Automation Security Risk Assessment

Vorgehensweisen zur Durchführung von Risikobewertungen

Um Security-Schutzmaßnahmen für die Automatisierungstechnik sinnvoll zu implementieren, wird eine Entscheidungsgrundlage benötigt. Eine Risikoanalyse, die Werte erfasst und ermittelt, kann das leisten. Der Beitrag stellt praktische Herangehensweisen zur Durchführung von Risikoanalysen vor, die eine Auswahl von hinreichenden Schutzmaßnahmen erlaubt.

SCHLAGWÖRTER Risikoanalyse / IT-Sicherheit / Bewertungsmethoden

Automation security – Risk assessment – Methods for risk assessment

In order to be able to implement appropriate security measures for automation systems, it is important to have a sound basis on which to make decisions. Such a basis can be provided by risk analysis, which draws on values in order to assess the threats faced by an automation system. This paper shows a practical approach to carrying out a risk analysis and select essential security measures.

KEYWORDS risk assessment / security / assessment methods

MARKUS RUNDE, BASF
WALTER SPETH, Bayer Technology Services
THOMAS STEFFEN, BASF
CHRISTOPH THIEL, Fachhochschule Bielefeld

Die aktuelle Entwicklung der Automatisierungstechnik nimmt starken Einfluss auf künftige Architekturen eben dieser Systeme. Wesentliche Faktoren dabei sind der hohe Grad an Vernetzung, aber ebenso der steigende Anteil an IT-Komponenten und Lösungen in der Automatisierungstechnik. Ziel sind durchgängige Automatisierungslösungen, die eine Optimierung der Produktionsprozesse erlauben.

Diese zunehmende Durchgängigkeit ermöglicht es jedoch, dass gängige Schwachstellen der IT und somit Bedrohungen aus diesem Umfeld leichter ihren Weg in die Automatisierungstechnik finden. Parallel dazu steigt die Anzahl der Bedrohungen, beispielsweise Malware, denen sich die Automatisierungstechnik stellen muss. [1]

Um der sich stetig ändernden Lage Herr zu werden, sind anwendbare und praktikable Schutzmaßnahmen gegen Bedrohungen erforderlich; beziehungsweise Maßnahmen, um bekannte und unbekannte Schwachstellen zu sichern. Je nach Automatisierungssystem steht hierbei dem Betreiber des Systems ein großes Portfolio an verschiedensten Maßnahmen zur Wahl. Doch aufgrund nicht erfasster Risiken ist gerade die zielgerichtete Auswahl von geeigneten Schutzmaßnahmen erschwert. So bleibt unklar, ob die getroffenen Maßnahmen ausreichend sind. Erst mit einer Erfassung des potenziellen Risikos können zielgerichtet Maßnahmen ergriffen werden. Risikoanalysen sind daher ein wesentlicher Bestandteil einer Automation-Security-Vorgehensweise, wie sie beispielsweise in der VDI-Richtlinie 2182 beschrieben ist [2]. Doch wie sieht eine securitybezogene Risikoanalyse im Umfeld von Automatisierungssystemen aus, und wie werden Risiken bewertet?

Ziel der vorliegenden Arbeit ist es, zwei praktikable Modelle für securitybezogene Risikoanalysen vorzustellen.

1. BEGRIFFE UND NORMATIVE GRUNDLAGE

Tatsächlich finden sich kaum zwei Experten, die sich einig darüber sind, was überhaupt der Begriff *Risiko* umreißt. Wenn selbst der Arbeitskreis, den die International Society for Risk Management zur Begriffsdefinition eingesetzt hat, nach einigen Jahren ohne Ergebnis aufgibt [3], ist Anlass zu Bedacht und Sorgfalt gegeben. Wir folgen einer (zwar ungenauen, aber für die folgenden Betrachtungen ausreichenden Begriffsbildung) und sprechen von Risiko, wenn etwas, das für uns einen Wert darstellt, einer Gefährdung (ungezielt) oder Bedrohung (gezielt) ausgesetzt ist. Somit fließen bei der Bewertung von Risiken die Bewertung der Gefährdungen beziehungsweise Bedrohungen und die Bewertung der Auswirkung auf den für uns wichtigen Wert ein.

Die Beschreibung von Modellen zur Risikoanalyse wird aber ebenso durch den unscharfen Gebrauch zahlreicher Begriffe erschwert. Wir versuchen diese Begriffe weitestgehend entsprechend ihrer Bedeutung in VDI/VDE 2182 [2] und IEC 62443 [4-7] zu verwenden.

