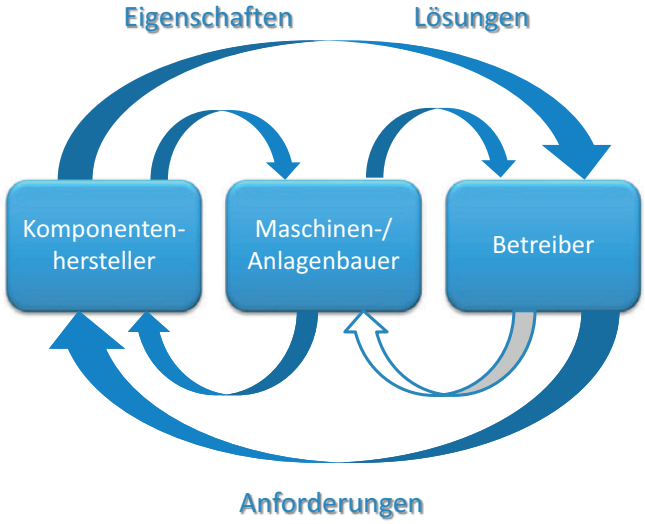
Zielgruppe und Abgrenzung

Über dieses an die Industrie angepasste Vorgehen werden die kritischen Werte (Assets) ermittelt und die notwendigen »Mindest-Hygiene-Maßnahmen« adressiert. Der CSC ICS richtet sich somit insbesondere an die Betreiber von Industrieanlagen in kleinen und mittleren Unternehmen, die damit eine erste strukturierte Bewertung zur Cyber-Sicherheit erhalten. Dazu dient vor allem das hierfür entwickelte Vorgehensmodell, das eine Risikoeinschätzung ermöglicht. Die Ergebnisse der Risikoeinschätzung können mit Handlungsempfehlungen, die auf gültige Normen und Standards verweisen, abgeglichen werden. Die aus der Analyse entstehenden Unterlagen können dann als Basis für die Maßnahmenumsetzung und das Managen des Betriebs genutzt werden. Der Leitfaden dient nicht dazu, eine Norm oder einen Standard zu ersetzen oder konkrete Handlungsempfehlungen in Form einer Schritt-für-Schritt-Anleitung zu liefern. Es soll vielmehr der Einstieg in das Thema Cyber-Sicherheit im Industrieumfeld erleichtert werden und eine Sensibilisierung im Umgang mit dem Thema stattfinden.

Methode / Ansatz

Der methodische Ansatz richtet sich nach dem bewährten Sechs-Stufen-Vorgehensmodell des Cyber-Sicherheits-Checks (CSC) der Allianz für Cyber-Sicherheit und berücksichtigt die klassischen Ziele der Cyber- oder Informationssicherheit – Vertraulichkeit, Integrität und Verfügbarkeit.

Die Schritte 2 bis 5 sind jedoch an die Gegebenheiten in der Industrie (Anlagen- und Maschinenbetreiber) angepasst und die Prioritäten der Schutzziele verändert.



Quelle: A. Teuscher

Der CSC ICS soll den Betreiber ferner unterstützen, die Security-Anforderungen über den Lebenszyklus (Life Cycle) besser zu verstehen und an den Maschinen- und Anlagenbauer oder Hersteller adressieren zu können. Der nicht ausgefüllte Pfeil in der Abbildung zeigt die in der Praxis üblicherweise bestehende Lücke auf. In aller Regel werden eben gerade hier keine Security-Anforderungen vom Betreiber explizit aufgestellt und so wird durch die heute vorhandene physikalische Verknüpfung der klassischen IT und der OT neuen Angriffsvektoren der Boden bereitet.