IT-Sicherheit und Automation

Anwendung der VDI/VDE 2182 in der Prozessindustrie

Akutelle Ereignisse haben das Thema „IT-Sicherheit für Automatisierungssysteme“ in den Fokus gerückt und dabei Fragen nach dem richtigen Vorgehen aufgeworfen. Die VDI/VDE 2182 beschreibt hierfür mit ihrem Managementmodell einen ganzheitlichen Lösungsansatz. Der Beitrag betrachtet die wesentlichen Inhalte der Richtline aus Sicht des Betreibers in der Prozessindustrie und gibt Hinweise zu deren praktischer Umsetzung.

SCHLAGWÖRTER Kommunikation / IT-Sicherheit / Managementsystem

IT-Security and Automation –
Application of VDI/VDE 2182 in the Process Industry

Some recent events made the topic „IT Security” the focal point and raised a lot of questions for the appropriate approach. The VDI/VDE 2182 and its corresponding management model describe a holistic solution. This article considers the significant contents of the guideline from the perspective of an operator in the process industry and provides information on putting them into practice.

KEYWORDS Communication / IT Security / Management System

MICHAEL KUSCHMITZ, Bayer Technology Service

Die IT-Sicherheit der in Unternehmen eingesetzten Systeme, inklusive des speziellen Bereichs der industriellen Automation, ist verschiedenen Bedrohungen ausgesetzt. Dies kann ein nennenswertes Sicherheits- und Geschäftsrisiko darstellen. Um diese Risiken zu beherrschen, müssen finanzielle Mittel aufgewendet werden, die dadurch für Investitionen in das eigentliche Geschäft des Unternehmens nicht mehr zur Verfügung stehen. Die optimale Balance zwischen der Höhe dieser Aufwendungen und der Größe des verbleibenden Restrisikos wird erreicht, indem man sich in der Praxis der Methoden des Risikomanagements bedient.

Als Grundlage für den Aufbau eines Managementsystems für die IT-Sicherheit in der Automation wurde die Richtlinie VDI/VDE 2182 „Informationssicherheit in der industriellen Automatisierung“ erarbeitet. Daran war auch der Namur-Arbeitskreis 2.8 „Internettechnologien“ beteiligt, der sich diesem wichtigen Thema schon seit mehreren Jahren widmet. Die Ergebnisse dieser Arbeit sind in das Namur-Arbeitsblatt NA115 eingeflossen [3].

Die Richtlinie beinhaltet das eigentliche Managementsystem, das in Form eines Vorgehensmodells abgebildet wird. Darüber hinaus beschreibt sie Best Practices aus dem Bereich der IT-Sicherheit, die an die speziellen Gegebenheiten und Anforderungen im Bereich der industriellen Automation angepasst wurden. Sie umfasst ebenso ein Rollenmodell, das die unterschiedlichen Blickwinkel der Zielgruppen Systemhersteller, Integratoren/Anlagenbauer und Betreiber auf dieses Thema abbildet. Diese Aspekte wurden getrennt für Systeme in der Fertigungsautomation (FA) und Prozessautomation (PA) betrachtet.

Die Richtlinie gliedert sich in das Hauptdokument „Grundlagen und allgemeines Vorgehensmodell“ und je ein Dokument für jede Zielgruppe. Anfang 2011 sollen das endgültige Hauptdokument (Weißdruck) und die übrigen als Entwurf (Gründruck) veröffentlicht werden.

1. VORGEHENSMODELL AUS BETREIBERSICHT

In der VDI/VDE 2182 wird ein Vorgehensmodell verwendet, das so allgemein gehalten ist, dass sich die Anforderungen aller Zielgruppen der Richtlinie darauf abbilden lassen. Deshalb soll das Modell an dieser Stelle zunächst auf die konkrete Sicht des Betreibers angepasst werden.

