atp magazin

SONDERDRUCK

Transforming Automation
Ausgabe 11-12 2018

Organisation der IT-Sicherheit in der Produktion

In zehn Schritten zur sicheren Produktionsanlage

Der folgende Beitrag befasst sich mit der IT-Sicherheit von Produktionsanlagen aus Betreibersicht. Hierbei liegt der Fokus auf den organisatorischen Aspekten der IT-Sicherheit. In einer Bestandsaufnahme werden zunächst die Probleme herausgearbeitet, die entstehen, sofern sich eine Organisation im Wesentlichen auf technische Aspekte der IT-Sicherheit konzentriert. Daraus wird die Notwendigkeit organisatorischer Maßnahmen abgeleitet. Eine Betrachtung von Normen und Standards, die sich mit den organisatorischen Aspekten der IT-Sicherheit in der Produktion befassen, liefert das Grundgerüst für die Ableitung eines Maßnahmenplans. Der daraus resultierende 10-Punkte-Plan zur Umsetzung der IT-Sicherheit in der Produktion schließt den Beitrag ab.

SCHLAGWÖRTER IT-Sicherheit / Organisatorische Aspekte / Vorgehensmodell

Organizational aspects of IT security in production – Ten steps towards a secure production plant

This article deals with the IT security of production plants from the operator‘s point of view. The focus is on the organizational aspects of IT security. The first step is to identify the problems that arise when an organization focuses essentially on technical aspects of IT security. Conclusions are drawn about the necessary organizational measures. An examination of regulations and standards that deal with the organizational aspects of IT security in production provides the basis for formulating an action plan. The 10-point plan for the implementation of IT security in production concludes the contribution.

KEYWORDS IT security / organizational aspects / procedural model

PEER ReView 31.07.2018

KARL-HEINZ NIEMANN, Hochschule Hannover

Die Bedrohungen in Bezug auf die IT-Sicherheit von Produktionsanlagen sind in den letzten Jahren angestiegen. Dabei erreicht die Schadenshöhe einzelner Vorfälle mittlerweile beachtliche Ausmaße. So spricht die Firma Maersk in Ihrem Finanzbericht für das zweite Quartal 2017 [1] von einem erwarteten Schaden in Höhe von 200 bis 300 Mio. US-Dollar, durch einen Cyber-Vorfall, der den Logistikteil des Unternehmens weiterstgehend lahmgelegt hatte. Das Unternehmen musste in kürzester Zeit 45 000 Client-Rechner und 400 Server neu installieren [2]. Laut [3] belaufen sich die durchschnittlichen Kosten für einen Cyber-Sicherheitsvorfall für ein kleineres oder mittleres Unternehmen (KMU) auf 60 000 Euro und für ein Großunternehmen auf 1,12 Mio. Euro.

Neben der Schadenshöhe erreicht auch die Schadenhäufigkeit ein hohes Ausmaß. In der Cyber-Sicherheitsumfrage 2017 des BSI [4] gaben 70 % der befragten Unternehmen an, im Jahr 2016 oder 2017 Opfer von Cyber-Angriffen gewesen zu sein. In der Hälfte der Fälle waren die Angreifer erfolgreich. Jeder zweite Betrieb (51 %) gab zudem an, dass es zu Produktions- beziehungsweise Betriebsausfällen gekommen sei.

Neben technischen Maßnahmen im Produktionsbereich (Abschottung, Segmentierung, Schutz gegen Schadsoftware) sind auch organisatorische und Ausbildungsaspekte für das Personal zu beachten. Immer mehr Angreifer dringen über social Engineering in die Kommunikationsnetze von Unternehmen vor. Social Engineering ist gemäß [5] „eine Methode, um unberechtigten Zugang zu Informationen oder IT-Systemen durch ‚Aushorchen' zu erlangen. Beim Social Engineering werden menschliche Eigenschaften wie beispielsweise Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt."

Das BSI klassifiziert in [6] Social Engineering und Phishing als Bedrohung Nr. 1 für industrielle Automatisierungssysteme. Für die kritische Infrastruktur der Vereinigten Staaten gibt das National Cybersecurity and Communications Integration Center Social Engineering, (Spear Phishing) als häufigste bekannte Angriffsursache an [7]. Auch im Kontext von Industrie 4.0 werden die Rolle des Menschen [8] und die Notwendigkeit für Ausbildung des Personals und von Verfahrensanweisungen in Bezug auf die IT-Sicherheit betont.

Zusammenfassend lässt sich festhalten, dass die Ausbildung des Personals sowie die Etablierung organisatorischer Prozesse, neben den technischen Maßnahmen, ein wesentlicher Baustein für die IT-Sicherheit in der Produktion sind.

1. PROBLEMBESCHREIBUNG IT-SICHERHEIT IN DER PRODUKTION

Das folgende Kapitel gibt eine Bestandsaufnahme der Ist-Situtation und der damit verbundenen Probleme, so wie man sie in vielen kleineren und mittleren Unternehmen vorfindet, wieder. Hierbei werden exemplarisch zwei ausgewählte Punkte, die Organisation der IT-Sicherheit sowie technische Maßnahmen im Detail betrachtet, da diese erfahrungsgemäß ein häufiges Problem darstellen. Das Dokument fokussiert dabei auf den Produktionsbereich. In den gängigen Normen, zum Beispiel der DIN ISO/IEC 27001 [9] wird in der Regel der Begriff Informationssicherheit verwendet. Veröffentlichungen im Bereich der Automatisierungstechnik verwenden oft den Begriff der IT-Sicherheit oder der Cyber-Security. Auf Grund des Bezuges zur Automatisierungstechnik verwendet dieser Beitrag daher den Begriff IT-Sicherheit.

