Erstellung eines detaillierten Risikobehandlungsplans

Heiko Rudolph · Sascha Giebelhausen · Matthias Müller

admeritia GmbH
{heiko.rudolph | sascha.giebelhausen | matthias.mueller}@admeritia.de

Zusammenfassung

Diese Ausarbeitung beschreibt die Konzeption, Erstellung und Umsetzung eines detaillierten Risikobehandlungsplans auf Basis einer detaillierten Risikoeinschätzung (Detailed Risk Assessments) nach dem Standard IEC 62443-2-1. Dabei werden sowohl die Planung von standardbasierten technischen und organisatorischen Maßnahmen, als auch die Berücksichtigung der aktuellen Betriebsorganisation als Basis für den zu erstellenden Risikobehandlungsplan behandelt. Die Workshop-basierte Umsetzungsempfehlung basiert dabei auf den gesammelten Auffälligkeiten der detaillierten Risikoeinschätzung, ohne den Ist-Zustand der Betriebsorganisation aus dem Auge zu verlieren. Durch diesen Ansatz wird die Chance genutzt, eine IT-Sicherheit sowohl auf dem faktischen Sicherheitsniveau aufzusetzen, als auch alle Maßnahmen risikoorientiert und mit dem Fokus auf die Betriebsverträglichkeit zu planen und umzusetzen. Aufgrund der Verankerung der Methodik in den Industriestandard IEC 62443, beziehen sich die Praxisbeispiele auf Projekterfahrungen aus der vernetzten Automatisierung. Die Vorgehensweise ist allerdings auch auf alle anderen Branchen anwendbar, insbesondere wenn ein funktionierendes Risiko- bzw. Sicherheitsmanagement etabliert ist oder sich im Aufbau befindet. Dabei muss ein Sicherheits-Managementsystem nicht zwingend zertifiziert sein oder auf dem Standard IEC 62443 basieren.

1 Einleitung

In der vernetzten Automatisierung sind für eine risikobasierte Steuerung kontinuierliche Risikoanalysen unausweichlich. Risikobehandlungspläne sind dabei ein wesentlicher Bestandteil dieses Risikomanagements, um die einzelnen Risiken nicht nur zu erkennen, sondern sie entsprechend der gewählten Risikostrategie und -bereitschaft zu behandeln. Ein solcher Risikobehandlungsplan gehört innerhalb eines Sicherheitsmanagementsystems zu einem der zentralen Elemente. Dabei handelt es sich allerdings meist nicht um eine detaillierte Variante. Er dient lediglich dazu, für jedes Risiko eine Maßnahme festzulegen, wie diese im Kontext der vier generischen Risikobehandlungsstrategien (vermeiden, transferieren, reduzieren, akzeptieren) behandelt werden. Durch einen detaillierten Risikobehandlungsplan können die einzelnen Risikobehandlungen betriebsverträglich und mit Blick auf das Risiko- und Sicherheitsmanagement nachhaltig als Maßnahmenbündel geplant und umgesetzt werden, auch wenn kein zertifiziertes Sicherheitsmanagementsystem vorhanden ist.

2 Risikomanagement

Die IT-Sicherheit in der vernetzten Automatisierung wird in der Regel risikobasiert gesteuert. Dies wird so auch in den einschlägigen Standards und Normen empfohlen, wie z.B. in der IEC

P. Schartner · A. Baumann (Hrsg.) · D•A•CH Security 2017 · syssec (2017) 250-258.

62443-Reihe [Inte15], welche sich im aktuellen Entwurf ohnehin an der streng am Risikomanagement ausgerichteten ISO/IEC 27001 [IsIe13] orientiert. Das bietet vor allem den Vorteil, dass die Risikolevel je nach Risikobereitschaft organisationsintern selbst bestimmt werden können. Die Automation Security kann durch die zur Verfügung stehenden Risikostrategien nach dem Angemessenheitsgrundsatz umgesetzt werden. Ihre Steuerung über das Risikomanagement lässt sich dabei schlank über eine Policy und eine Automation Security Governance realisieren und benötigt nicht zwangsweise ein Managementsystem, welches sich naturgemäß kaum mit der operativen Sicherheit beschäftigt, sondern reinweg das Managementsystem bereitstellt.