Das Durchführen einer securitybezogenen Risikoanalyse bietet natürliche Anknüpfungspunkte zu Vorgehensweisen einer Risikoanalyse im Umfeld der funktionalen Sicherheit (safety) [8-10]. Andererseits müssen Unterschiede berücksichtigt werden: Im Gegensatz zur Sicht der Safety bedeutet aus Sicht der Security ein Schadensereignis, dass ein Angreifer (bewusst und intelligent) mit Hilfe von Schwachstellen in das zu schützende System eindringt. Da sich sein Verhalten nicht vorhersagen lässt, lassen sich Wahrscheinlichkeiten für Angriffe beziehungsweise Bedrohungen a priori nicht vollständig festlegen. Ferner lassen sich aus Sicht der Security nicht einmalig auf Basis einer securitybezogenen Risikoanalyse die Schutzmaßnahmen festlegen, sondern im Laufe der Lebenszeit des Automatisierungssystems muss die Bedrohungslage immer neu bewertet und gegebenenfalls neue Maßnahmen eingeführt werden. Hier sind wiederum die IEC-Reihe 62443 [4-7] und die VDI-Richtlinie 2182 [2] zu erwähnen.

Generelles Ziel der securitybezogenen Risikoanalyse ist es, für den Betrachtungsgegenstand mögliche securitybezogene Gefährdungen und Bedrohungen zu identifizieren und hieraus (ausgehend von der Definition von Schutzzielen) Risiken zu analysieren beziehungsweise zu benennen. In der Welt der Security

werden dabei die Schutzziele der Verfügbarkeit, der Vertraulichkeit, der Integrität und gegebenenfalls weitere Schutzziele separat betrachtet. Diese Unterscheidung ist nicht nur sinnvoll bei der Einschätzung von Bedrohungen, sondern auch bei der Überlegung zu möglichen Angriffsvektoren wie auch bei der Auswahl von Schutzmaßnahmen. Auf Basis einer durchzuführenden Bewertung der securitybezogenen Risiken erfolgt dann die gezielte Auswahl und Umsetzung von Schutzmaßnahmen, die abschließend auf ihre Wirksamkeit überprüft werden. Ist dieser Zyklus abgeschlossen, erfolgt in regelmäßigen und/oder sinnvollen Abständen eine erneute Analyse der möglichen Risiken, um einer möglichen geänderten Bedrohungssituation entgegenzuwirken.

Das Identifizieren von Bedrohungen gehört zu den anspruchsvolleren Aufgaben innerhalb der Durchführung einer Risikoanalyse. Als Einstiegspunkt für diese Aufgabe eignen sich bereits bestehende Listen beziehungsweise Kataloge von mehr oder weniger generischen Bedrohungen. Beispielsweise beschreibt der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnologie eine Reihe von Bedrohungen, die unabhängig vom konkreten Angriffsziel eines Automatisierungssystems in einer Risikoanalyse berücksichtigt und natürlich um weitere ergänzt werden können [11].

Während dieses grundlegende Schema auf Basis der genannten Standards für beide vorgestellten Methoden der Risikoanalyse gilt, gibt es zahlreiche Freiheitsgrade, die dazu führen, dass sich die vorgestellten Methoden doch in verschiedenen Punkten unterscheiden. Dies beginnt bei dem Ausgangspunkt der Risikoanalyse, die entweder das definierte Automatisierungssystem als Ganzes betrachtet (Methode 1, siehe Abschnitt 2.1) oder von einzelnen Komponenten und Assets ausgeht, die dann wiederum zu Teilsystemen zusammengefasst werden (Methode 2, siehe Abschnitt 2.2) und reicht bis zu verschiedenen Arten der Bewertung der Bedrohungen.

2. VORGEHENSWEISEN/ANALYSE-ANSÄTZE

2.1 Methode 1: Systembasierte Vorgehensweise

Die systembasierte Vorgehensweise lässt sich in drei grundsätzliche Phasen gliedern. Zunächst wird das abstrakte Risiko der untersuchten Produktionsanlage ermittelt. Daraus wird im zweiten Schritt der postulierte Schutzbedarf abgeleitet. Im dritten Schritt wird das aktuelle Schutzniveau ermittelt.