1.1 Organisation der IT-Sicherheit

Die Beherrschung der IT-Sicherheit im Produktionsbereich stellt gerade kleine und mittlere Unternehmen vor neue Herausforderungen. Während die IT-Sicherheit im Office-Bereich in der Regel etabliert ist, sind die Verantwortlichkeiten im Produktionsbereich oft nicht oder nur unzureichend geregelt. Bild 1 zeigt auf der linken Seite das IT-Sicherheitsmanagement eines fiktiven Unternehmens, bei dem der Produktionsbereich nicht in das IT-Sicherheitsmanagement des Unternehmens integriert ist. Der rechte Teil von Bild 1 wird in Kapitel 4 diskutiert werden.

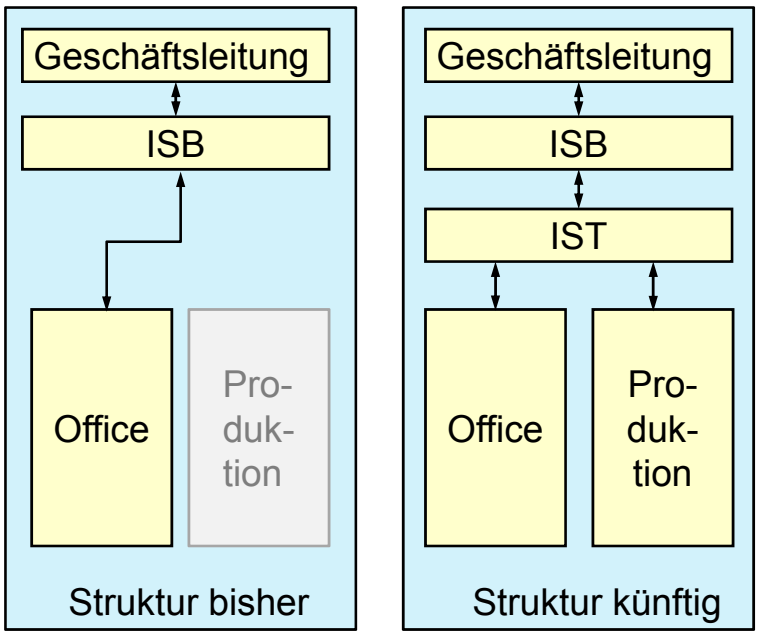

BILD 1: Organisation der IT-Sicherheit bisher und künftig

Die Situation des fiktiven Unternehmens stellt sich wie folgt dar:

- Der Informationssicherheitsbeauftrage (ISB) fühlt sich im Wesentlichen für den Office-Bereich zuständig.
- Die Prozesse für den Office-Bereich sind etabliert und Standardprozesse sind definiert.
- Die Zuständigkeit für den Produktionsbereich ist nicht explizit definiert oder die verantwortliche Person ist nicht in die Organisationsstruktur der IT-Sicherheit eingebunden.
- Im Produktionsbereich ist keine klare Verantwortlichkeit für die IT-Sicherheit definiert. Prozesse sind nicht beschrieben.
- Die IT-Sicherheitsprozesse im Office-Bereich und im Produktionsbereich sind allenfalls getrennt organisiert aber nicht aufeinander abgestimmt.
- Die Lage ist teilweise von einem gewissen gegenseitigen Unverständnis für die Anforderungen des Office- und Produktionsbereiches geprägt.

Die beschriebene Organisationsform führt zu Defiziten für die IT-Sicherheit im Produktionsbereich, da sich viele Aspekte der IT-Sicherheit nicht eindeutig einem der beiden Bereiche zuordnen lassen. Siehe hierzu auch [10]. Da im Kontext von Industrie 4.0 mit einem weiteren Zusammenwachsen der Kommunikationsarchitekturen innerhalb und außerhalb des Unternehmens zu rechnen ist [11], werden die Auswirkungen der beschriebenen Situation noch weitreichender werden.

1.2 Fokus auf technische Maßnahmen

Ein standardisiertes Vorgehen für die IT-Sicherheit in der Produktion ist der so genannte Defense-in-Depth-Ansatz [12]. Dieses Vorgehen beschreibt die Kombination verschiedener Schutzmaßnahmen. Im Fokus steht dabei ein gestufter Schutz des Perimeters (Abschottung nach Außen) in Verbindung mit weiteren Schutzmaßnahmen in Inneren. Hierzu zählen unter anderem Abschottung des Netzwerkes durch Firewalls, Einrichtung von demilitarisierten Zonen, Unterteilung des Netzwerkes in Zonen und Abschottung dieser Zonen, Schutz gegen Schadsoftware. Eine detaillierte Beschreibung dieses Vorgehens findet man in [13].

Bild 2 zeigt die im Rahmen des Defense-in-Depth-Konzeptes gebildeten Zonen und die Abschottung der Zonen durch Firewalls. Ziel der Abschottung ist es, das Vordringen von Angreifern in die nächste Zone zu verhindern oder zumindest zu erschweren. Bei der Bewertung dieses Konzeptes sind allerdings auch Innentäter zu berücksichtigen. Innentäter arbeiten innerhalb der jeweiligen Zone und haben so gegebenenfalls direkten Zugriff auf die Assets in dieser Zone. Laut einer Studie des SANS-Instituts sind 25 % der Angriffe auf Beschäftigte und 16 % auf Service-Provider zurückzuführen [14]. Das heißt, 41 % der Fälle sind in Summe auf Innentäter zurückzuführen.