In der Automation ist häufig aufgrund der verteilten Betriebsstätten und ihrer autarken Regelung der Verantwortlichkeiten ein zentrales Managementsystem nicht von großem Nutzen. Ferner ist es in der vernetzten Automatisierung meist extrem wichtig, eine betriebsverträgliche Ausrichtung der Maßnahmen zu finden, die der hohen Verantwortlichkeit für den Betrieb im Kontext der Rahmenbedingungen, wie z.B. die Vermeidung von Umwelt-, Personen- und Gesundheitsschäden, gerecht wird.

Der Risikomanagementansatz erfordert eine kontinuierliche Risikoeinschätzung und die konsequente Einführung von Risikobehandlungsplänen und deren folgerichtige Nachbearbeitung sowie ein Ausnahme- und Eskalationsmanagement. Eine regelmäßige Risikoeinschätzung wird in der Regel einerseits mit Hilfe einer zu regelnden initialen und weiterer regelmäßigen sowie anlassbezogenen Risikoanalysen sichergestellt.

Der Kern des Risikomanagements ist in den Risikobehandlungsplänen zu sehen, da hier die grundsätzlichen Risikostrategien Reduzierung, Transfer, Akzeptanz und Vermeidung gewählt werden und durch Auswahl konkreter Maßnahmen zum Tragen kommen. Risikobehandlungspläne bestehen aus technischen und organisatorischen Maßnahmen. Die Kunst ist dabei, das vorherrschende Betriebsregime so zu berücksichtigen, dass die im Risikobehandlungsplan definierten Maßnahmen von der Betriebsführung akzeptiert, gelebt und betrieben werden können. So ist es an einigen Stellen sinnvoll, betroffene Mitarbeiter in entsprechenden Workshops zur Maßnahmenfestlegung mit einzubinden. Die Betriebsverträglichkeit steht hier im absoluten Vordergrund, da ansonsten wenig nachhaltige Maßnahmen definiert werden, welche keine allzu großen Halbwertzeiten aufweisen dürften. Die Betriebsverträglichkeit muss u.a. durch die konsistenten Verfahren und Betriebsprozesse sichergestellt werden.

Insbesondere, wenn kein Sicherheitsmanagementsystem (z.B. (Cyber-)Security-Managementsystem (CSMS) gemäß IEC 62443 oder Information-Security-Managementsystem (ISMS) gemäß ISO/IEC 27001) vorhanden ist, ist die risikobasierte und betriebsverträgliche Ausrichtung der Automation Security das Maß der Dinge, wie es im Übrigen der Kern von Informationssicherheitsmanagementsystemen ist.

2.1 Risikoeinschätzung / -bewertung

Eine Risikoeinschätzung beinhaltet auch die Bewertung der Risiken. Eine für die meisten Fälle geeignete Risikoeinschätzungsmethodik ruht auf einem szenarienorientierten Threat-Agent-Model, in dem Threat-Agents für Systemgruppen (Asset-Gruppen) in Abhängigkeit ihrer Kritikalitäten bzw. Schutzbedarfe über Angreifereigenschaften (Zugang, Fähigkeiten, Ressourcen) ermittelt werden. Das geschieht über eine einfach zu parametrierende Modellierung der vorgenannten Relationen. Ist die Risikoeinschätzungsmethodik einmal modelliert, kann sie in der Regel für die nächsten Risikoeinschätzungen wiederverwendet werden, ggf. leicht modifiziert

hinsichtlich bestimmter, sich unter Umständen geänderter Eigenschaften [RuGo15]. Eine solche Risikoeinschätzungsmethodik entspricht den in der IEC 62443-2-1 geforderten Detailed Risk Assessments. Abgerundet wird die Risikoeinschätzungsmethodik durch verifizierende Untersuchungen, wie z.B. Firewall Reviews, Netzwerkverkehrsanalysen und ggf. sogar technische Auditierungen und Security Tests [RBKG15], deren Ergebnisse und Findings in die Methodik eingespeist werden können.