Das PLT-Security-Konzept bildet die Grundlage aller Aktivitäten des Betreibers und damit seines Sicherheitszyklus, der sich für ihn in drei wesentliche Segmente gliedern lässt (siehe Bild 1):

- Risikoanalyse und Gegenmaßnahmen – hauptsächlich Systemdesign
- Betreiben – Notfallprävention und Notfallbeherrschung
- Überprüfen – ständige Überwachung und Audits

Der Neustart des Zyklus erfolgt entweder turnusmäßig, bei Systemänderungen, beim Eintritt bestimmter Ereignisse oder bei festgestellten Abweichungen im Rahmen der Überprüfungen.

2. PLT-SECURITY-KONZEPT

Das PLT-Security-Konzept beschreibt die generell anzuwendenden Grundsätze und Basis-Konzepte. Dabei spannt sich der Bogen von Aspekten der Organisation und Verantwortlichkeiten über Werkzeuge und Vorgehensweisen – bezogen auf die einzelnen Abschnitte des Sicherheitszyklus – bis hin zu Schnittstellen und Anforderungen an die Systeme beziehungsweise die damit im Zusammenhang stehenden Dienstleister.

Die Grundlage des Konzeptes sollte die IT-Sicherheitsrichtlinie des Unternehmens bilden. Um die Kompatibilität sicherzustellen, wird in der Praxis das PLT-Security-Konzept oft als Subdokument zur IT-Sicherheitsrichtlinie eingeordnet und in Zusammenarbeit oder in Abstimmung mit der Unternehmens-IT erarbeitet.

Der Geltungsbereich des PLT-Security-Konzeptes kann das gesamte Unternehmen oder auch nur Unternehmensbereiche, bis hinunter auf die Ebene einzelner Betriebe, umfassen. Es ist also zu prüfen, ob das ganze Unternehmen mit einem einzigen Vorgabedokument abgedeckt werden kann, besonders dann, wenn es sich um international verteilte Niederlassungen mit unterschiedlichen Gegebenheiten und Anforderungen handelt. Bei dieser Konstellation würden sich daraus eher generelle Konzepte mit einem geringen Detaillierungsgrad ergeben. Eine praktische Lösung kann beispielsweise eine hierarchische Struktur von mehreren Konzeptpapieren sein, deren obere Ebene übergeordnete und deren untere Ebene angepasste Detailvorgaben für die verschiedenen Niederlassungen beziehungsweise Betriebe beinhalten.

3. RISIKOANALYSE UND GEGENMASSNAHMEN

Dieser Abschnitt ist der Eintrittspunkt in den Sicherheitszyklus und bezieht sich hauptsächlich auf das Systemdesign.

3.1 Strukturanalyse

Die Grundlage der Analyseaktivitäten bildet die Strukturanalyse. Diese muss nicht bei jedem Neustart des Sicherheitszyklus durchlaufen werden, wenn frühere Ergebnisse weiter Gültigkeit besitzen.

Die Hauptfragen der Strukturanalyse sind: „Was soll betrachtet werden?“ und „Welche Rand-/Umgebungsbedingungen bestehen, und wie sind die Schnittstellen gestaltet?“ Es erfolgt daraufhin eine gedankliche Zerlegung des Gesamtsystems in Betrachtungsgegenstand und Einsatzumgebung, die Schnittstellen und Übergänge dazwischen beziehungsweise die jeweiligen Einflüsse aufeinander. Dabei werden nicht nur die Bestandteile des eigentlichen Systems betrachtet, sondern auch das relevante Umfeld (wie Räume, Energieversorgung, Gebäude-Infrastruktur.).

In der Praxis zeigt sich, dass die wichtigste Grundlage eine vollständige Dokumentation darstellt. Das betrifft auch die Altsysteme, die häufig zur Einsatzumgebung gehören. Eine einheitliche Art und Weise der Dokumentation hat sich als große Hilfe bei der Arbeit der Experten erwiesen, die meist mehrere Systeme bearbeiten und sich somit nicht in jedem Fall wieder neu orientieren müssen.

Durch eine gründliche Strukturanalyse ergibt sich darüber hinaus die Chance, Typicals („Standard“-Bausteine von Systemen/Systemteilen) zu identifizieren. Dadurch müssen die folgenden Analysen und Festlegungen von Gegenmaßnahmen nicht für jedes System wieder von Grund auf neu erstellt werden. Und bei Änderung der Sicherheitslage oder anderer Gegebenheiten lassen sich alle betroffenen Systeme schnell und einfach identifizieren.