Eine Abwehr von Innentätern ist nicht durch eine Abschottung der Anlage zu erreichen, sondern eher

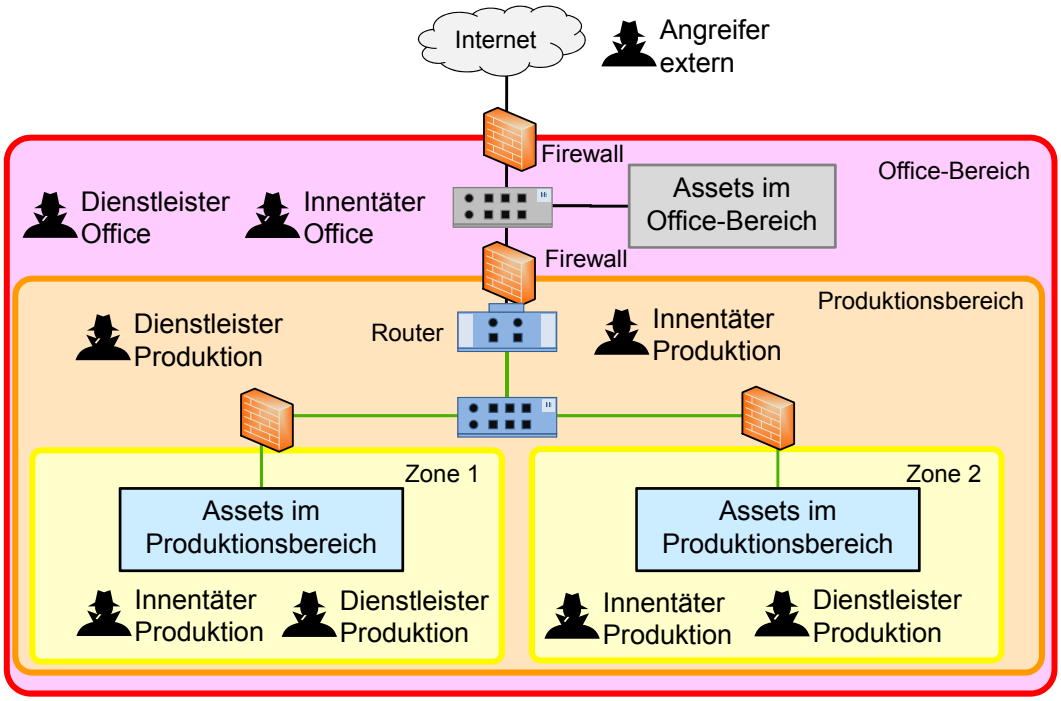

BILD 2: Defense in Depth und mögliche Angreifer

durch organisatorische und technische Maßnahmen innerhalb der jeweiligen Zone. Dies zeigt auch ein Vorfall aus dem Kernkraftwerk Gundremmingen, bei dem eine Schadsoftware auf einem vollkommen isoliert aufgebauten Rechner gefunden wurde [15]. Auch die Empfehlungen des BSI zu Innentätern [16] zielen im Wesentlichen auf organisatorische Maßnahmen (zum Beispiel Vorschreiben von Policies, Identitäts- und Rechtemanagement).

1.3 Schlussfolgerungen aus der Problembeschreibung

Die beschriebene Situation beleuchtet nur zwei ausgewählte Aspekte der IT-Sicherheit in der Produktion. Dennoch erlaubt die Beschreibung die Schlussfolgerung, dass nur durch eine Kombination von technischen und organisatorischen Maßnahmen ein wirksamer Schutz gegen Cyber-Angriffe im Produktionsbereich über ein integriertes Vorgehensmodell erreicht werden kann [17]. Ein alleiniger Blick auf technische Maßnahmen reicht nicht aus. Einen ersten Eindruck über den eigenen Stand von technischen und organisatorischen Maßnahmen im Produktionsbereich kann über einen Quick Check [18] gewinnen. Im Rahmen dieses Quick-Checks werden sowohl technische als auch organisatorische Aspekte in einem Fragebogen erfasst, anschließend bewertet und der Status ermittelt. Einen stark vereinfachten Fragebogen für eine erste Statusaufnahme liefert auch der VDMA [19].

2. NORMEN UND LEITLINIEN ZUR ORGANISATORISCHEN ASPEKTEN DER IT-SICHERHEIT IN DER PRODUKTION

Im Folgenden werden Normen und Leitlinien betrachtet, welche Hinweise für die Etablierung eines Organisationsmodells für die IT-Sicherheit geben. In der Regel wird hier von einem Information Security Management System (ISMS) gesprochen.

2.1 Normreihe ISO 27000

Die Normreihe ISO 27000 kann als Basisnorm für die IT-Sicherheit angesehen werden. Die hier definierten Modelle und Vorgehensweisen finden sich auch in abgewandelter Form in den anderen Normen und Richtlinien zur IT-Sicherheit wieder. Die Norm ISO 27002 [20] bietet einen Leitfaden für das Informationssicherheitsmanagement. Zusätzlich liefert die Norm ISO TR 27019 [21] einen Leitfaden für das Informationssicherheitsmanagement für Steuerungssysteme in der

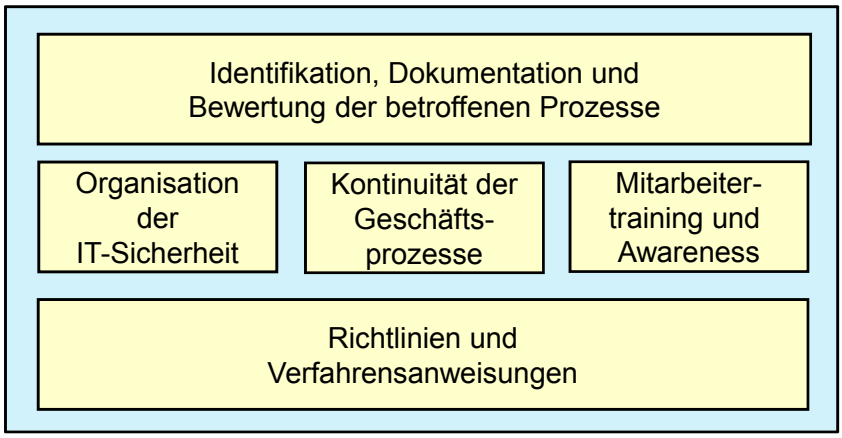

BILD 3: Bestandteile der IEC 62443-2-1

Energieversorgung. Die Normreihe ist ausgesprochen umfassend und wird von Automatisierungstechnikern oft als komplex empfunden. Ein Einstieg in die ISO-27000-Reihe wird daher zunächst über entsprechende Lehrbücher [22] und nicht über die Norm selber empfohlen.