Bei der Bestimmung des Schutzbedarfs von Systemen bzw. Assets können Security Level (SL) sowie Systems Requirements (SR) und Foundational Requirements (FR) unterstützen, wie sie der Standard IEC 62443-3-3 beschreibt. Die hieraus letztlich resultierenden Protection Level können bei der Erstellung von Risikobehandlungsplänen (Risk Treatment Plan, RTP) äußerst hilfreich sein. Sie können als Risiko- und Reifegradlandkarten zur Steuerung der IT-Sicherheit genutzt werden. Sofern Safety-relevante Systeme eine Rolle spielen, muss gemäß der Norm IEC 61511 [Inte16] eine Risikoeinschätzung [RuGo16] vorgenommen werden. Die obige Risikoeinschätzungsmethodik kann hierfür entsprechend modifiziert genutzt werden.

Solche detaillierten Risikoeinschätzungen werden in aller Regel für bestimmte Betriebe oder Anlagen auf Grundlage einer Geschäftsauswirkungsanalyse abgestuft initial und sodann regelmäßig, z.B. zweijährig durchgeführt. Häufig ist in der Automation Security Policy festgeschrieben, dass bei signifikanten Änderungen an der Anlage, wie z.B. der Erneuerung des Leitsystems, im Rahmen des Projektmanagements, z.B. bei der Einführung neuer Systeme und bei Betriebsübernahmen, wie bei Fusionen und Unternehmenszukäufen erneute detaillierte Risikoeinschätzungen vorgenommen werden müssen.

2.2 Risikostrategie / Risikobehandlungsoptionen

Für den Risikobehandlungsplan werden alle ermittelten Risiken gesammelt dargestellt. Im Anschluss daran erfolgt die Festlegung, mit welcher Risikostrategie sie behandelt werden. So wird die Vermeidungsstrategie gewählt, wenn es keine Rechtfertigung für das System oder den Service gibt, der dem Risiko zugrunde liegt. Gerade in Betriebsumgebungen mit „Shared Services“, die z.B. die Firewalls zwischen bestimmten Netzsegmenten administrieren, wird die Transferstrategie angewendet. Unabdingbar sind dann häufig SLAs/OLAs (Service Level Agreements/Operational Level Agreements), die das Risiko auch tatsächlich transferieren und auf diese Weise für klare Verantwortlichkeiten sorgen. Soll die Akzeptanzstrategie gewählt werden, ist es von großer Bedeutung, dass der Risikoeigentümer das akzeptierte Risiko auch formal, z.B. durch Unterschrift übernimmt. Eine implizite Übernahme des Risikos ist in den meisten Fällen nicht zu empfehlen. Definitiv die häufigste Risikostrategie ist freilich die Reduzierung des Risikos. Hierfür müssen die Eintrittswahrscheinlichkeit bzw. die Auswirkungen bei einem Ereignis durch entsprechende Maßnahmen reduziert werden.

2.3 Ermittlung von detaillierten Maßnahmen

Die Reduzierung bedingt Maßnahmen. Solche Maßnahmen lassen sich aus den gängigen Standards, wie z.B. der IEC 62443- oder der ISO/IEC 27000-Reihe entlehnen. Besonders die Anlehnung an die Security und Protection Level des IEC 62443-3-3 ist hier ein vielversprechender Ansatz. Zu einigen Technologien ist die Normierung noch nicht ausgeprägt genug oder noch nicht vorhanden, wie es das Beispiel der Virtualisierung zeigt. An dieser Stelle muss auf Best Practices zurückgegriffen werden.

Unabhängig davon, welche Maßnahme gewählt wird, ist es äußerst wichtig, die Maßnahme operativ auch betreiben zu können. Als Grundsatz gilt dabei, dass eine risikoreduzierende Maßnahme rückwirkungsfrei auf den Betrieb sein sollte.

Für das Sicherheitsmanagement ist es bedeutsam, die Maßnahme in eine Vorgabe, z.B. in eine Policy oder in ein Regelungsdokument eines Sicherheitsmanagementsystems zu wandeln. Dies verhindert auch die Wiederholung der Auffälligkeiten zu einem späteren Zeitpunkt, da die Ursächlichkeit des Fehlers prozessual behoben wurde.