Beachtet werden muss auch die Ausführung der Übergänge zwischen Betrachtungsgegenstand und Einsatzumgebung. Deren Gestaltung sollte so erfolgen, dass die Einflüsse der beiden Teile aufeinander möglichst gering sind und sich dadurch die Betrachtungen bei der Analyse auf den jeweiligen Teil beschränken lassen. Ein Beispiel für eine solche Strukturierung beziehungs-

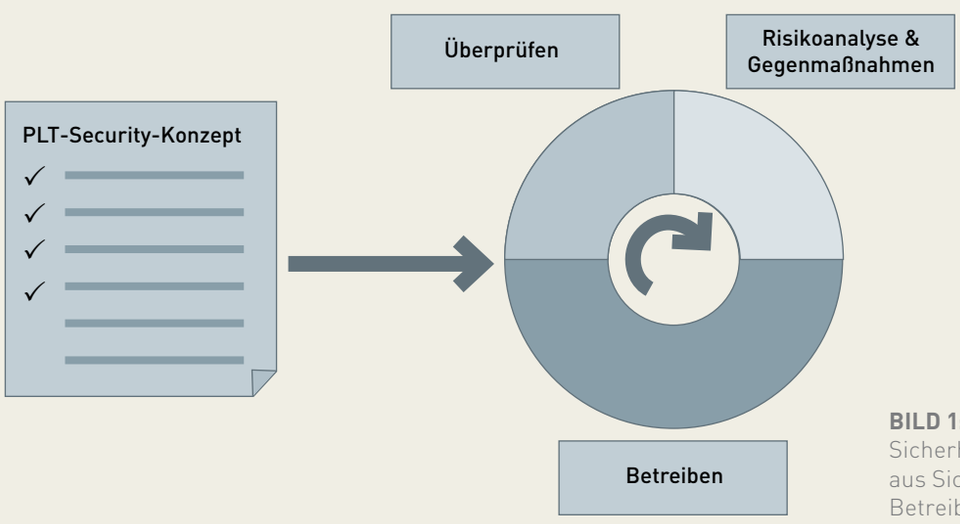

BILD 1: Sicherheitszyklus aus Sicht des Betreibers

weise Clusterung ist die in der Praxis häufig eingesetzte Barriere zwischen PLT- und Office-Netzwerken, die so beschaffen ist, dass beide Netze möglichst rückwirkungsfrei betrieben werden können.

3.2 Implementierung

Vor Beginn des Analysevorganges sieht die VDI/VDE 2182 die Bildung eines Analyseteams mit der Besetzung von bestimmten Rollen vor, die den Know-how-Bedarf für diese Aufgabe widerspiegeln (technische und Anwendungs-Experten, Entscheider, Koordinatoren und so weiter). In der Praxis kann eine Person auch mehrere Rollen repräsentieren, jedoch sollten der gleichen Person nicht Aufgaben mit potenziell gegensätzlichen Interessen übertragen werden. Eine zentrale Fachstelle kann durch die Bereitstellung von Experten und Bündelung von Know-how für die Teambesetzung vorteilhaft sein.

Für den Analysevorgang gibt die Richtlinie einen strukturierten Ablauf vor:

- Identifikation der materiellen und immateriellen Assets
- Identifikation der Schutzziele und möglicher Bedrohungen mit Auslösern und Folgen
- Ermittlung des bestehenden Risikos aus Schadensausmaß und Eintrittswahrscheinlichkeit und Definition des akzeptablen Restrisikos
- Falls das bestehende Risiko das akzeptable Restrisiko übersteigt, erfolgt die Festlegung und Umsetzung von Gegenmaßnahmen und deren Überprüfung auf Wirksamkeit

In der Praxis wird gerade dem Test der Maßnahmen oft noch nicht die notwendige Aufmerksamkeit geschenkt.