Die Normreihe ISO 27000 fokussiert nicht auf einen speziellen Anwendungsbereich, hat sich aber insbesondere im Office-Bereich stark etabliert. Daher ist sie vielen Informationssicherheitsbeauftragten bekannt und es besteht häufig der Wunsch des ISB, neben dem Office-Bereich, auch den Automatisierungsbereich nach der Normreihe ISO 27000 abzusichern. Viele der Vorgehensweisen lassen sich ebenfalls auf die Automatisierungstechnik übertragen. Allerdings steht mit der Normreihe IEC 62443 ein speziell auf die Automatisierungstechnik zugeschnittener Standard zur Verfügung, der viele spezielle Aspekte der Automatisierungstechnik (hohe Verfügbarkeit, eingeschränkte Möglichkeiten zum Patch-Management Remote Service) zusätzlich berücksichtigt.

2.2 IT-Grundschutz des BSI

Das Bundesamt für Sicherheit in der Informationstechnik bietet mit dem IT-Grundschutz ein systematisches Vorgehensmodell für die Ermittlung und Umsetzung von IT-Sicherheitsmaßnahmen für die Informationstechnik in Unternehmen. In [23] beschreibt das BSI das Managementsystem zur Implementierung des BSI-Grundschutzes. Ursprünglich zielte der BSI-Grundschutz auf den Office-Bereich eines Unternehmens. Mit dem Anfang 2018 veröffentlichten IT-Grundschutzkompendium [24] hat das BSI einen gut strukturieren und verständlichen Nachfolger für die IT-Grundschutzkataloge geschaffen. Hier werden nun auch Themen wie zum Beispiel Virtualisierung, Cloud-Services und industrielle IT behandelt.

2.3 Normreihe IEC 62443

Die Normreihe IEC 62443 berücksichtigt speziell die Automatisierungstechnik. Auch wenn einige Teile bisher lediglich als Entwurf vorliegen, bietet Sie dennoch schon heute einen umfassenden Einstieg in die IT-Sicherheit in der Automation. Zur Zeit liegt der Umfang aller Normteile bei zirka 1200 Seiten. Die Quellen [25] und [26] liefern einen Einstieg in die Normreihe.

Im Weiteren werden lediglich die Teile der Normreihe IEC 62443 betrachtet, die sich mit organisatorischen Aspekten der IT-Sicherheit in der Automation befassen. Der Normentwurf IEC 62443-2-1 [27] beschreibt die organisatorische Basis für den Aufbau eines ISMS für den Produktionsbereich, das in dieser Norm „Industrial Automation Control System Security Management System“ (IACS-SMS) genannt wird.

Bild 3 zeigt die wesentlichen Aspekte der IEC 62443-2-1. Übergreifend werden zunächst die betroffenen Prozesse identifiziert, bewertet und dokumentiert. Dann werden insbesondere die Organisation der IT-Sicherheit, die Kontinuität der Geschäftsprozesse und die Einbindung des Personals betrachtet. Daraus leiten sich dann Richtlinien und Verfahrensanweisungen ab.

Der Normentwurf IEC TR 62443-2-3 [28] befasst sich mit der Organisation des Patch-Managements für Automatisierungssysteme. Die Teile IEC 62443-2-4 [29] beziehungsweise die deutsche Fassung DIN IEC 62443-2-4-100 [30] befassen sich mit den Anforderungen an das IT-Sicherheitsmanagement von Dienstleistern für industrielle Automatisierungssysteme. Weiterhin ist die DIN EN 62443-3-2 [31] zu nennen, die sich mit der Risikoanalyse und dem Systemdesign befasst sowie

die DIN IEC 62443-3-3 [32], die sich mit Systemanforderungen zur IT-Sicherheit und Security-Level befasst.

2.4 Nationale Standards und Richtlinien

Die VdS-Richtlinie 3473 [33] ist auf kleine und mittlere Unternehmen zugeschnitten und beschreibt in einer kompakten Form die Anforderungen an ein ISMS. Diese Anforderungen sind zunächst generisch ohne spezifischen Anwendungsbezug beschrieben. Für die Automatisierungstechnik werden dann ergänzende Anforderungen in der VdS 10020 [34] definiert. Beide Normen sind gemeinsam zu betrachten. Die VdS-Richtlinien beschreiben die Anforderungen in einer klaren und spezifischen Form, sodass daraus einfach entsprechende Handlungsanweisungen abzuleiten sind. Neben technischen werden auch organisatorische Aspekte abgebildet.

Neben den bisher beschriebenen Normen und Richtlinien bieten verschiedene Verbände und Organisationen Leitfäden für Betreiber an. So sind hier die Dokumente des Bitkom [35], des VDMA [26, 36] zu nennen. Auch die VDI 2182 Blatt 1 [37] sowie die folgenden Teile beschreiben detailliert die organisatorischen Maßnahmen für die Umsetzung der IT-Sicherheit im Produktionsbereich. Hierbei geht die Norm auf die Rollen Hersteller, Integrator und Betreiber ein. Bezüglich der Prozessindustrie sind die Namur-Dokumente NA 115 [38] und NE 153 [39] zu nennen.

3. IN ZEHN SCHRITTEN ZUR IT-SICHERHEIT IN DER PRODUKTION

Die vorangehenden Kapitel haben die Notwendigkeit organisatorischer Maßnahmen belegt und die zu Grunde liegenden Normen und Richtlinien beschrieben. In diesem Kapitel folgt nun ein Vorschlag, um in zehn Schritten zu einer sicheren Produktionsanlage zu kommen. Die zehn Punkte sind als übersichtliche Zusammenfassung der bisher beschriebenen Literatur zu sehen. Die VdS 3473 [33] verfügt über eine ähnliche Struktur. Es ist zu beachten, dass diese zehn Punkte einen Überblick über die zu adressierenden Themengebiete liefern. Diese ersetzen jedoch keine detaillierte Analyse der Einzelaspekte.