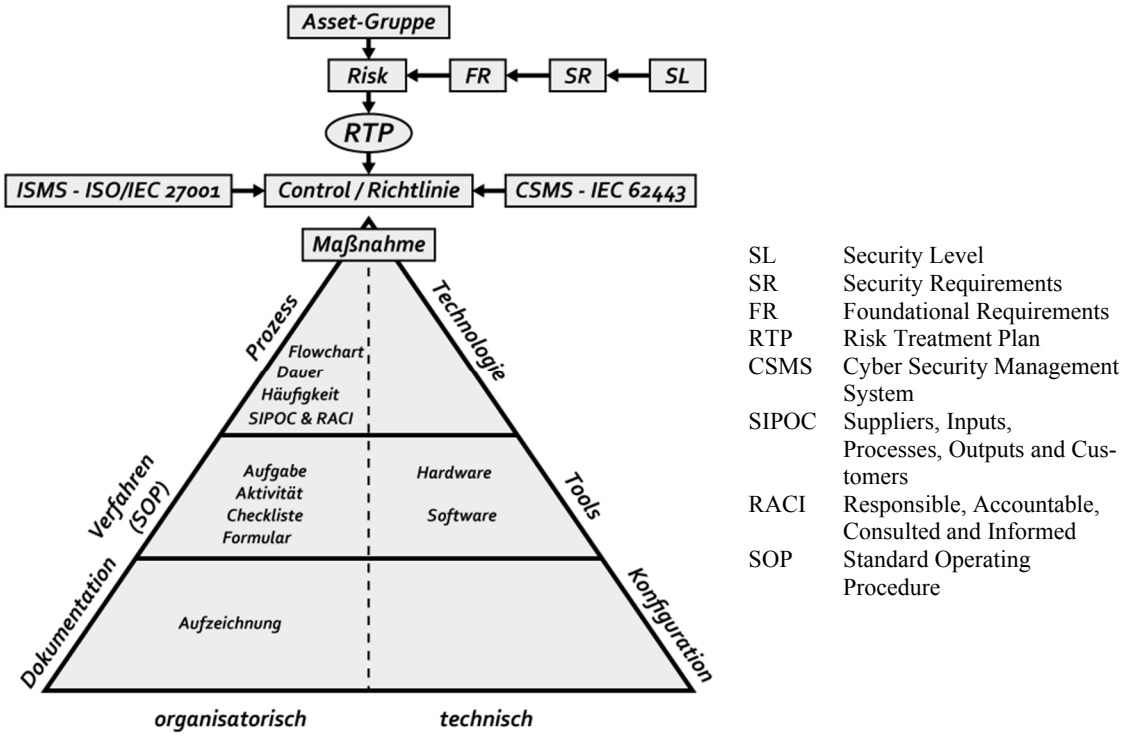

Abb. 1: Struktur des Risikobehandlungsplans

Um die Maßnahme für die operative Sicherheit so zu gestalten, dass sie nachhaltig implementiert und im Betrieb aufrechterhalten werden kann, muss sie sowohl organisatorisch als auch technisch aufeinander abgestimmt konzeptioniert und implementiert werden. Andernfalls würde eine Degradation des Security Levels zu Tage treten, welche meist implizit eine (erneute) Erhöhung des Risikolevels nach sich zieht.

2.3.1 Organisatorische Maßnahmen

Der organisatorische Maßnahmenstrang erstreckt sich in erster Linie über die Prozess- und Verfahrensebene, in denen die Vorgaben aus den Richtlinien der entsprechenden Maßnahme (Control) betriebsgerecht definiert und niedergeschrieben, bzw. angepasst werden müssen.

So muss jeder Prozess, der sich aus einer Maßnahme, bspw. dem Patch-Management, ableitet mit entsprechenden Parametern wie Dauer, Häufigkeit und Verantwortlichkeiten, dokumentiert werden.

Auch in den Verfahren muss genau beschrieben werden, welche Aufgabe oder Aktivität durchzuführen ist und wie dies zu geschehen hat. Des Weiteren muss das Verfahren entsprechende Formulare oder Checklisten bereithalten. Letztere können auch für die Aufzeichnungen zu Dokumentationszwecken dienen, in dem sie nach der Erledigung einer Aktivität ausgefüllt werden

oder dieser Schritt automatisch aus einer Softwarelösung generiert wird. So kann auch der Nachweis für spätere Auditierungen leichter erfolgen.