Schritt 1: Das abstrakte Risiko der Produktionsanlage leitet sich aus der aktuellen Bedrohungslage und den Auswirkungen eines erfolgreichen Angriffs ab. Diesem Vorgehen liegt folgende Definition des securitybezogenen Risikos zugrunde:

Risiko = Wahrscheinlichkeit des Angriffs • Auswirkungen des erfolgreichen Angriffs

Die Herausforderung besteht darin, dass weder Wahrscheinlichkeit noch Auswirkungen quantitativ ermittelt werden können. Insbesondere die Bedrohungslage ist schwer abzuschätzen und kann beispielsweise die Angriffshäufigkeit im Branchenumfeld oder konkrete Angriffsabsichten (zum Beispiel Ankündigung durch Hackergruppen wie Anonymous) berücksichtigen. Die Bewertung erfolgt in Form einer Bedrohungskennzahl, die in vier Stufen von *niedrig* bis *sehr hoch* reicht.

Zur Einschätzung der Auswirkungen werden bekannte Kennzahlen der Produktionsanlage, wie Wiederbeschaffungswert, Ergebnisbeitrag oder Umweltfolgenabschätzung herangezogen. Diese Kennzahlen werden normiert, gewichtet und zu einer Auswirkungskennzahl zusammengefasst, die ebenfalls in vier Stufen von niedrig bis sehr hoch reicht.

Aus Bedrohungs- und Auswirkungskennzahl leitet sich das abstrakte Risiko anhand des in Bild 1 dargestellten Zusammenhangs ab. Das beschriebene Vorgehen impliziert, dass das abstrakte Risiko eine A-priori-Kenngröße ist, also insbesondere die Erkenntnisse der Risikoanalyse nicht berücksichtigt. Ebenfalls unberücksichtigt bleiben etwaige, vorhandene Schutzmaßnahmen.

Schritt 2: Die Bestimmung des Schutzbedarfs (und damit der Schutzziele) ergibt sich durch eine eineindeutige Abbildung des abstrakten Risikos auf vier Schutzbedarfsniveaus (*target protection level*, siehe Bild 2). Diesem Ansatz liegt folgende, aus der Safety bekannte, Argumentation zugrunde: Je höher das abstrakte Risiko, desto größer muss die Risikoreduktion ausfallen, um das Risiko unter das akzeptable Restrisiko zu reduzieren.

Auch im Bereich Safety wird aus Prozessrisiko ohne Schutzmaßnahmen (hier: Bedrohungskennzahl) und der Folgenabschätzung (hier: Auswirkungskennzahl) die Sicherheitsanforderungsstufe (SIL) (hier: target protection evel) abgeleitet. Die Target Protection Level orientieren sich dabei an den *Security Level* aus der IEC 62443-3-3 [7] und wurden wie folgt festgelegt:

1 | Schutz gegen gewöhnliche, gelegentliche und eher zufällige Angriffsszenarien,
2 | Schutz gegen vorsätzlich durchgeführte Angriffsszenarien, die einfache Hilfsmittel und wenig Ressourcen, durchschnittliche Fähigkeiten und geringe Motivation zum Einsatz bringen,
3 | Schutz gegen vorsätzlich durchgeführte Angriffsszenarien, die hochentwickelte Hilfsmittel und mäßige Ressourcen, leitsystemspezifische Fähigkeiten und mäßige Motivation zum Einsatz bringen.