Bild 4 zeigt die erforderlichen zehn Schritte. Es wurde bereits beschrieben, dass viele Unternehmen den Schwerpunkt auf technische Maßnahmen (Schritte 6 und 7) legen. Die Klassifizierung der Aufgaben in Bild 4 in „Fokus Technik“ und „oft vernachlässigt“ ist eine persönliche Einschätzung des Autors, die er in verschiedenen Industrie-Projekten gewonnen hat. Im Weiteren werden hier die zusätzlich erforderlichen Schritte betrachtet.

Oft vernachlässigt	1. Management Commitment 2. Organisation der Zuständigkeiten und Prozesse 3. Leitlinie/Richtlinie 4. Personal 5. Wissen
Fokus Technik	6. Identifizieren, Bewerten und Schützen der Assets a) Automatisierungssysteme b) Netzwerke 7. Externer Zugriff
Oft vernachlässigt	8. Datensicherung 9. Störungen und Ausfälle 10. IT-Sicherheitsvorfälle

BILD 4: Die 10 Schritte zur sicheren Produktionsanlage

1. Management Commitment

Der IT-Sicherheitsprozess sollte als Top-Down-Prozess initiiert werden. Aufgabe der Geschäftsleitung wäre, die entsprechenden Verantwortlichkeiten zu definieren, die IT-Sicherheitsstrategie für Office- und Produktionsbereich schriftlich darzustellen und den Beschäftigten und Dienstleistern zur Kenntnis zu geben. Das BSI forderte schon im Jahr 2015 dazu auf, Cyber-Security in der Produktion zur Chefsache zu machen [40].

2. Organisation der Zuständigkeiten und Prozesse: Die Verantwortlichkeiten für den IT-Sicherheitsprozess sind zu benennen.

Der Informationssicherheitsbeauftragte (ISB) sollte die Gesamtverantwortung für den Office- und Produktionsbereich übernehmen. Gegebenenfalls ist fachliche Unterstützung hinzuzuziehen. Das Informationssicherheitsteam (IST) sollte gemäß Bild 1 aus Verantwortlichen aus dem Office- und Produktionsbereich zusammengesetzt sein. Das IST wäre mit der Umsetzung der IT-Sicherheitsstrategie zu beauftragen und dient ferner als Anlaufstelle bei Störungen oder Ausfällen. Die Rollenbeschreibung eines ISB findet sich zum Beispiel in [41].

3. Leitlinien/Richtlinien

Das Personal muss durch Leitlinien/Richtlinien darüber informiert werden, welche Handlungen zulässig und welche nicht zulässig sind. Hierbei können für den Office-Bereich und den Produktionsbereich unterschiedliche Richtlinien gelten. In solchen Richtlinien sind zum Beispiel folgende Fragen zu klären:

- Nutzung mobiler Datenträger
- Anschluss von Geräten an das Produktionsnetzwerk
- Nutzung persönlicher Geräte (BYOD)
- Weitergaben von Passworten
- Regelungen bei Abwesenheit von Mitarbeitern
- Regelungen für externes Personal (Fremdfirmenmanagement)

REFERENZEN

[1] Camron, J., Frederiksen S., Glismand, F. (2017). *A.P. Møller - Mærsk A/S Interim Report Q2 2017.* Abgerufen von: http://investor.maersk.com/node/23456/pdf

[2] Scherschel, F. A. (2018). *Nach NotPetya-Angriff: Weltkonzern Maersk arbeitete zehn Tage lang analog.* Abgerufen von: https://www.heise.de/newsticker/meldung/Nach-NotPetya-Angriff-Weltkonzern-Maersk-arbeitete-zehn-Tage-lang-analog-3952112.html

[3] Kaspersky Lab. (2017). *IT-Sicherheitsvorfall kostet europäische große Unternehmen 1,12 Millionen und kleine Firmen 68,880 Euro.* Abgerufen von: https://www.kaspersky.de/about/press-releases/2017_it-sicherheitsvorfall-kostet-europaische-unternehmen

[4] Bundesamt für Sicherheit in der Informationstechnik (BSI). (2017). *Cyber-Sicherheits-Umfrage 2017: Cyber-Risiken, Meinungen und Maßnahmen.* Abgerufen von: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/ACS/cyber-sicherheits-umfrage_2017.pdf;jsessionid=E14010AA03E93E3598938DABED390E90.2_cid369?__blob=publicationFile&v=3

[5] Bundesamt für Sicherheit in der Informationstechnik (BSI). (2018). *IT Grundschutzkatalog G 5.42 Social Engineering.* Abgerufen von: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05042.html

[6] Bundesamt für Sicherheit in der Informationstechnik. (2016). *Top 10 Bedrohungen und Gegenmaßnahmen 2016: Industrial Control System Security.* Abgerufen von: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf?__blob=publicationFile&v=4

[7] National Cybersecurity and Communications Integration Center. (2016). *Year in Review 2016 - Incident Response Pie Charts FY2016.* Abgerufen von: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_IR_Pie_Chart_S508C.pdf

[8] Bundesministerium für Wirtschaft und Energie BMWi. (2016). *IT-Sicherheit für die Industrie 4.0: Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie.* Abgerufen von: https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/it-sicherheit-fuer-industrie-4-0.pdf?__blob=publicationFile&v=4

[9] ISO/IEC 27001:2013 + Cor. 1:2014. (2015). Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme – Anforderungen. DIN: www.beuth.de

[10] Siegwarth, C., Adamzyk, H., Frey, G. (2018). Industrial Security - IEC 62443 in der I4.0 Analyse. In *VDI Tagungsband Automation, 2018, Baden-Baden*, 369–381.

[11] Bundesministerium für Wirtschaft und Energie BMWi. (2016). *IT-Security in der Industrie 4.0: Handlungsfelder für Betreiber.* Abgerufen von: http://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/leitfaden-it-security-i40.pdf?__blob=publicationFile&v=8

[12] Department of Homeland Security 2016). *Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies: Recommended Practice.* Abgerufen von: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

[13] Knapp, E. D., & Langill, J. T. (2014). Industrial Network Security: *Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems.* Syngress.

