Digitalisierung in der Prozessindustrie – Aber bitte mit Security-Kompetenz!

Marina Leuning, Erwin Kruschitz

Unternehmen der Prozessindustrie verfügen aktuell über hoch ausgereifte Systeme, die einen nachhaltigen Betrieb mit langen Lebenszyklen ermöglichen. Gleichzeitig hat die Automatisierung einen so hohen Grad der Vernetzung erreicht, dass eine Produktion ohne sie nicht mehr vorstellbar ist. Eingebettete Systeme kommunizieren selbstständig miteinander, Anlagenführer steuern und überwachen aus der Ferne, Wartungspersonal greift weltweit zu und führt Konfigurationsänderungen aus. In solch einer vernetzen Welt endet der Schutz von Produktionsanlagen nicht mehr am Werkstor. Über Netzwerk-Verbindungen können Angreifer in die Systeme eindringen, diese manipulieren und damit weite Bereiche vollständig lahmlegen. Neuere Vorfälle wie Trisis/Hatman/Triton zeigen, dass zunehmend Schadsoftware zum Einsatz kommt, die sich explizit gegen Produktionsanlagen richtet. Damit ändern sich auch die Anforderungen in Bezug auf die IT-Sicherheit in der Produktion stetig.

Schattenseiten der Digitalisierung

Die einzelnen Funktionsdomänen im Produktionsbereich der Prozessindustrie – Produktionsmanagement, Asset-Management, Qualitätsmanagement und Logistik – sind jede für sich heute bereits weitgehend automatisiert und digitalisiert. Die Digitale Transformation wird die Domänen selbst miteinander zu einer Operational Technology (OT) verschmelzen. Jede dafür neu geschaffene digitale Verbindung stellt einen zusätzlichen Nutzen dar, birgt indes auch erhöhte Risiken für Missbrauch.

Risikoanalyse als erste Gegenmaßnahme

Risikoanalysen bilden den ersten Schritt in Richtung Gegenmaßnahmen. Dabei werden bestehende Risiken identifiziert und Handlungsempfehlungen abgeleitet. Abbildung 1 zeigt, welche Komponenten für die Risikobeurteilung einer PLT-Schutzeinrichtung betrachtet werden sollen. Sensoren, Aktoren und die programmierbare Steuerung bilden den Kern der Sicherheitseinrichtung. Aber auch das Programmiergerät und die Konfigurationseinrichtungen für Sensoren und Aktoren beeinflussen die Sicherheitsfunktion. Datenverbindungen und Dienste wie der Verzeichnisdienst zur Regelung des Benutzerzugriffs sind relevant. Auch die Integrität von Daten (z. B. Anlagendokumentation) spielt – zusammen mit der Organisation und Personen – eine wesentliche Rolle und wird entsprechend auf Risiken beurteilt. Mit dem NAMUR Arbeitsblatt 163 „IT-Risikobeurteilung von Prozessleittechnik-Sicherheitseinrichtungen“ sowie der dazugehörigen Checkliste, die in der atp plus 2-3 2017 ausführlich beschrieben worden sind, wurde ein Handlungswerkzeug geschaffen, das eine effektive und ressourcenschonende IT-Risikobeurteilung ermöglicht. Dadurch sollen im Wesentlichen folgende Fragen beantwortet werden:

- Wie sicher (secure) ist meine Prozessleittechnik-Schutzeinrichtung?
- Wie sicher muss sie mindestens sein?

IT-Security Management heute

Die Komplexität des Security-Managements nimmt stetig zu. Cyberangriffe sind heute derart ausgefeilt, dass ihre Abwehr ein hohes Maß an Know-how und Ressourcen erfordert. IT-Prozesse und -Infrastrukturen sind mit Blick auf die neuesten Angriffsarten ständig auf dem neuesten Stand zu halten. In Zukunft werden deutlich mehr Ressourcen für die Bewältigung der Herausforderungen benötigt. Die bisherigen Grundsäulen des Security-Managements – Schützen / Erkennen / Wiederherstellen – werden für sich allein den Anforderungen nicht mehr gerecht.

