Erfolgsfaktoren für die Digitalisierung in der Prozessindustrie

Die Digitalisierung der Prozessindustrie schreitet immer weiter voran. Bei aller Euphorie über die Möglichkeiten der Digitalisierung zeigen sich jedoch auch Schattenseiten. Denn die IT-Sicherheit muss mit der Digitalisierung Schritt halten. Zur Identifizierung relevanter Risiken stellen IT-Risikoanalysen ein zentrales Instrument dar. Auch die Kompetenz der Personen und Organisationen muss der Komplexität der Anlage gewachsen sein. Doch was genau ist eigentlich mit Kompetenz gemeint?

Von Marina Leuning und Erwin Kruschitz, anapur AG

Die Automatisierung hat einen so hohen Grad der Vernetzung erreicht, dass eine Produktion ohne sie nicht mehr vorstellbar ist. Unternehmen der Prozessindustrie verfügen über hochausgereifte Systeme, die einen nachhaltigen Betrieb mit langen Lebenszyklen ermöglichen. Eingebettete Systeme kommunizieren selbstständig miteinander, Anlagenführer steuern und überwachen aus der Ferne, Wartungspersonal greift weltweit zu und führt Konfigurationsänderungen aus. In solch einer vernetzten Welt endet der Schutz von Produktionsanlagen nicht mehr am Werkstor.

Angreifer können über Netzwerkverbindungen 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 auch explizit gegen die „Safety" von Produktionsanlagen richtet. Damit ändern sich auch die Anforderungen in Bezug auf die IT-Sicherheit in der Produktion.

Gegenmaßnahme: Risikoanalyse

Risikoanalysen bilden den ersten Schritt in Richtung Gegenmaßnahmen. Dabei werden bestehende Risiken identifiziert und Handlungsempfehlungen abgeleitet. Für eine Risikoanalyse muss Expertise aus den Bereichen Automatisierungstechnik, IT, Cybersecurity und aus dem verfahrenstechnischen Prozess an einen Tisch. Das kann durchaus schwierig werden.

Dieser Problematik ist die NAMUR (Interessensgemeinschaft Automatisierungstechnik in der Prozessindustrie) entgegengetreten und hat das Arbeitsblatt 163 „IT-Risikobeurteilung von Prozessleittechnik-Sicherheitseinrichtungen" geschaffen. Damit soll eine effektive und ressourcenschonende IT-Risikobeurteilung ermöglicht werden. Ein Safety-Ingenieur wird damit in die Lage versetzt, innerhalb eines Tages und ohne spezielle Cybersecurity-Kenntnisse eine IT-Risikobeurteilung durchzuführen.

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 (zum Beispiel Anlagendokumentation) spielt – zusammen mit der Organisation und Personen – eine wesentliche Rolle und wird entsprechend auf Risiken beurteilt.

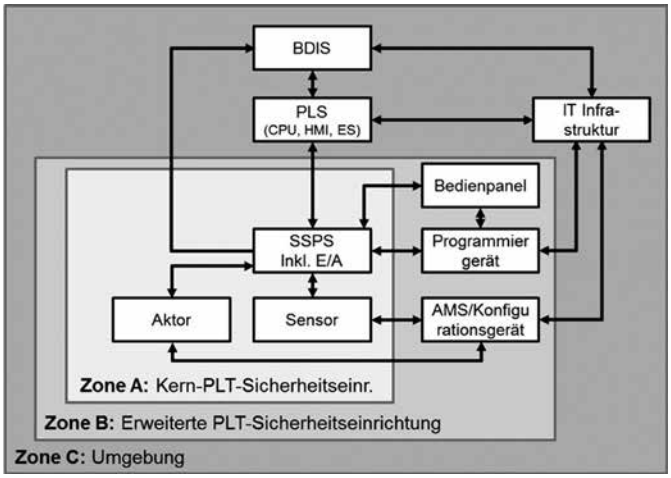

Abbildung 1: Zonenmodell nach NA 163 (NAMUR)

Ziele des „NA 163“-Verfahrens

Ziel des Arbeitsblattes ist die Bereitstellung einer praxistauglichen Risiko-Beurteilungsmethode für PLT-Ingenieure. Die Besonderheit: Die Durchführung des „NA 163“-Verfahrens ist innerhalb eines Tages pro System ohne tiefere Cybersecurity-Kenntnisse durchführbar. Vorhandene Schwachstellen werden aufgedeckt und konkrete Verbesserungsmaßnahmen anhand einer Checkliste vorgeschlagen. Mit dem NAMUR Arbeitsblatt 163 „IT-Risikobeurteilung von Prozessleittechnik-Sicherheitseinrichtungen“ sowie der dazugehörigen Checkliste 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?