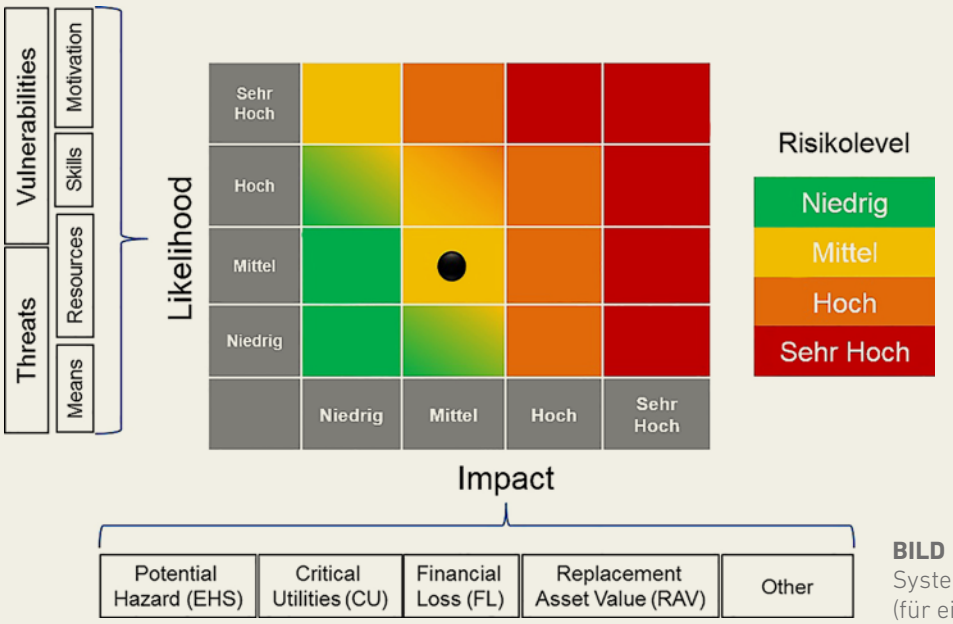

BILD 1: Methode 1 – System-Risikoermittlung (für eine einzelne Anlage)

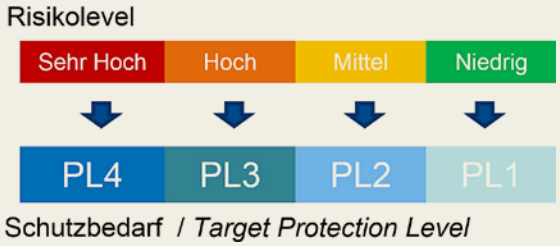

BILD 2: Methode 1 – Zuweisung eines Schutzbedarfs

4 | Schutz gegen vorsätzlich durchgeführte Angriffsszenarien, die hochentwickelte Hilfsmittel und stark erweiterte Ressourcen, leitsystemspezifische Fähigkeiten und hohe Motivation zum Einsatz bringen.

Schritt 3: Die Ermittlung des aktuellen Schutzniveaus erfolgt anhand eines Fragebogens, praktischer Analysen des Automatisierungssystems sowie vorhandener Systemdokumentation. Der Fragebogen enthält zirka 200 Detailfragen, die in folgende acht Kategorien gruppiert sind, die von den sieben *Foundational Requirements* der IEC 62443-3-3 [7] abweichen.

1 | Security Organization (Organisationsstruktur)
2 | Architecture & Integrity (Securityarchitektur)
3 | Remote Access (Fernzugriff)
4 | Process Recovery (Systemsicherung und -wiederherstellung)
5 | Incident Management (Handhabung von Securityvorfällen)
6 | Change Management (Handhabung von Veränderungen)
7 | Awareness & Training (Sensibilisierung und Weiterbildung)
8 | Identity & Access Management (Identitäts- und Zugriffskontrolle)

Die Strukturierung des Fragebogens erleichtert die Auswertung und vermeidet thematische Sprünge beim Ausfüllen. In jeder Kategorie wird zudem zwischen Fragen hinsichtlich technischer Maßnahmen sowie zugehöriger Prozessreife unterschieden. Die Einschätzung der Prozessreife erfolgt anhand des CMMI-Modells [13]. In der Praxis helfen dabei leicht verständliche Fragen, wie „Ist die Durchführung von einer Person abhängig?“, „Gibt es eine Vertreterregelung?“, „Gibt es einen schriftlichen Durchführungsleitfaden?“, „Gibt es zugehörige Schulungen?“, „Gibt es Qualitätssicherungsmaßnahmen?“. Die Prozessreife wird erfasst, weil technische Maßnahmen durch

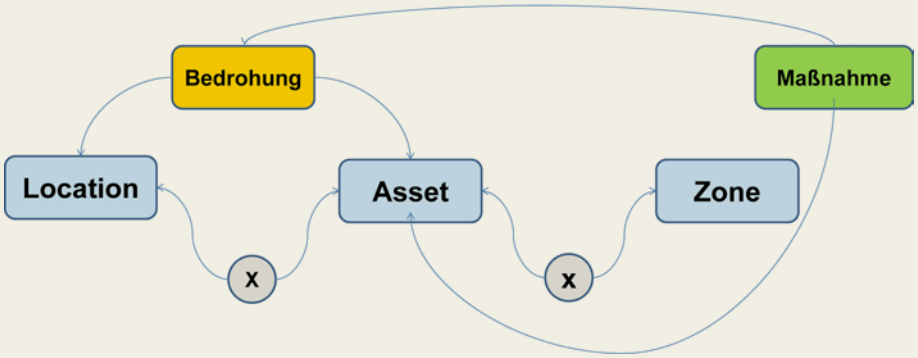

BILD 3: Methode 2: Asset-Risk-Relationship Model (Das Symbol "x" steht hier für N:M-Verknüpfung.)

falsches Nutzerverhalten geschwächt oder gar unwirksam werden können.