Bei der Analyse ordnet die Richtlinie dem Betreiber naturgemäß eine funktionale Sicht („Lastenheft-Niveau“) und die Festlegung des akzeptablen Restrisikos zu. Der Integrator besitzt eine Sicht auf Details beziehungsweise konkrete Geräte („Pflichtenheft-Niveau“) und ermittelt daraus das Istrisiko. Deshalb wird die Erstellung der Analyse von beiden Rollen gemeinsam vorgenommen, wobei in der Praxis die PLT des Betreibers oft auch gleichzeitig die Integratorrolle repräsentiert, da sie nicht nur für die Beauftragung eines Anlagenbauers verantwortlich ist, sondern selbst auch die Auslegung von Systemen vornimmt. Systemhersteller können ebenfalls gleichzeitig auch Integrator im Sinne der Richtlinie sein, wenn sie, statt nur einzelne Komponenten, komplette Systeme liefern oder die Applikationssoftware erstellen.

Für die Analyse schlägt die Richtlinie Werkzeuge vor, beispielsweise eine Risikomatrix, die Schadensausmaß und Eintrittswahrscheinlichkeit auf das Istrisiko abbildet und dieses wichtet, sowie eine Analysetabelle zur Dokumentation der Ergebnisse der einzelnen Analyseschritte. Deren Aufbau folgt idealerweise dem Analyseablauf. Die konkrete Festlegung der Werkzeuge, deren Umsetzung als Liste, Datenbank oder ähnlich und die Risikowichtung in der Risikomatrix sind Inhalt des PLT-Security-Konzepts.

In der Praxis erleichtern dieser formalisierte Ablauf und die dazu passende Dokumentation wesentlich Reviews und Analyse-Updates bei veränderten Rahmenbedingungen. Alle betrachteten Systemteile und Szenarios sind eindeutig beschrieben und bilden dadurch auch die Grundlage für die detaillierte Überprüfung der Wirksamkeit der Gegenmaßnahmen, da sich die entsprechenden Testfälle aus den dokumentierten Szenarios einfach herleiten lassen.

Um aus einer potenziellen eine akute Bedrohung werden zu lassen, müssen drei Bedingungen erfüllt sein:

- Es gibt eine Schwachstelle
- Es gibt einen Angriffspfad zur Ausnutzung dieser Schwachstelle
- Es ist eine ausreichend hohe Motivation beziehungsweise ein Auslöser vorhanden, die Schwachstelle über diesen Angriffspfad auszunutzen

Wirksame Gegenmaßnahmen zu ergreifen, bedeutet also die Einflussnahme auf eine oder mehrere dieser Bedingungen.

Da die Eintrittswahrscheinlichkeit im Bereich der IT- und PLT-Security in hohem Maße von Menschen und deren Motivation abhängt, sind die Analyseergebnisse nur qualitativ beschreibbar und die Bestimmung der Eintrittswahrscheinlichkeiten relativ schwierig. Zumal darüber hinaus die menschliche Motivation vielfach nicht als bewusst (zum Beispiel Hacking), sondern als fahrlässig (beispielsweise Fehlkonfiguration) einzustufen ist.

Im Bereich der Anlagensicherheit wirken dagegen immer vorhandene Naturgesetze, sodass in diesem Fall eine quantitative Ermittlung von Wahrscheinlichkeiten mittels statischer Methoden möglich ist.

Die vorgestellte formalisierte Art der Risikoanalyse wird heute schon genau so oder ähnlich in vielen anderen Bereichen genutzt, die zwar einen anderen Fokus haben, aber die gleichen Systeme betrachten wie die PLT-Security. Es zeigt sich in der Praxis, dass Teile dieser Analysen auch für die PLT-Security genutzt werden können und sich damit der Analyseaufwand reduzieren lässt. Beispielhaft seien GMP-Risikoanalysen (Fokus: Patientensicherheit) und Risikoanalysen der Anlagensicherheit genannt.