2.3.2 Technische Maßnahmen

Für die technischen Aspekte der gewählten Maßnahme muss unter Berücksichtigung der betrieblichen Rahmenbedingungen, technischen Gegebenheiten und der Anforderungen an die Lösung, zuerst die Technologie bestimmt werden. Diese birgt meist eine entsprechende Hard- und Software-Anforderung für die benötigten Werkzeuge in sich. Hierbei bietet es sich auch an mehrere Maßnahmen zu bündeln, um ggf. auf gemeinsame Hardware zurückzugreifen. Der Lösungsansatz der zentralen Dienste basiert bspw. auf diesem Prinzip [RuGr12]. Die Ausgewählte Lösung muss natürlich entsprechend sicher konfiguriert und das Ergebnis im organisatorischen Strang dokumentiert werden. So ist die Verzahnung der Technik mit den Vorgabedokumenten sichergestellt.

3 Betriebsorganisation

Für die betriebsverträgliche Regelung kann eine einfache Methodik herangezogen werden, namentlich der Betriebsorganisationsleitsatz. Dieser besteht aus der Fragestellung:

- WER macht
- WAS
- WOMIT
- WIE (oft)
- nach WELCHEN REGELN?

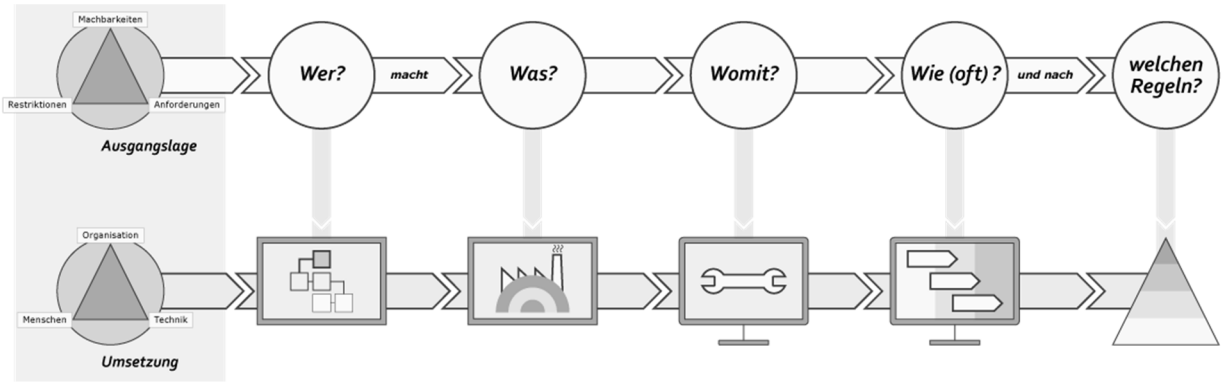

Abb. 2: Betriebsorganisation

Es empfiehlt sich dringend, die einzelnen Elemente der Betriebsorganisation zunächst in ihrer Ausgangslage und somit im vorherrschenden Betriebsregime zu betrachten. In aller Regel unterliegt das dominierende Betriebsregime Handlungszwängen und Restriktionen, welche die Machbarkeiten bestimmter Maßnahmen eingrenzen. Das Verständnis des Betriebsregimes ist unabdingbar für den nachhaltigen Erfolg des Risikobehandlungsplans.

Am Beispiel des Patch-Managements im Automatisierungsumfeld lässt sich der Betriebsorganisationsleitsatz gut veranschaulichen.

3.1 Wer?

Im ersten Schritt wird untersucht, welche personellen Kräfte für den operativen Betrieb der Sicherheitsmechanismen bereitstehen und wie die Sicherheitsmechanismen in der Ist-Situation administriert und betrieben werden. Es empfiehlt sich, das vorhandene Rollenmodell zu beschreiben, mit dem die derzeitigen Betriebsabläufe bewältigt werden. In den allermeisten Fällen dürfte kein zusätzliches Personal bereitgestellt werden können, so dass die Maßnahmen des Risikobehandlungsplans mit dem vorhandenen Rollenmodell abgedeckt werden müssen. In ausgewachsenen oder konzernähnlichen Organisationen können RACI-Matrizen [JaKe09] ein hilfreiches Element sein, die Verantwortlichkeiten zu verdeutlichen.

Allerdings sind für das Patch-Management der Betreiber und der Hersteller des Automatisierungssystems gleichermaßen verantwortlich. Es muss also eine Abstimmung geben, welche Maßnahmen möglich sind und ggf. gemeinsame Lösungen ausgearbeitet werden.