Jede Frage ist ferner einem Schutzbedarfsniveau zugeordnet, sodass erkennbar ist, welche Fragen beim Ausfüllen bereits ausgelassen werden dürfen. Zudem wird der Adressat genannt (etwa Betrieb, Systemlieferant) und eine Referenz zur Quelle der Frage angegeben (beispielsweise firmeninterne Vorgabe, IEC Norm).

Im praktischen Teil werden die Firewalls hinsichtlich ihrer Konfiguration, Firmware, Regelwerk und aktiver Datenverbindungen überprüft. Die beiden letztgenannten Aktivitäten werden in Form eines Datenflussdiagramms dokumentiert. Diese Übersicht erleichtert die Klärung mit dem Betrieb, welche Verbindungen beziehungsweise Firewall-Freischaltungen tatsächlich benötigt werden. Sofern betrieblich vertretbar, werden PC und Server einem Schwachstellenscan unterzogen, woraus sich Empfehlungen hinsichtlich Systemhärtung- und Softwareaktualisierungen ableiten lassen.

Abgerundet wird die Ermittlung des Schutzniveaus mit einem Rundgang in Schaltraum und Messwarte, wodurch sich die im Fragebogen getroffenen Aussagen, die Einhaltung von Verfahrensanweisungen und die Aktualität der Systemdokumentation (wie Netzwerkplan oder Komponentenübersicht) stichprobenartig überprüfen lassen.

Report: Nachdem auch der letzte Schritt der systembasierten Risikoanalyse abgeschlossen ist, werden die Ergebnisse in einem Report festgehalten. Darin wird zunächst die Aussage getroffen, ob das in Schritt zwei ermittelte Schutzbedarfsniveau erreicht wurde. Da sich diese Information allein aus dem Fragebogen ableitet, kann zusätzlich angegeben werden, in welchen Kategorien Nachbesserungsbedarf besteht.

Zentrales Element des Reports ist die Schwachstellenliste, die alle erkannten Bedrohungen für das Automatisierungssystem aufführt und hinsichtlich ihrer potenziellen Auswirkung in vier Stufen von niedrig bis sehr hoch bewertet. Diese Bewertung erfolgt im Vier-Augen-Prinzip durch zwei Experten aus unterschiedlichen Securityfachrichtungen. Falls die Schwachstelle durch den Fragebogen aufgedeckt wird, dient die Schutzniveau-Zuordnung der entsprechenden Fragen als Anhaltspunkt. Es fließen aber ebenso Abhängigkeiten verschiedener Befunde in die Bewertung ein („Können zwei Schwachstellen in einer Angriffskette (attack tree) kombiniert werden?"). Alle Schwachstellen werden detailliert beschrieben und Lösungen, samt Implementierungsreihenfolge, vorgeschlagen.

Durch die Analyse des Firewall-Regelwerks konnten zahlreiche, unmittelbar verwertbare Erkenntnisse gewonnen werden. Die zugehörigen Schutzmaßnahmen sind meist kostengünstige und schnell umsetzbare Regelwerksänderungen mit hohem Sicherheitsgewinn.

Die Berücksichtigung der Prozessreife im Fragenkatalog hat das Sicherheitsbewusstsein der beteiligten Betriebsangehörigen erhöht. Zudem lässt sich die Prozessreife oft durch Anpassen betrieblicher Verfahrensanweisungen einfach und kostengünstig verbessern. Positiv hervorzuheben ist ferner, dass sich der Arbeitsaufwand für die systembasierte Risikoanalyse in Grenzen hält. Im Rahmen zweier Pilotanwendungen waren je 100 Mannstunden nötig, von denen lediglich zirka 30 Stunden auf den Produktionsbetrieb entfielen.

Auswirkung	Vertraulichkeit	Integrität	Verfügbarkeit										
			< 5 min	1h	4h	8h	12h	1d	3d	7d	1m	3m	6m
Produktionsausfälle	2	3	1	1	2	2	2	2	2	3	3	3	4
Verstoß gegen Gesetze, Verträge	0	0	0	0	0	0	0	0	0	0	0	0	0
Know-how-Diebstahl	2	0	0	0	0	0	0	0	0	0	0	0	0
Beeinträchtigung der Aufgabenerfüllung	0	0	0	0	0	0	0	1	1	1	2	2	2
Schäden an Mensch und Umwelt	1	3	1	1	2	3	3	3	3	3	3	4	4
Imageschaden	0	0	0	0	4	0	0	0	1	1	2	2	2