Das heute meist übliche Vorgehen, einen Basisschutz über die Umsetzung von Standardmaßnahmen zu schaffen, wird derzeit schon von einzelnen Unternehmen durch die vollständige und formalisierte Analyse gemäß VDI/VDE 2182 ergänzt, um die bisherigen Lösungen zu optimieren oder kritische Systeme detaillierter zu betrachten. Es ist zu beachten, dass die Wirkung der Gegenmaßnahmen von der vollständigen Betrachtung und der konsistenten Umsetzung abhängt. Teillösungen bieten meist keine Teilsicherheit, sondern gar keine. Nicht jede (Standard-)Maßnahme passt auch zu

jedem System. Sie kann sich an einigen Stellen sogar als kontraproduktiv erweisen. Eine tiefergehende Analyse ist also unabdingbar.

Das Vorgehen und die Ansätze für die Analyse und die Gegenmaßnahmen sind von der Art des Betrachtungsgegenstandes abhängig. Im IT- beziehungsweise MES-Bereich ist oft eine strikte Standardisierung möglich. Hier kommen meist viele gleichartige Systeme zum Einsatz. Prozessleitsysteme sind dagegen im Detail häufig Unikate. Auch bei gleicher Systemversion können unterschiedliche Softwarestände bezogen auf Servicepacks, Patches und so weiter und auch verschiedene Ausstattungen an Optionspaketen ein differenziertes Herangehen bedingen.

4. BETREIBEN

Der längste und damit bedeutendste Abschnitt im Lifecycle der Systeme ist deren Betrieb. Das Thema PLT-Security wird mit der Analyse und der Umsetzung von Gegenmaßnahmen im Systemdesign nicht abgeschlossen, sondern damit werden nur die Grundlagen geschaffen. PLT-Security ist als ein Prozess zu verstehen, der auch das Betreiben der Systeme ständig begleitet.

Der Dokumentation kommt auch hier, wie in allen anderen Teilen des Sicherheitszyklus, eine zentrale Bedeutung zu. Neben der Vollständigkeit und möglichst einheitlichen Art und Weise ist eine zentrale Ablage und damit ein schneller Zugriff verschiedener Abteilungen in der Praxis von Vorteil.

Die Richtlinie gliedert Schutzmaßnahmen beim Betreiben der Systeme in zwei Teile: Notfallprävention und Notfallbeherrschung.

4.1 Notfallprävention

Unter die Notfallprävention fallen folgende Maßnahmen:

- Verhindern von Ereignissen/Notfällen
- Erkennung von Ereignissen und Zuständen, die den Normalbetrieb der Systeme beeinträchtigen
- Vorsorgliches Begrenzen des Schadensausmaßes im Fall eines Ereignisses

Neben technischen Maßnahmen spielen dabei vor allem organisatorische Aspekte eine große Rolle. Der klaren Zuordnung von Tätigkeiten und Verantwortlichkeiten innerhalb der Organisationsstruktur kommt eine große Bedeutung zu. Dabei hat sich in der Praxis die klassische Aufgabenteilung innerhalb der PLT auch für diesen Bereich bewährt. Die PLT-Betriebsbetreuung ist für betriebsspezifische Aufgaben zuständig; die zentralen Fachstellen dagegen für Aufgaben, für die gebündeltes beziehungsweise betriebsübergreifendes Know-how notwendig ist.

In Teilbereichen zeigt sich dabei ein Trend, klassische Aufgaben der Betriebsbetreuung zu zentralisieren. Das betrifft zum Beispiel die Datensicherung der Systeme. Daraus kann sich der Vorteil ergeben, dass sich zum einen der Vorgang weiter automatisieren lässt und damit das Personal entlastet wird. Zum anderen lässt sich damit sicherstellen, dass diese Vorgänge für alle betreffenden Systeme gleichartig ablaufen und mit höherer Wahrscheinlichkeit richtig ausgeführt werden als von vielen verschiedenen Personen, denen das Vorgehen nur per Anweisung vorgegeben wird.

Eine große Bedeutung kommt auch dem Konzept zum Einbringen von Software beziehungsweise Datenträgern in die Systeme zu. Da die Systeme dafür nach außen geöffnet werden müssen, haben sich eine Reihe von Best-Practice-Lösungen zur Risikoreduzierung herauskristallisiert. Beispielsweise werden Datenträger vorab auf einem Quarantänesystem auf Schadsoftware überprüft und die Live-Systeme durch das Sperren von Laufwerken, der Autostart-Funktionen und so weiter zusätzlich geschützt.