[14] SANS Institute. (2018). *The State of Security in Control Systems Today.* Abgerufen von: https://www.sans.org/reading-room/whitepapers/analyst/membership/36042

[15] Kernkraftwerk Gundremmingen (2016). *Aktuelle Informationen aus dem Kernkraftwerk Gundremmingen -Betriebsbericht Nr. 4/2016 vom 25.4.2016.* Abgerufen von: http://www.kkw-gundremmingen.de/betriebsberichte.php?id=45

[16] Bundesamt für Sicherheit in der Informationstechnik. (2018). *Industrial Control System Security: Innentäter.* Abgerufen von: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_061.pdf?__blob=publicationFile&v=3

[17] Mettler, H., Krausz, S., Geiger, R. (2018). Integriertes Vorgehensmodell zur Planung und Umsetzung eines ISMS in der pharmazeutischen Produktion. In *VDI Tagungsband Automation, 2018, Baden-Baden,* 383–392.

[18] VdS Schadenverhütung GmbH (o. J.). *VdS Quick Check für Industrial Control Systems.* Abgerufen von: https://www.vds-quick-check.de/der-vds-quick-check-fuer-ics-im-detail/

[19] VDMA - Verband der Maschinen und Anlagenbauer e. V. (2014). *VDMA Fragenkatalog Industrial Security.* Abgerufen von: http://pks.vdma.org/documents/105969/142443/VDMA%20Fragenkatalog%20Security_2014_final.pdf/29d94802-ae85-4478-b1e5-cc4be852f002

[20] DIN EN ISO/IEC 27002:2017-06. (2017). Informationstechnik - Sicherheitsverfahren - Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27002:2017. DIN: www.beuth.de

[21] DIN ISO/IEC TR 27019 DIN SPEC 27019. (2015). Informationstechnik – Sicherheitsverfahren – Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002 (ISO/IEC TR 27019:2014), 2015. DIN: www.beuth.de

[22] Kersten, H., Klett, G., Reuter, J., & Schröder, K. W. (2016*). IT-Sicherheitsmanagement nach der neuen ISO 27001: ISMS, Risiken, Kennziffern, Controls*. Springer-Verlag.

[23] Bundesamt für Sicherheit in der Informationstechnik (BSI). (2008). *BSI-Standard 100-1 - Managementsysteme für die Informationssicherheit (ISMS).* Abgerufen von:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1001.pdf?__blob=publicationFile

[24] Bundesamt für Sicherheit in der Informationstechnik (BSI). (2018). *IT-Grundschutz-Kompendium: Edition 2018.* Abgerufen von: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2018.pdf?__blob=publicationFile&v=7.

[25] Kobes, P. (2016). *Leitfaden Industrial Security: IEC 62443 einfach erklärt.* VDE Verlag.

[26] VDMA - Verband der Maschinen und Anlagenbauer e. V. (2016). *Leitfaden Security für den Maschinen- und Anlagenbau Der Weg durch die IEC 62443*. Abgerufen von: http://pks.vdma.org/documents/105969/15311113/1479910314521_INS%20Security-Leitfaden%20VDMA_v1.0_WEB.pdf/b615dd92-3b84-4e93-afb6-23f54fead723

[27] ISA6244321 (99.02.01). (2014). Security for industrial automation and control systems Part 2-1: Industrial automation and control system security management system. ISA: www.isa.org

[28] IEC TR 62443-2-3:201. (2015). Security for industrial automation and control systems - Part 2-3: Patch Management in the IACS environment. IEC: www.iec.ch

[29] DIN IEC 62443-2-4:2017-01. (2016). IT-Sicherheit für industrielle Automatisierungssysteme - Teil 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme (IEC 62443-2-4:2015 + Cor.:2015). DIN: www.beuth.de

[30] DIN IEC 62443-2-4-100:2017-09. (2017). IT-Sicherheit für industrielle Automatisierungssysteme - Teil 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme (IEC 65/637A/CDV:2016). DIN: www.beuth.de

[31] DIN EN 62443-3-2:2018-10. (2018). Sicherheit für industrielle Automatisierungssysteme - Teil 3-2: Sicherheitsrisikobeurteilung und Systemgestaltung (IEC 65/690/CDV:2018); Deutsche und Englische Fassung prEN 62443-3-2:2018, - Entwurf. DIN: www.beuth.de

[32] DIN IEC 62443-3-3:2015-06. (2015). Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme - Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level (IEC 62443-3-3:2013 + Cor.:2014), - Entwurf, 2015. DIN: www.beuth.de

[33] VdS 3473:2015-07. (2015). Informationssicherheit in kleinen und mittleren Unternehmen (KMU). VdS: www.vds.de

[34] Vds 10020. (2018). Cyber Security für kleine und mittlere Unternehmen (KMU) - Leitfaden zur Interpretation und Umsetzung der VdS 3473 für Industrielle Automatisierungssysteme. www.vds.de

[35] BITKOM - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (2006). *IT-Risiko- und Chancenmanagement im Unternehmen: Ein Leitfaden für kleine und mittlere Unternehmen.* Abgerufen von: https://www.bitkom.org/Publikationen/2006/Leitfaden/Leitfaden-IT-Risiko-und-Chancenmanagement-fuer-kleine-und-mittlere-Unternehmen/060601-Bitkom-Leitfaden-IT-Risikomanagement-V10-final.pdf.

[36] VDMA - Verband der Maschinen und Anlagenbauer e. V. (2016). *Leitfaden Industrie 4.0 Security: Handlungsempfehlungen für den Mittelstand.* Abgerufen von: https://industrie40.vdma.org/documents/4214230/15280277/1492501068630_Leitfaden_I40_Security_DE.pdf/836f1356-12e6-4a00-9a4d-e4bcc07101b4

[37] VDI/VDE 2182 Blatt 1:2011-01. (2011). Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell, 2011. VDI: www.beuth.de

[38] NAMUR. (2006). NA115: IT-Sicherheit für Systeme der Automatisierungstechnik: Randbedingungen für Maßnahmen beim Einsatz in der Prozessindustrie. NAMUR: www.namur.net

[39] NAMUR (2015). NE 153: Automation Security 2020 – Design, Implementierung und Betrieb industrieller Automatisierungssysteme. NAMUR: www.namur.net.