BILD 4: Methode 2: Beispiel für die Bestimmung der Kritikalität

Schutzbedarf	Vertraulichkeit	Integrität	Verfügbarkeit										
			< 5 min	1h	4h	8h	12h	1d	3d	7d	1m	3m	6m
Komponente 4711	0	3	0	0	0	0	0	1	1	1	2	2	2

BILD 5: Methode 2: Beispiel für Schutzbedarf einer Komponente

2.2 Methode 2: Asset-basierte Vorgehensweise

Die Asset-basierte Vorgehensweise basiert auf den in Bild 3, hier *Asset-Risk-Relationship Model* genannt, dargestellten Zusammenhängen.

Ein *Asset* bezeichnet dabei ein materielles oder immaterielles Gut, das für den Besitzer oder Eigentümer einen gewissen Wert darstellt. Also gehören Information oder Software ebenso dazu wie Computersysteme, Infrastrukturkomponenten, wie Switches oder Router, oder auch Automatisierungssysteme. An den Assets setzen die Angriffe an, vor denen das Automatisierungssystem geschützt werden muss. Ein materielles Asset wird als *Komponente* bezeichnet. Das weist darauf hin, dass es Teil eines größeren Konstrukts (der Komposition) ist. Ebenso kann es aus Konstituenten bestehen, also seinerseits eine Komposition von Komponenten sein.

Eine *Zone* umfasst Komponenten, die eng mit einander verflochten sind, etwa durch intensiven und vielfältigen Kommunikationsbedarf, und die gemeinsam eine Funktion ausführen. Daher ist *funktionale Gruppe* eine äquivalente Bezeichnung für eine Zone. In der realen Welt können die Komponenten einer Zone durchaus in verschiedenen Lokationen verbaut sein. In erster Näherung können die Ebenen der Automatisierungspyramide nach ISA 95 [14] als Zonen verstanden werden.

Eine *Lokation* (Örtlichkeit) wird hinsichtlich der physischen Zugangsmöglichkeiten betrachtet. In einer Lokation können viele Assets beziehungsweise Komponenten verortet sein, die zu einer oder auch mehreren Zonen gehören.

Bedrohungen im Kontext des Modells der Asset-basierten Vorgehensweise der Risikoanalyse beziehen sich auf ein oder mehrere Assets und werden als Umstände oder Ereignisse verstanden, die (einzelne oder mehrere) Schutzziele des oder der Assets verletzen und eine beschreibbare *Auswirkung* haben, das heißt zu einem *Schaden* führen können. Jeder Bedrohung werden zunächst die betroffenen Schutzziele zugeordnet. Die Wahrscheinlichkeit für das Eintreten eines Schadens wird nicht differenziert betrachtet, sondern es wird grundsätzlich angenommen, dass jede Bedrohung mit absoluter Sicherheit (also Eintrittswahrscheinlichkeit 100%) zu einem Schadensereignis führen wird. Dies entspricht der Vorstellung, dass ein denkbarer Angriff tatsächlich früher oder später durchgeführt werden wird.

Statt der Bewertung der Wahrscheinlichkeit ordnen wir einer Bedrohung ein Gewicht auf einer ganzzahligen Skala von 0 bis 4 zu. Dieses Gewicht beschreibt, wie *leicht* ein entsprechender Angriff durchgeführt werden kann. Dies hängt natürlich vom Angreifer ab, der daher übergreifend für die Risikoanalyse hinsichtlich seiner Motivationsstärke, seiner Fähigkeiten wie auch seiner Ressourcen (analog zu IEC 62443) eingeschätzt wird. Ebenso wird die *Exponiertheit* der von der konkreten Bedrohung betroffenen Komponente(n), das heißt wie einfach der Zugang zur Komponente ist, berücksichtigt: Eine direkte Verbindung der Komponente zum Internet, eine Isolation (air gap), ein Passwort-Schutz spielen hier auf der logischen Seite ebenso eine Rolle wie Autostart-Laufwerke oder zugängliche USB-Ports auf der physikalischen.