Neben dem Einbringen von Änderungen zur Korrektur oder Anpassung von Funktionalitäten handelt es sich hierbei auch um Softwareveränderungen wie Patches und aktuelle Pattern für Virenscanner, die der Verbesserung der PLT-Security dienen sollen. Trotzdem ist für diese sehr sorgfältig zu betrachten, ob deren Vorteile nicht durch Nachteile, die sich durch das Einbringen in die Systeme ergeben können, wieder zunichte gemacht werden. Beispielhaft seien hierfür genannt: das Herabsetzen der Verfügbarkeit durch Systemstillstand während der Installation von Patches und die Kommunikationskanäle zu Pattern-Servern, die zusätzliche offene Verbindungen in den Netztrenn-Barrieren erfordern können.

Zur frühzeitigen Erkennung von Fehlern und anderen unerwünschten Zuständen dient das Monitoring. „Frühzeitig“ bedeutet, dass die Erkennung möglichst zu einem Zeitpunkt erfolgen sollte, zu dem noch Handlungsspielraum zur Behebung besteht, bevor ein nennenswerter Schaden eintritt. Dabei werden sowohl die Aspekte, die sich auf die korrekte Funktion der einzelnen Systembestandteile beziehen (Systemgesundheit), als auch die der PLT-Security (zum Beispiel Logs der verschiedenen Sicherheitskomponenten) überwacht. Eine große Bedeutung kommt dabei der Festlegung von sinnvollen Grenzwerten zu, bei deren Verletzung vom Eintritt eines Ereignisses ausgegangen werden muss. Da diese Festlegungen eine vollständige Dokumentation der Systembestandteile und ein hohes Maß an Expertenwissen erfordern, sind sie in der Praxis meist nur in Zusammenarbeit mit Herstellern und Integratoren zu treffen. Die manuelle Auswertung der laufend anfallenden Monitoringdaten ist durch deren Menge und komplexen Zusammenhänge untereinander meist nicht zu leisten. Hierzu sind zentrale Tools als Informationsdrehscheibe sehr nützlich. Diese setzen idealerweise die Daten aller relevanten Systembestandteile in Bezie-

hung und treffen möglichst automatisiert einfach zu erfassende Diagnoseaussagen.

Die komplexen technischen Zusammenhänge und die Notwendigkeit, ein hohes Bewusstsein für ein angemessenes Handeln in Bezug auf die PLT-Security (Awareness) zu pflegen, erfordern ein Konzept zur Schulung der Mitarbeiter. Diese Schulungen sollten regelmäßig erfolgen und nicht nur bei Änderungen oder Vorfällen. Da der betreffende Personenkreis die Spezialisten der PLT beziehungsweise PLT-Security bis hin zu den Anwendern der Systeme umfasst, haben sich in der Praxis Schulungen mit rollenspezifischen Inhalten und Wiederholungszyklen bewährt.

4.2 Notfallbeherrschung

Die Notfallbeherrschung umfasst alle Aktivitäten zur Aufrechterhaltung oder zur schnellen Wiederherstellung des Geschäftsbetriebes im Ereignisfall, das Einleiten und Durchführen eines Notbetriebs sowie die Störungssuche/-beseitigung.

Im Fall eines Ereignisses kommt es vor allem auf schnelles, effizientes und richtiges Handeln an, um das Schadensausmaß so gering wie möglich zu halten. Die vorab getroffene, klare Festlegung und vor allem auch Erprobung der Melde- und Eskalationswege ist deshalb von entscheidender Bedeutung. Hilfreich kann eine Kategorisierung nach Störungsarten sein, da je nach zu erwartenden Folgen des Ereignisses gegebenenfalls andere Eskalationswege gelten. Darüber hinaus ist auch die umfassende und zeitnahe Verfügbarkeit von Informationen für alle Betroffenen bedeutsam. Hier hat sich zum Beispiel deren Publizierung über die vielerorts bestehenden Intranetseiten der PLT-Communities bewährt.