[40] Junker, H. (2013). Cyber-Sicherheit zur Chefsache machen: Firmen sind meist ungenügend vor IT-Attacken geschützt. In *atp magazin, 2013*(7-8), 20–21

[41] Kersten, H., & Klett, G. (2015). *Der IT Security Manager: Aktuelles Praxiswissen für IT Security Manager und IT-Sicherheitsbeauftragte in Unternehmen und Behörden*. Springer-Verlag.

[42] Slay, J., & Miller, M. (2007, March). Lessons learned from the maroochy water breach. In *International Conference on Critical Infrastructure Protection* (pp. 73-82). Springer, Boston, MA.

[43] Department of Homeland Security. (2018). *ICS-CERT Alerts*. Abgerufen von: https://ics-cert.us-cert.gov/alerts

[44] Siemens AG. (2018). *Siemens ProductCERT und Siemens CERT*. Abgerufen von: https://www.siemens.com/global/de/home/produkte/services/cert.html

[45] WAGO Kontakttechnik GmbH & Co. KG. (2018). *Wago Security - Hinweise Automatisierungskomponenten.* Abgerufen von: https://www.wago.com/de/automatisierungstechnik/security

[46] VDI/VDE 2182 Blatt 2.3:2017-09. (2017). Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Maschinen- und Anlagenbauer für Betreiber Presswerk. VDI: www.beuth.de

REFERENZEN

[47] VDI/VDE 2182 Blatt 3.3:2013-06. (2016). Informationssicherheit in der industriellen Automatisierung Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Betreiber LDPE-Anlage, 2013. VDI: www.beuth.de

[48] ISA 62443-3-1: Technical Report Security Technologies for Industrial Automation and Control Systems, , Rev. 2, 2007.

[49] SANS Institute. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*. Abgerufen von: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[50] Bundesamt für Sicherheit in der Informationstechnik (BSI). (2018). *Fernwartung im industriellen Umfeld.* Abgerufen von: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_108.pdf?__blob=publicationFile&v=3

[51] NAMUR. (2011). NA 135: Fernwartung bei Systemen der Automatisierungstechnik in der Prozessindustrie. NAMUR: www.namur.net

[52] Bundesamt für Sicherheit in der Informationstechnik (BSI) (2018). *Schutz vor Ransomware - Präventive Maßnahmen zur Absicherung vor Krypto-Trojanern*. Abgerufen von: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_124.pdf?__blob=publicationFile&v=2

[53] Bundesamt für Sicherheit in der Informationstechnik (BSI). (2018). *IT Grundschutz: CON.3 Datensicherungskonzept.* Abgerufen von: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_3_Datensicherungskonzept.html

[54] Niemann, K. (2014). IT-Security-Konzepte für die Prozessindustrie. *atp Magazin, 56*(07-08), 62-69. Abgerufen am Oktober 22, 2018 von http://ojs.di-verlag.de/index.php/atp_edition/article/view/2256

Eine Aufstellung der notwendigen Richtlinien findet sich in [33] in Verbindung mit [34].

4. Personal

In diesem Beitrag wurde herausgearbeitet, dass das Personal einen wesentlicher Faktor für die IT-Sicherheit im Unternehmen darstellt. Das Personal ist über Schulungen zu trainieren und die Einhaltung der Richtlinien durch das Personal ist zu überwachen. Weiterhin sind Prozesse zu definieren, wie beim Eintritt und beim Ausscheiden von Personal zu verfahren ist. Ein IT-Sicherheitsvorfall in einem australischen Klärwerk war möglich, weil ein ausgeschiedener Dienstleister im Besitz der Passworte aller drahtlosen Zugangspunkte zum Automatisierungsnetzwerk war und diese von außerhalb des Werksgeländes erreichbar waren [42]. Durch entsprechende Prozesse bei Ausscheiden von Dienstleistern (Entzug von Zugriffsrechten bei Beendigung des Vertragsverhältnisses) wäre dieser Vorfall vermeidbar gewesen.

5. Wissen

Viele Automatisierungstechnikhersteller zum Beispiel [44, 45] und auch staatliche Organisationen [43] stellen Betreibern Informationen über bekannte Schwachstellen und Maßnahme zur Behebung oder Mitigation zur Verfügung. Die Prozesse im Unternehmen sind so zu organisieren, dass dieses Wissen genutzt und die für das Unternehmen notwendigen Maßnahmen abgeleitet werden.

6. Identifizieren, Bewerten und Schützen der Assets

In diesem Schritt erfolgt eine systematische Erfassung aller Assets und der Netzwerkstruktur. Das hierfür notwendige Vorgehen ist in der VDI 2182 Teil 1 [37] beschrieben. Die besonderen Aufgaben des Betreibers bei diesem Prozess finden sich in der VDI 2182 in den Teilen 2.3 [46] und 3.3 [47]. In der Regel folgen der Erfassung eine Bewertung der Assets und die Ableitung des Schutzbedarfes für die Komponenten und drahtlosen und kabelgebundenen Netzwerke. Übliche Schutzmaßnahmen sind zum Beispiel Zugangsschutz zur Anlage und deren Komponenten, Abschottung von Netzwerken, Segmentierung von Netzwerken, Virenschutz, Applikations-Whitelisting, Errichten demilitarisierter Zonen et cetera Weitere Informationen hierzu finden sich in der IEC 62443 in den Teilen 3-1 [48], 3-2 [31] und 3-3 [32]. Da viele Unternehmen in ihren Prozessen zu diesem Punkt schon weit fortgeschritten sind, erfolgt aus Platzgründen an dieser Stelle keine weitere Detaillierung.