Nicht jedes Asset muss in gleicher Weise geschützt werden und nicht alle Schutzmaßnahmen können sofort finanziert und implementiert werden. Um eine sinnvolle Rangfolge zu erstellen, ist die Betrachtung

der direkten oder indirekten Auswirkungen, (Produktionsausfälle, Verstoß gegen Gesetze oder Verträge, Know-how-Diebstahl, Beeinträchtigung der Aufgabenerfüllung, Schäden an Mensch und Umwelt, Imageschaden), die die Kompromittierung einer Komponente mit sich bringen kann, wichtig. Es ist sinnvoll, diese Kritikalität vor dem Hintergrund jedes einzelnen Schutzzieles separat zu betrachten, in Bild 4 beispielsweise die Spalten Vertraulichkeit, Integrität und Verfügbarkeit. So mag die Sabotage eines Assets einen nicht hinzunehmenden Ausfall der Verfügbarkeit bedeuten, das Ausspionieren, also die Verletzung der Vertraulichkeit, jedoch nicht. Die *Kritikalität* wird jedem Asset zugeordnet. Als mögliche Werte für die Kritikalität vergeben wir die ganzzahligen Werte 0 (geringe Auswirkung bei Kompromittierung des Schutzzieles) bis 4 (massive/existenzielle Auswirkung bei Kompromittierung des Schutzzieles). Basierend auf der Definition der Zonen sollten alle Komponenten einer Zone die gleiche Kritikalität haben, sodass wir auch von der *Kritikalität der Zone* sprechen.

Der *Schutzbedarf* einer Komponente innerhalb einer Zone leitet sich aus der Kritikalität der Zone und der Exponiertheit der Komponente ab. Der Schutzbedarf wird wie die Kritikalität separat für jedes Schutzziel festgelegt, siehe Bild 5. Entsprechend entstammen die einzelnen Werte einer ganzzahligen Skala von 0 bis 4.

Im Gegensatz zur sonst üblichen Betrachtungsweise, siehe [12], verstehen wir Schutzbedarf nicht als A-priori-Wert, sondern berücksichtigen bereits umgesetzte *Maßnahmen* (zur risk mitigation oder als compensating control). Eine Maßnahme kann sich auf ein oder mehrere Assets und eine oder mehrere Bedrohungen (hinsichtlich Kritikalität und Exponiertheit) auswirken und kann in ihrem Reifegrad je Schutzziel auf einer Skala von 0 bis 4 gewertet werden. In diesem Sinne reduzieren Maßnahmen den Schutzbedarf.

Ein *Risiko* kann nun als Diskrepanz zwischen aktuellem Schutzbedarf und vorhandenen Bedrohungen betrachtet werden: Es gilt, unter allen Bedrohungen, denen Assets in Lokationen ausgesetzt sein können, je Schutzziel zu bewerten, inwieweit der Schutzbedarf des Assets überzogen wird. Aus dem Schutzbedarf, der Kritikalität und Exponiertheit kann basierend auf den dargestellten Zusammenhängen die Berechnung der Risikowerte erfolgen. Folgende Werte sind vorgesehen: 0 (kein oder geringes Risiko), I, II, III und IV (existenzielles Risiko).

Soll das Risiko kompensiert werden, sind weitere Maßnahmen auszuwählen, die – wiederum bezogen auf die einzelnen Schutzziele – den Bedrohungen entgegenwirken und in ihrer summarischen Wirkung die Schutzziele hinreichend sichern. Sind zu den Maßnahmen Kosten ausgewiesen, ergibt sich in Ihrer Auswahl eine entsprechende Planung. Auch das ist bereits in der VDI-Norm [2] vorgesehen.

Die Durchführung der vorgestellten Methode inklusive der Berechnungen kann leicht durch einfache Werkzeuge, wie zum Beispiel Tabellenkalkulationen, unterstützt werden. Zudem bietet es sich an, bereits vorab Kataloge von Bedrohungen und möglichen Maßnahmen zu erstellen, aus denen bei einer konkreten Analyse entsprechend ausgewählt werden kann.

REFERENZEN

[1] Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2015, 2015

[2] VDI/VDE 2182-1: Informationssicherheit in der industriellen Automatisierung – Allgemeines Vorgehensmodell. Beuth 2011, http://www.beuth.de

[3] *Talabis, M., Martin, J.*: Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis. Syngress 2015

[4] IEC 62443-1-1: Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models. IEC 2009

[5] IEC 62443-2-1: Security for industrial automation and control systems – Requirements for an IACS Security Management Control Systems. IEC 2012

[6] IEC 62443-3-2: Security for Industrial Automation and Control Systems – Security Risk Assessment and System Design. IEC 2013

[7] IEC 62443-3-3: Security for Industrial Automation and Control Systems, System Security Requirements and Security Levels. IEC 2013

[8] IEC 60812 Ed. 2.0: Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA). IEC 2006