3.2 Was?

Die Maßnahmen sollten auf der organisatorischen Ebene mit Prozessen und Verfahren untersetzt sein. Hieraus ergeben sich die Aufgaben und Aktivitäten, welche durch das Rollenmodell abgedeckt sein müssen.

3.2.1 Dokumentation

Der Betreiber dokumentiert den gesamten Ablauf des Patch-Vorganges. Dazu wird eine Dokumentation erstellt, welche eine Gesamtliste aller verwendeten technischen Komponenten der Prozessleittechnik, für die eine Aktualisierung erforderlich ist, beinhaltet.

3.2.2 Kommunikationsaustausch

Der Betreiber realisiert einen regelmäßigen und wiederkehrenden Informationsaustausch mit dem Hersteller. Zu diesem Zweck muss der Hersteller eine zyklisch aktualisierte Liste der freigegebenen Patches zur Verfügung stellen. Neben dem Informationsaustausch mit dem Hersteller, können darüber hinaus auch unabhängige Informationsquellen verwendet werden, die Aufschluss über notwendige Patches geben. Dazu zählen z.B. ICS-CERT (The Industrial Control Systems Cyber Emergency Response Team), BSI oder Fachpresse.

3.2.3 Testphase

Vor dem Einspielen des Patches auf der realen Automatisierungskomponente muss im Vorfeld vom Betreiber überprüft werden, dass der Patch mit dem Zielsystem kompatibel ist und die Sicherheitslücke im vollen Umfang schließt. Weiterhin muss sichergestellt sein, dass ein Ausfall der Automatisierungskomponente ausgeschlossen werden kann. Daher ist vor dem Einspielen des Patches eine Testphase vorgesehen. Innerhalb der Testphase überprüft der Betreiber den Patch auf Kompatibilität mit dem Zielsystem.

3.2.4 Installationsphase

In der Installationsphase muss zunächst festgelegt werden, wer die Patches anweist und wer die Installation durchführt. Der Bearbeiter / Verantwortliche wird in der Dokumentation erfasst. Hinzu kommt, dass die Installationsphase im Vorfeld gründlich geplant sein muss. Ein möglicher Zeitpunkt der Einspielung sollte langfristig mit eingeplant werden. Im Idealfall wird das Einspielen mit z.B. Wartungsarbeiten, bei denen ein Neustart der Anlage erforderlich ist, kombiniert.

3.2.5 Kontrolle und Notfallplan

Nach der Installationsphase muss der Betrieb bzw. die einzelnen Funktionen auf Kompatibilität überprüft werden. Im Idealfall besitzt der Betreiber dafür eine Art Checkliste mit aufgelisteten Konfigurationen, die sukzessiv überprüft werden können. Falls es trotz vorherigem Test des Patches zu einer Störung kommen sollte oder bestimmte Funktionen nicht mehr ordnungsgemäß funktionieren, müssen vordefinierte Maßnahmen ergriffen werden, die in einem Notfallplan vorher festgelegt wurden. Maßnahmen können u.a. die Deinstallation des Patches, das Einspielen eines Backups oder die Wiederherstellung des Gesamtsystems sein. Weiterhin muss kontrolliert werden, ob möglicherweise weitere Systeme durch die Störung betroffen sind. Dazu muss der Betreiber mit der Anlage vertraut sein und das Zusammenspiel einzelner Automatisierungskomponenten kennen.

3.3 Womit?

Für die Durchführung der Tätigkeiten müssen alle relevanten Technologien und Lösungen, die dafür notwendig sind, definiert werden. Im Weiteren müssen die Tools und notwendige Software genauso wie die erforderliche Hardware bekannt sein. Diese Gesichtspunkte können ebenso wie die grundlegenden Konfigurationen den Prinzipien der systemtechnischen Sicherheit entnommen werden. Diese können als organisationsinterne Standards entsprechend entwickelt und über das Sicherheitsmanagement bzw. eine Policy (Annex) vorgegeben werden.

Dabei ist zu berücksichtigen, wie die Aufgaben im Rahmen des derzeitigen Betriebsregimes bereits gelöst werden. Anzustreben ist eine möglichst geringe Änderung des Betriebsregimes, was freilich zwingend die Kenntnisse des bestehenden Betriebs voraussetzt.