Bislang steht aus Security-Sicht der Schutz von Komponenten im Vordergrund, durch Standards wie Patch- und Firewallmanagement. Diese sind jedoch nicht in der Lage,

Kompromittierungen zu erkennen. Diese Aufgabe übernimmt ein Angrifferkennungssystem. Um im Schadensfall Daten wiederherstellen zu können, ist ein Configuration-Management unabdingbar.

Soweit der Stand der Technik heute. Doch welche weiteren Securityvoraussetzungen müssen - in Anbetracht der zunehmenden Komplexität – zukünftig geschaffen werden, um Automatisierungsanlagen ausreichend zu sichern?

Kompetenz als Schlüsselfaktor für die Digitale Transformation

Häufig wird die Security von Computersystemen im Unternehmen an Experten delegiert. Es wird verkannt, dass bereits Planungsdaten wie z. B. Risikoanalysen einen Schlüssel für Angreifer darstellen. Angesichts des hohen technischen Aufwands, um die IT-Sicherheit gegen Angriffe von außen zu gewährleisten, wird der Faktor Mensch von innen viel zu sehr unterschätzt. Wenn dieser nicht für Bedrohungen sensibilisiert ist, stellt er ein hohes Risiko dar. Beispiele hierfür sind das Öffnen von Anhängen an E-Mails oder schlecht vergebene Passwörter. Viele Mitarbeiter wähnen sich im internen Netz in einer vermeintlich sicheren Zone, in der folglich keine Risiken vorhanden sind. Ein trügerischer Irrglaube, der Angreifern das Leben einfach macht. In Zukunft sind deshalb eine stärkere Sensibilisierung der Mitarbeiter sowie der Aufbau erforderlicher Kompetenzen gefragt. Doch was genau ist eigentlich mit Kompetenz gemeint?

In der Praxis muss ein Betriebsleiter, der für die Safety einer Automatisierungsanlage verantwortlich ist, nicht zwingend Algorithmen beherrschen und Netzwerke analysieren können. Wichtiger ist vielmehr, dass dieser die Prozesse (Produktions- und Geschäftsprozesse), Daten und Systeme kennt und daraus die erforderlichen Security-Anforderungen ableiten kann. Neben der Kenntnis über bereits existierende Security-Maßnahmen soll ein Betriebsleiter in der Lage sein, folgende Fragen zu beantworten:

▸ Welche Systeme gehören zur Anlage (Kenntnis über Produktions- und Geschäftsprozesse)

▸ Mit welchen Auswirkungen ist bei einer Kompromittierung zu rechnen?

▸ Welcher Notfallplan kommt im Fall einer Kompromittierung zum Einsatz?

▸ Wer ist Security-Verantwortlicher?