[9] IEC 61025 Ed. 2.0: Fault Tree Analysis (FTA). IEC 2006

[10] IEC 61882: Hazard and operability studies (HAZOP studies) – Application guide. IEC 2001

[11] *Langner, R.*: Robust Control System Networks. Momentum Press 2011

[12] BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise" Version 2.0. Bundesamt für Sicherheit in der Informationstechnik 2008

[13] CMMI-Capability Model (http://cmmiinstitute.com), Aufruf am 14.12.2015

[14] ANSI/ISA-95.00.01: Enterprise-Control System Integration Part 1: Models and Terminology. ANSI 2000

ZUSAMMENFASSUNG UND FAZIT

Risikoanalysen sind unerlässlich, um festzustellen, ob ein erforderliches Sicherheitsniveau erreicht wird und um die Angemessenheit von Schutzmaßnahmen zu bewerten. Zahlreiche Standards fordern die Durchführung von Risikoanalysen, erlauben aber bei der konkreten Gestaltung einer Risikoanalyse zum Teil große Freiheitsgrade. Im Beitrag wurden zwei in der Praxis erstellte und erprobte Methoden zur Durchführung von Risikoanalysen vorgestellt, die das Spektrum der Freiheitsgrade verdeutlichen können. Unabhängig von der jeweiligen Methode muss jedoch betont werden, dass die Ergebnisse jeder Risikoanalyse letztendlich von einzelnen Interpretationen und Bewertungen von Menschen abhängen, die (idealerweise) als Experten entweder bei den Vorgaben der Methode oder bei den Schritten im Rahmen der Durchführung einer Methode ihre individuellen Erfahrungen und Einschätzungen mit einfließen lassen.

MANUSKRIPTEINGANG
15.12.2015
Im Peer-Review-Verfahren begutachtet

AUTOREN

Dr.-Ing. **MARKUS RUNDE** (geb. 1984), ist Mitglied des NAMUR-Arbeitskreises 4.18 „Automation Security“. Er hat Elektro- und Informationstechnik an der Hochschule Hannover studiert. Die Promotion erfolgte 2014 an der Otto-von-Guericke Universität in Magdeburg im Themenfeld der integrierten Security-Maßnahmen für Automatisierungskomponenten. Sein aktuelles Tätigkeitsfeld bei der BASF SE in Ludwigshafen umfasst neben der Projektbetreuung von PLS-Migrationen deren Automation Security sowie Kommunikationstechnologien.

BASF SE, GTG/ED – DCS Project Support and Advanced Basic Automation,
Carl-Bosch-Str. 38, D-67056 Ludwigshafen,
Tel. +49 (0) 621 609 89 11,
E-Mail: markus.runde@basf.com

Dr. **WALTER SPETH** (geb. 1959), ist Mitglied des NAMUR-Arbeitskreises 4.18 „Automation Security“. Nach dem Studium der Physik mit abschließender Promotion auf dem Feld der Teilchenphysik folgten Tätigkeiten als Berater, Abteilungsleiter und Geschäftsführer in der IT-Branche mit Schwerpunkt Security und Biometrie. Seine derzeitigen Aufgabenfelder bei Bayer Technology Services sind: Produktschutz durch Track-und-Trace-Lösungen für die Pharma-Branche, Schwachstellenanalyse für industrielle Produktionsanlagen hinsichtlich Cyber-Angriffen und Software-Entwicklungsstrategien für sicheren Code.

Dr.-Ing. **THOMAS STEFFEN** (geb. 1983) hat Informationstechnik an der TU Kaiserslautern studiert und 2013 dort promoviert. In seiner Dissertation beschäftigte er sich mit drahtlos vernetzen Regelungssystemen. Derzeit arbeitet er im Fachzentrum für Automatisierungstechnik der BASF SE in Ludwigshafen, wo er in den Arbeitsgebieten Technologieentwicklung, Qualitätssicherung und Automation Security für Prozessleitsysteme tätig ist.

Prof. Dr. **CHRISTOPH THIEL** (geb. 1968) ist Professor für sichere und zuverlässige Softwaresysteme am Campus Minden der Fachhochschule Bielefeld. Zuvor war er in verschiedenen Unternehmen und Organisationen in der anwendungsnahen Forschung und Beratung mit den Schwerpunkten Sicherheit und Datenschutz tätig. Seine aktuellen Forschungsinteressen liegen auf den Gebieten Sicherheit industrieller Produktionsanlagen, Entwicklung sicherer und zuverlässiger Software und Sicherheitsmanagement.