Den zweiten großen Themenkreis der Notfallbeherrschung bilden die Tools zur Problemanalyse und -beseitigung. Auch hier sollte vorab klar definiert sein, welche Arten von Fehlern oder Störungen mit welchen Tools bearbeitet, welche Versionen dabei verwendet werden und welche Personen die Arbeiten ausführen sollen. Die entsprechenden Werkzeuge sind verfügbar und der Personenkreis auf dem erforderlichen Wissens- und vor allem auch praktischen Trainingsstand zu halten, um diese zielgerichtet und effizient einsetzen zu können. Darüber hinaus sind die Vorgaben und Freigaben der Systemhersteller für den Einsatz der verschiedenen Werkzeuge zu beachten. Da in vielen Fällen auf Tools zurückgegriffen wird, die auch im Office-Bereich eingesetzt werden, kann eine Zusammenarbeit mit der Unternehmens-IT aufgrund möglicher Synergieeffekte ein vorteilhafter Weg sein.

5. ÜBERPRÜFEN

Der dritte und letzte Abschnitt im Vorgehensmodell des Betreibers ist das Überprüfen. Hierbei unterscheidet die VDI/VDE 2182 zwischen laufenden Überwachungen und Audits.

Die laufenden Überwachungen lassen sich wiederum in das Monitoring, das im Rahmen der Notfallprävention durchgeführt wird, und die ständige Beobachtung der Sicherheitslage gliedern. Da in der IT- beziehungsweise PLT-Security die Höhe des Risikos von einer sich in ständiger Bewegung befindlichen Sicherheitslage bestimmt wird, ist sowohl deren lückenlose Beobachtung wie auch die damit verbundene Überprüfung der bisher getroffenen Einschätzungen entscheidend. Hierbei zeigt sich dann auch der Wert einer Analysedokumentation, die für diese Aufgaben praktisch und aufwandsarm nutzbar ist. Sollten sich Diskrepanzen zwischen vorhandener und neuer Einschätzung der Risiken ergeben, ist der Sicherheitszyklus neu zu starten. Um den Aufwand für eine möglichst lückenlose Beobachtung der Sicherheitslage zu reduzieren, ist auch hier die Kooperation mit den Herstellern und der Unternehmens-IT ein oft beschrittener Weg.

Demgegenüber dienen Audits der formalen oder qualitativen Überprüfung der Einhaltung der Vorgaben, die im Rahmen des PLT-Security-Konzeptes oder der einzelnen Schritte des Sicherheitszyklus definiert wurden. Da die Wirksamkeit des Managementsystems wesentlich von seiner vollständigen Umsetzung abhängt, stellen Audits einen nicht zu unterschätzenden Erfolgsfaktor dar. Sie sollten jedoch nicht nur als Überwachungsaktivität gesehen werden, sondern sie dienen auch dem Erfahrungsaustausch und spielen deshalb im kontinuierlichen Verbesserungsprozess eine große Rolle.

In der Praxis zeigt sich, dass regelmäßige Audits für Unternehmen mit vielen, dazu noch international verteilten, Niederlassungen eine personelle Herausforderung darstellen können. Praktikable Lösungen hierfür sind zum Beispiel die Integration der PLT-Security-Aspekte in allgemeine PLT-Audits oder die Kooperation mit anderen Abteilungen oder externen Spezialisten vor Ort.

6. ZUSAMMENARBEIT MIT HERSTELLERN UND INTEGRATOREN

Die wichtigste Forderung aus Sicht des Betreibers ist es, dass sich der Aufwand in Bezug auf die PLT-Security auf ein Minimum reduzieren muss. Das bezieht sich sowohl auf den Aufwand, der dem Betreiber direkt entsteht wie auch auf die Mehrkosten, die über die Preisbildung von Herstellern und Integratoren an ihn weitergegeben werden. Der Durchsetzung dieses Anliegens widmet sich auch die Namur schon seit etlichen Jahren. Um diesem Anspruch gerecht zu werden, müssen alle Aspekte der PLT-Security möglichst früh im Lebenszyklus der Systeme verankert werden [3].