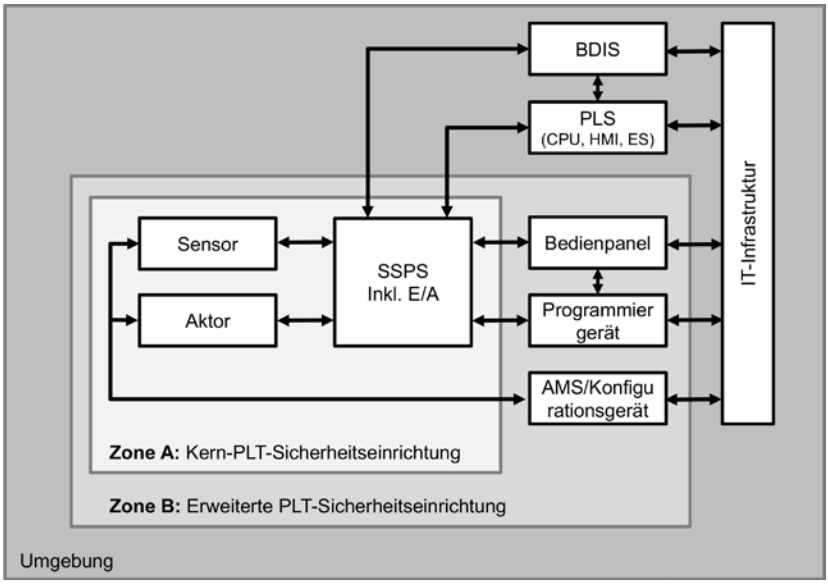

Abbildung 1: Das Zonenmodell nach NA 163. Abbildung © NAMUR

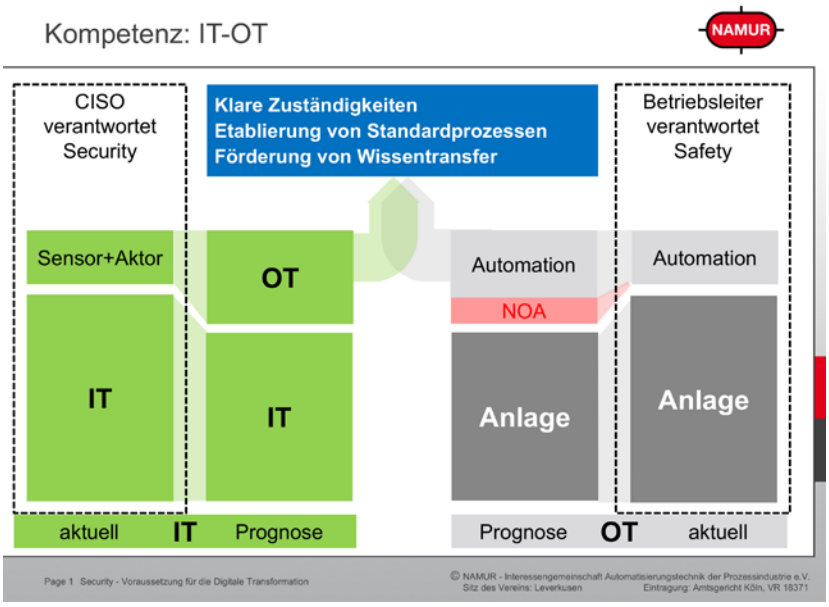

Abbildung 2: Kompetenz von IT und OT. Abbildung © anapur AG 2017

Vernetzung von IT und OT als Voraussetzung für die Digitale Transformation

Für Automatisierungsspezialisten steht die Verfügbarkeit der Anlagen im Vordergrund während das Hauptaugenmerk von IT-Abteilungen in erster Linie darauf ausgerichtet ist, die Integrität und Vertraulichkeit der Daten sicherzustellen. Die beiden Bereiche arbeiten deshalb häufig noch eher nebeneinander als miteinander. Durch unterschiedliche Kenntnisse und Hintergrundinformationen von IT und OT kann es zu Umsetzungsproblemen kommen. Zum Beispiel werden von der IT Vorgaben definiert, die im OT-Bereich aufgrund der Technik nicht ohne weiteres umsetzbar sind. Für den Erfolg der Digitalen Transformation müssen IT und OT zukünftig nahtlos ineinandergreifen und zusammenarbeiten.

Klare Zuständigkeiten

Die noch vorherrschenden recht unterschiedlichen Sicht-

Kategorie	Klassische Unternehmens-IT	Automatisierung
Performance	- keine garantierten Abarbeitungszeiten - hohe Latenz u. U. akzeptabel	- garantierte Abarbeitungszeiten - Latenz ist zum Teil hart begrenzt
Verfügbarkeit	- Rebooten produktiver Systeme nicht ungewöhnlich - Kurzfristig anberaumte Wartungsvorgänge (z. B. Patch) - Wartungsausfälle verursachen geringe Kosten	- Reboot im produktivem Umfeld nicht akzeptabel - Wartungszyklen nur mit langem Vorlauf - Wartungsausfälle verursachen hohe Kosten
Beurteilung von Risiken	- Vertraulichkeit und Integrität von Daten stehen im Vordergrund - Wesentliche Risiken betreffen die nachhaltige Störung von Geschäftsprozessen	- Schutz von Mensch und Umwelt stehen im Vordergrund - Wesentliche Risiken betreffen den unzureichenden Schutz von Menschen und die Zerstörung von Produktionskapazitäten. Auswirkungen auf die Umwelt sind möglich
Systemressourcen / Dediziertheit	- Systeme verfügen über freie Ressourcen, die beispielsweise die Installation von IT-Security-Tools auf dem System erlauben	- Installation von fremden Softwarekomponenten auf den Systemen nicht oder erst nach Freigabe vorgesehen, z. B. Virenschutzprogramme, Programme für Videoanbindung