Eine IT-Risikobeurteilung mag zwar ohne tiefe Cybersecurity-Expertise machbar sein. Die Herstellung eines sicheren Zustands aber nicht.

Kompetenz als Schlüsselfaktor

Ohne die Expertise von Cybersecurityspezialisten kommt man nicht aus. Doch allein können diese nicht für den sicheren Anlagenzustand sorgen. Ein Betriebsleiter, der gesetzlich für die Safety einer Prozessanlage verantwortlich ist, muss nicht zwingend Algorithmen beherrschen und Netzwerke analysieren. Diese Aufgabe wird er an seine Ingenieure delegieren. Die Kompetenz, die vom Betriebsleiter gefordert wird, ist vielmehr, dass dieser die Prozesse (Produktions- und Geschäftsprozesse), Daten und Systeme kennt und daraus die erforderlichen Security-Anforderungen ableiten kann. Bereits Daten aus dem Planungsstadium wie zum Beispiel Prozess-Risikoanalysen können einen Schlüssel für Angreifer darstellen. Entsprechend sind Planungsingenieure und insbesondere Partnerfirmen gefordert, eine Klassifizierung der entsprechenden Dokumente durchzuführen. Einfallstore wie das Öffnen von Anhängen an E-Mails oder schlecht vergebene Passwörter können letztlich durch jeden geöffnet werden. Entsprechend ist auch jeder für Security verantwortlich.

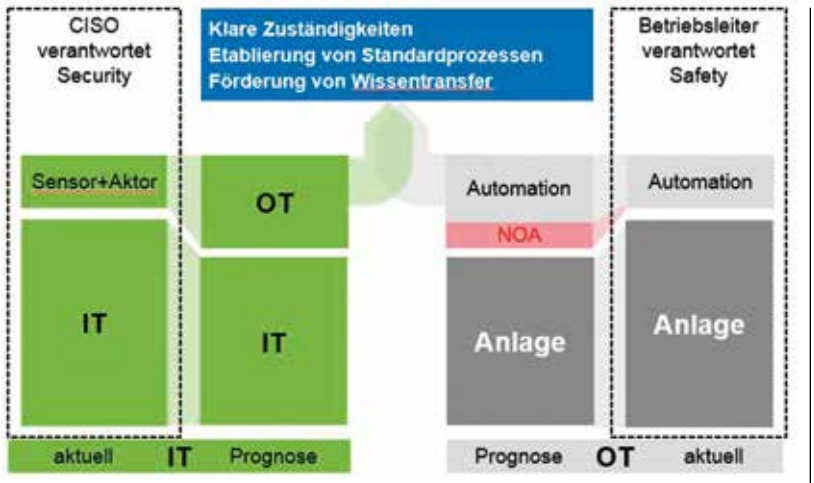

Abbildung 2: Kompetenz von IT und OT, anapur AG 2017

Zusammenarbeit von IT und OT

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 Operational Technology (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. Die noch vorherrschenden recht unterschiedlichen Sichtweisen 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. Digitalisierungsprozesse umfassen sowohl Anforderungen an die Automationstechnologie als auch an die IT. Durch die Etablierung von Standardprozessen für IT und OT wird beispielsweise festgelegt, wann und von wem Software-Updates durchzuführen sind. Automatisierungsspezialisten und IT-Experten können aufgrund der verschiedenen Perspektiven und des unterschiedlichen Know-how, das sie einbringen, voneinander lernen. Der Austausch von Wissen soll gefördert werden und eine enge Zusammenarbeit und Kooperation stattfinden.

Fazit

Die digitale Transformation wird stattfinden – mit oder ohne Security(kompetenz). Eine erfolgreiche Digitalisierung wird nur mit Cybersecurity zu erzielen sein. Insbesondere die Prozessindustrie kann sich angesichts der Risiken für Gesundheit und Umwelt keine Experimente erlauben. Doch auch die Kompetenz der Mitarbeiter und der Organisationseinheit sowie die Zusammenarbeit und Kooperation von IT und OT bilden wesentliche Parameter für einen nachhaltigen Erfolg. Der Fachkongress IMI 2018 – IT meets Industry – veranstaltet von anapur – setzt hier an und hat sich als Industrial Cyber Security Konferenz etabliert.