Dadurch ergeben sich aus Sicht des Betreibers eine Reihe von Anforderungen an die anderen beiden Rollen „Hersteller“ und „Integrator“, deren Beitrag die notwendigen Grundlagen für eine erfolgreiche Umset-

zung schaffen muss. Beispielhaft seien hier folgende genannt:

- Die PLT-Security muss ein Designziel der Systeme sein.
- Alle Eigenschaften und Funktionen der Systeme müssen vollständig dokumentiert sein.
- Die von den Herstellern und Integratoren vorgeschlagenen Lösungen müssen spezifisch für den Bereich der industriellen Automation anwendbar sein.
- Hersteller und Integratoren müssen Know-how-Führer sein, PLT-Security muss zu ihrer Kernkompetenz gehören.
- Der Betreiber muss bei veränderter Sicherheitslage sofort die notwendigen Informationen und in Notfällen die benötigte Experten-Hilfe erhalten können.

Aus heutiger Sicht zeigt sich hierzu in der Praxis allerdings leider noch ein spürbarer Nachholbedarf was das Problembewusstsein und die Lösungskompetenz betrifft.

7. FAZIT

Die Richtlinie VDI/VDE 2182 beschreibt eine Möglichkeit zum Umgang mit dem Thema der PLT-Security. Sie „erfindet“ dabei nicht grundlegend Neues, sondern verbindet über ihr Vorgehensmodell bewährte Bausteine des Risikomanagements zu einem effizienten und vollständigen Prozess. Da es sich um ein noch relativ junges Themenfeld handelt, muss zukünftig noch ein erhebliches Maß an weiteren praktischen Erfahrungen gewonnen werden, bis sich optimale Werkzeuge, Risiko-Bewertungsmaßstäbe und so weiter eindeutig herauskristallisieren. Ebenso muss auch die Richtlinie parallel zu diesen Erfahrungen weiterentwickelt werden.

Aus heutiger Sicht lässt sich feststellen, dass viele der beschriebenen Teilaspekte schon angewandt werden und sich auch erste vollständige Umsetzungen in Namur-Unternehmen im Teststadium befinden. Insbesondere mit technischen Best-Practice-Lösungen ist man an vielen Stellen schon gut vertraut. Bei der Umsetzung der analytischen und organisatorischen Aspekte zeigt sich jedoch noch deutliches Verbesserungspotenzial.

MANUSKRIPTEINGANG
13.12.2010
Im Peer-Review-Verfahren begutachtet

DANKSAGUNG

Mein besonderer Dank gilt den Kollegen des Namur-Arbeitskreises 2.8 „Internettechnologien“ für die sehr konstruktive Unterstützung bei der Erarbeitung dieses Beitrages.

REFERENZEN

[1] VDI/VDE 2182: Informationssicherheit in der industriellen Automatisierung
[2] Schmidt, K.: Der IT-Security Manager. Carl Hanser Verlag München 2006
[3] NA115: IT-Sicherheit für Systeme der Automatisierungstechnik: Randbedingungen für Maßnahmen beim Einsatz in der Prozessindustrie. Juni 2006

AUTOR

Dipl.-Ing. (FH) **MICHAEL KUSCHMITZ** (geb. 1971) ist seit 1999 Mitarbeiter der Bayer AG und in unterschiedlichen Funktionen der PLT-Betriebsbetreuung und Projektabwicklung tätig. Seit 2006 ist er bei der Bayer Technology Services GmbH beschäftigt und dort als Lead Engineer für die Prozessleittechnik in Investitionsprojekten verantwortlich. Darüber hinaus beschäftigt er sich mit den Themen „funktionale Sicherheit“ und „IT-Security in der Automation“. Innerhalb der Namur ist er im Arbeitskreises 2.8 „Internettechnologien“ und in der GMA im Fachausschuss 5.22 „IT-Security in der Automatisierungstechnik“ tätig.

Bayer Technology Services GmbH,
Geb. 118, D-42096 Wuppertal, Tel. +49 (0) 202 36 28 19,
E-Mail: michael.kuschmitz@bayer.com