Abbildung 3: Beim Thema Netz-Sicherheit gibt es gravierende Unterschiede zwischen IT und OT.
Abbildung © Bundesamt für Sicherheit in der Informationstechnik, ICS-Security-Kompendium 2013

weisen auf die fortschreitenden Digitalisierungsprozesse müssen überwunden werden. Durch die Definition von klaren Zuständigkeiten wird geregelt, wer für die Sicherheit zuständig ist und wer im Ereignisfall welche Rolle spielt.

Etablierung von Standardprozessen

Digitalisierungsprozesse umfassen sowohl Anforderungen an die Automationstechnologie als auch an die IT. Verbindliche Vorgehensweisen für IT und OT definieren beispielsweise, wann und von wem Software-Updates durchzuführen sind.

Förderung von Wissenstransfer

Automatisierungsspezialisten und IT-Experten können aufgrund der verschiedenen Perspektiven und des unterschiedlichen Know-hows, das sie einbringen, voneinander lernen. Es sollte eine enge Zusammenarbeit und Kooperation stattfinden.

Vernetzung und Austausch-auf Community-Ebene als Voraussetzung für die Digitale Transformation

Um den Herausforderungen der Digitalisierung zu begegnen, ist ein Austausch miteinander – auch über das eigene Unternehmen hinaus – und das Lernen voneinander mehr denn je von Nöten.

Konkret zählen dazu insbesondere die Erarbeitung von Best Practices sowie ein kontinuierliches Monitoring der aktuellen Sicherheitslage.

Erarbeitung und Austausch von Best Practices

Vor dem Hintergrund der gehäuften IT-Sicherheitsvorfälle sollten Best Practices gesammelt werden, um beispielsweise Schwachstellen frühzeitig zu erkennen und zu beheben. Dies geschieht durch den intensiven Austausch mit anderen Organisationen und Gremien. Der NAMUR-Arbeitskreis Automation Security beispielsweise hat in seiner Praxis-Reihe 2017 drei Dokumente zu Architektur, Systemhärtung und Patchmanagement veröffentlicht (siehe NAMUR-Website, www.namur.net). Hier finden sich auch weitere vom Arbeitskreis betreute Empfehlungen und Arbeitsblätter (wie z. B. NA 163).

Kontinuierliches Monitoring der aktuellen Sicherheitslage

Ein frühzeitiges Erkennen von sicherheitsrelevanten Ereignissen ermöglicht ein rechtzeitiges Reagieren und das Abwenden von möglichen Schäden. Aus diesem Grund sollte eine Strategie entwickelt werden, wie und von wem sicherheitsrelevante Ereignisse erfasst und dokumentiert werden und welche Reaktionen erforderlich sind. Ebenso muss festgelegt werden, wie ein sicherer Zustand wiederhergestellt werden kann.

Fazit

Die Digitale Transformation wird stattfinden. Mit oder ohne Security(kompetenz)! Aber der Erfolg der Digitalisierung hängt wesentlich von der Cybersecurity ab. Neben sicheren Komponenten und der Zuverlässigkeit von Safety Systemen bilden die Kompetenz der Mitarbeiter und der Organisationseinheit sowie die Kooperation von IT und OT die wesentlichen Parameter für den nachhaltigen Erfolg.

Marina Leuning
anapur AG
67227 Frankenthal
Tel: +49 (0)6233 880393-16
m.leuning@anapur.de

Erwin Kruschitz
Namur AK 4.18 Automation Security und Vorstand
anapur AG
67227 Frankenthal
Tel. +49 6233 8803930
info@anapur.de