3.3.1 Dokumentation

Der Betreiber verwendet für die Erfassung ein geeignetes Datenbankmanagementsystem (DBMS), damit zum einen Änderungen schneller übernommen werden können und zum anderen doppelte Einträge (Redundanzen) vermieden werden.

3.3.2 Testphase

Die reale Umgebung in Form einer virtuellen Umgebung (Verwendung von Virtualisierungssoftware) wird vom Betreiber nachgebaut oder er realisiert die reale Umgebung durch das Vorhandensein funktionaler gleicher Komponenten.

3.3.3 Installationsphase

Wie in der Testphase ist die empfohlene Vorgehensweise bei der Einspielung des Patches, dass zunächst nur Teilkomponenten aktualisiert werden. Die gesamte Aktualisierung wird anschließend sukzessiv fortgeführt. Bei einem redundanten Aufbau ist es sinnvoll, dass nur ein Teilsystem aktualisiert wird. Die Aktualisierung des Teilsystems kann in Teilinstallationen durchgeführt werden.

3.4 Wie (oft)?

Die Prozesse können in unterschiedlichen Notationen definiert sein. Dabei ist insbesondere an den Schnittstellen zwischen den unterschiedlichen Verantwortlichkeiten sicherzustellen, dass die richtigen Informationen und Ergebnisse bereitgestellt werden. In den Verfahren sollten neben den rein verfahrenstechnischen Punkten auch die Aspekte Frequenz und Dauer des Verfahrens und die personellen und finanziellen Ressourcenanforderungen des Verfahrens geregelt

sein. Insbesondere letzteres hilft ungemein, sich und ggf. Entscheidungsträgern die notwendigen Randbedingungen zu verdeutlichen.

Dabei sind auch die spezifischen Gegebenheiten der jeweiligen Umgebung zwingend zu berücksichtigen. Die Workflows unterscheiden sich häufig in Abhängigkeit von den involvierten Systemen / Assets in ihrem Ablauf. Auch die Dauer sowie die Frequenz aller Prozesse hängen von den spezifischen Rahmenbedingungen ab und sind entsprechend zu definieren. Eine solche Rahmenbedingung kann beispielsweise eine Revision oder ein Wartungsfenster sein. Ohne die frühestmögliche Einbeziehung der Betriebsebene dürfte das kaum sinnvoll möglich sein.

Das Patch-Management ist ein regelmäßiger und wiederkehrender Prozess. Das Intervall der Durchführung sollte idealerweise möglichst gering ausfallen, sodass frühzeitig benötigte Patches eingespielt werden können und mögliche Sicherheitsbedrohungen rechtzeitig verhindert werden können.

Bezüglich der Komponenten der Automatisierungstechnik, wie eine speicherprogrammierbare Steuerung (SPS), ist beim Patch-Management zu unterscheiden, ob der Patch-Vorgang im laufenden Betrieb durchgeführt werden kann oder ein Neustart des Systems durchgeführt werden muss. Auf Grund dessen ist es empfehlenswert, dass der Patch-Vorgang bei der nächstmöglichen Gelegenheit durchgeführt werden sollte. Das bringt den Vorteil mit sich, dass die Automatisierungskomponenten nicht unnötig ausgeschaltet werden müssen und somit ein unterbrechungsfreier Betrieb erzielt werden kann. Falls der Aufwand des Patch-Vorganges zu hoch sein sollte (aus wirtschaftlicher oder finanzieller Hinsicht), dann müssen als Alternative „Compensating Controls“ verwendet werden. Darunter zählen z.B. Firewalls, Netzwerksegmentierung oder VPN-Lösungen.

3.5 Nach welchen Regeln?

In allen vorgenannten Schritten ist immer zu beachten, nach welchem Vorgaben- und Regelwerk gearbeitet werden muss. Dabei sind zwei Fälle zu unterscheiden: Liegt bereits ein Regelwerk vor, so wird dieses eingehend betrachtet. Das bedeutet, dass die vorangegangenen Punkte auf dieses Regelwerk hin abgestimmt sein müssen. Ist das nicht der Fall, muss das Regelwerk ggf. angepasst werden, sofern eine Änderung der betrieblichen Strukturen technisch oder organisatorisch nicht möglich ist. Grundlagen für das Regelwerk sollten immer Best Practices sein, wie sie in Form der genannten Standards zur Verfügung stehen.