7. Externer Zugriff

Bekannte Vorfälle, wie der Angriff auf das ukrainische Energieversorgungsnetz [49], erfolgten über Remote-Zugänge. Diese Art von Zugängen ist aus Sicht der IT-Sicherheit besonders kritisch. Daher wird diesem Thema in diesem 10-Punkte-Plan ein eigener Punkt gewidmet. Der externe Zugriff ist so zu organisieren, dass die Verbindung geschützt (verschlüsselt) und nur

vom Unternehmen in Richtung Dienstleister aufgebaut werden kann. Es ist eine Multi-Faktor-Authentifizierung einzusetzen. Die Verbindung sollte zeitgesteuert automatisch zu trennen sein. Weitere Hinweise zum sicheren Aufbau einer Fernwartungsanbindung finden sich in der BSI-Richtlinie CS-108 [50] und im Namur-Arbeitsblatt NA135 [51].

8. Datensicherung
Das Aufkommen von Verschlüsselungstrojanern hat, wie in der Einleitung beschrieben, in Unternehmen zu nachhaltigen Schäden durch Datenverlust geführt [1]. Daher kommt dem Thema Datensicherung eine besondere Bedeutung zu. Eine Datensicherung ist regelmäßig durchzuführen. Die Sicherungssysteme sind so aufzubauen, dass diese nicht durch infizierte Systeme verschlüsselt werden können. Das ist bei Server-Laufwerken, die allgemein für Nutzer zugänglich und dauerhaft in Betrieb sind, nicht der Fall. Hier sind Lösungen zu suchen bei denen die Daten des Backupsystems für Geräte aus dem Netzwerk nicht erreichbar sind. Das BSI gibt in [52] Hinweise zur Absicherung gegen Krypto-Trojaner. Ein allgemeines Vorgehensmodell zur Datensicherung liefert das BSI in [53]. Besondere Aufmerksamkeit sollte darauf gelegt werden, dass in regelmäßigen Abständen die Wiederherstellung von Daten geübt wird.

9. Störungen und Ausfälle
Bei Störungen und Ausfällen hat die Wiederherstellung des laufenden Betriebes höchste Priorität. Erst danach folgen Analyse und Ursachenforschung. Im Rahmen eines Vorgehensmodells sollten Meldewege und Zuständigkeiten definiert sein und dokumentiert werden. Es ist auch festzulegen, wie bei einer Störung am Wochenende oder an Feiertagen zu verfahren ist. Das Verhalten und die Vorgehensweisen sind zu dokumentieren und zu erproben. Regelmäßige Übungen können das Notfallmanagement festigen und Lücken im Prozess auffindbar machen.

10. IT-Sicherheitsvorfälle
Die in Punkt 9 gennannten Störungen und Ausfälle können zunächst allgemeiner Natur sein. In diesem Abschnitt wird nun das Vorgehen bei IT-Sicherheitsvorfällen betrachtet. Es ist zunächst zu definieren und zu dokumentieren, was unter IT-Sicherheitsvorfällen zu verstehen ist. IT-Sicherheitsvorfälle sind an den ISB zu melden. Es ist zu definieren, in welchen Fällen das Top-Management zu involvieren ist und ob gegebenenfalls eine Information der Öffentlichkeit (Ad-Hoc-Mitteilung bei Aktiengesellschaften) zu erfolgen hat. Für das Erkennen von IT-Sicherheitsvorfällen können beispielsweise Netzwerküberwachungssysteme oder Honey-Pots dienen. Darüber hinaus bieten sogenannte Security-Information-and-Event-Management-Systeme (SIEM) die Möglichkeit, Security-relevante Daten zu erfassen und zu überwachen.

AUTOR

Prof. Dr.-Ing. **KARL-HEINZ NIEMANN** (1959) vertritt das Lehrgebiet Prozessinformatik und Automatisierungstechnik an der Fakultät I Elektro- und Informationstechnik der Hochschule Hannover. Neben seiner Lehrtätigkeit leitet er verschiedene Forschungsprojekte aus dem Bereich der IT-Sicherheit für Produktionsanlagen und dem Energiemanagement. Darüber hinaus ist er im VDI und in der PROFIBUS Nutzerorganisation in der Standardisierung tätig. Darüber hinaus ist Karl-Heinz Niemann Sprecher des Forschungsclusters Industrie 4.0 der Hochschule Hannover. Siehe https://forschungscluster.hs-hannover.de/industrie-40/

Hochschule Hannover,
Fakultät I – Elektro- und Informationstechnik,
Ricklinger Stadtweg 120,
30445 Hannover,
Tel. +49 (0) 511 92 96 12 64,
Karl-Heinz.Niemann@Hs-Hannover.de

Mit diesen zehn Schritten können die organisatorischen Prozesse für Unternehmen, Lieferanten und Dienstleister so organsiert werden, dass sie die technischen Maßnahmen sinnvoll ergänzen. Es ist zu beachten, dass die IEC 62443 künftig das Schutzniveau einer Anlage (Protection Level PL) anhand der Kombination der umgesetzten funktionalen Maßnahmen (Security Level SL) und des Reifegrades der organisatorischen Maßnahmen (Maturity Level ML) bewerten wird [25]. Nur durch das Erreichen von ausreichend hohen Schutzniveaus in beiden Bereichen (SL und ML) ist ein entsprechender Protection Level PL erreichbar.

4. ZUSAMMENFASSUNG UND FAZIT

Das beschriebene Vorgehensmodell basiert auf einer Kombination von technischen und organisatorischen Maßnahmen. Im Fokus liegt dabei die Absicherung der Anlage gegen Angriffe von außen, die Aufteilung der Anlage in Bereiche, die Abschottung der Bereiche untereinander und die Überwachung der Bereiche. Im Kontext von Industrie 4.0 werden künftig weitere Anforderungen entstehen, die darauf hinzielen, dass auch die echtzeitfähige Kommunikation innerhalb der abgeschotteten Bereiche gegen Manipulation geschützt wird. Die Namur hat in [39] entsprechende Anforderungen definiert. Die hierfür erforderlichen technischen Maßnahmen und Anforderungen an künftige Automatisierungssysteme beschreibt der Autor in [54].