Zumeist ist das Regelwerk nicht einfach und schon gar nicht schnell anzupassen. Häufig werden dann Ausnahmen vom Regelwerk notwendig. Diese sollten geregelt sein, was in der Policy oder im Managementsystem erfolgen kann. Die Ausnahmen sollten befristet und dokumentiert sowie ein Prozess mitsamt Verantwortlichkeiten definiert sein, wie die Ausnahmen genehmigt werden.

Sollte noch kein entsprechendes Regelwerk bestehen, kann dieses auf Basis des detaillierten Risikobehandlungsplans und der bestehenden Betriebsorganisation erstellt werden.

4 Empfohlene Vorgehensweise

Als Grundlage für die Erstellung eines detaillierten Risikobehandlungsplans sollte immer eine detaillierte Risikoeinschätzung dienen. Die Erkenntnisse und die darauf basierenden Maßnahmen, die festzulegen sind, betreffen eine Vielzahl von Stakeholdern im Unternehmen. Dazu gehören in der Regel mindestens die Verantwortlichen der Governance und des Betriebs, als

auch der Anlagenerrichter und ggf. Dienstleister, die entweder bei der Risikoeinschätzung oder bei der Planung und Umsetzung der Maßnahmen unterstützen.

Eine Workshop-basierte Vorgehensweise ist hierbei zu empfehlen, um diese Menge an Personen effizient und in direkter Abstimmung gemeinsam an den detaillierten Maßnahmen arbeiten zu lassen. Nach einem initialen Resolution-Workshop, in dem die Anforderungen und Rahmenbedingungen an eine Lösung von allen Seiten dargestellt wurden, kann es individuelle Arbeitsphasen der Stakeholder geben, in denen Vorschläge ausgearbeitet werden. Diese müssen in einem abschließenden Solution-Workshop abgestimmt und im detaillierten Risikobehandlungsplan finalisiert werden.

5 Ausblick

Wer seine IT-Sicherheit risikobasiert und betriebsverträglich steuern möchte erhält mit einem detaillierten Risikobehandlungsplan die Möglichkeit dies aus dem Risikomanagement zu tun und hierbei alle Verbesserungen direkt in ein mögliches Sicherheitsmanagementsystem einzubinden.

Die gesamte Ausarbeitung befasste sich mit der Umsetzung in der Automatisierung. Die Nutzung eines Risikobehandlungsplans ist aber auch in allen anderen Branchen zu empfehlen, insbesondere bei der Nutzung eines ISMS, da hier direkte Rückkopplungseffekte im Sinne es kontinuierlichen Verbesserungsprozesses erlangt werden. Die betriebliche Abhängigkeit kann hierbei branchenbedingt deutlich kleiner ausfallen.

Literatur

[Inte15] IEC Internation Electrotechnical Commission: IEC62443-1-1 bis -3-3, IEC Internation Electrotechnical Commission (2015).

[Inte16] IEC International Electrotechnical Commission: IEC 61511-X:2016, IEC International Electrotechnical Commission (2016).

[IsIe13] ISO International Organization for Standardization: ISO/IEC 27001:2013, ISO International Organization for Standardization (2013).

[JaKe09] J. M. Jacka, P. J. Keller: Business Process Mapping Workbook. Improving Customer Satisfaction, John Wiley & Sons Inc. (2009).

[RBKG15] H. Rudolph, A. Brown, M. Klassen, D. Goergen: Technische Sicherheitstests für ICS-Anlagen, Bundesamt für Sicherheit in der Informationstechnik (2015).

[RuGo15] H. Rudolph; D. Goergen: Empfohlene Umsetzung eines Detailed Risk Assessments nach IEC 62443, VDI (2015).

[RuGo16] H. Rudolph; D. Goergen: Security Anforderung an Safety Instrumented Systems (SIS) gemäß dem Standard IEC 61511, WEKA FACHMEDIEN GmbH (2016).

[RuGr12] H. Rudolph; T. Gronenwald: Durchgängiges Sicherheitsmanagement mit Hilfe von zentralen Diensten, Mesago Messe Frankfurt GmbH (2012).