Sicherheit von industriellen Steuerungssystemen

Andreas Martin Floß

HiSolutions AG
floss@hisolutions.com

Zusammenfassung

Dieser Beitrag stellt das neue Grundlagenwerk „ICS-Security-Kompendium“ zur Sicherheit von Industrial Control Systems (ICS) vor. Diese Systeme werden in der produzierenden Industrie und in weiteren schützenwerten Branchen eingesetzt, wie z. B. Wasser- und Energieversorgung, Ernährung, Transport sowie Verkehr. Ziel ist dieses Beitrages ist es, eine Einordnung dieses Werkes vorzunehmen und eine Bewertung der darin vorgeschlagenen Vorgehensweise und Best Practices für industrielle Steuerungsanlagen durch Aufzeigen von Stärken und Schwächen zu diskutieren sowie zusätzliche Aspekte zu erörtern. Die vorgeschlagenen BSI IT-Grundschutzstandards und die darin enthaltende Vorgehensweise nach BSI-Standard 100-2 haben sich im klassischen IT-Betrieb bei Behörden und auch in Unternehmen bereits bewährt. Die Sammlung der BSI IT-Grundschutzkataloge mit standardisierten Gefährdungen und Sicherheitsmaßnahmen sind schon heute für ICS methodisch gut anwendbar, jedoch mangelt es zum jetzigen Zeitpunkt meist an einem strukturierten Sicherheitsmanagement. Zudem fehlen bisher angepasste Maßnahmen für ICS, die bislang mühsam in einzelnen Risikoanalysen erarbeitet werden müssen. Dafür stellt nun das ICS-Security-Kompendium einige interessante Vorschläge in Form von Best Practices vor, die eine erste Hilfestellung geben können.

1 Inhalte des ICS-Security-Kompendium

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichte im November 2013 das ICS-Security-Kompendium [BSI13]. Dieses als Grundlagenwerk bezeichnete 123 Seiten umfassende Kompendium möchte IT-Sicherheits- und ICS-Experten eine Unterstützung beim Zugang zum Thema IT-Sicherheit in industriellen Steuerungssystemen (engl. Industrial Control Systems – kurz ICS) geben. Das Kompendium legt den Fokus auf Grundlagen und Empfehlungen speziell für die Betreiber von ICS. Zukünftig soll in einer Weiterentwicklung des Kompendiums ebenso auf die Belange von Herstellern, Maschinenbauern und Integratoren eingegangen werden.

Unter industriellen Steuerungssystemen versteht das BSI alle Arten von Automatisierungs-, Prozesssteuerungs- und Prozessleitsystemen, die physisch ablaufende Prozesse messen, steuern sowie deren Abläufe regeln und überwachen. Typischerweise sind ICS besonders in der produzierenden Industrie sowie in den als kritische Infrastrukturen (KRITIS) eingestuften Branchen, wie z.B. Energie- und Wasserwirtschaft oder Transport und Verkehr zu finden.

Das Kompendium verfolgt mehrere Zielsetzungen, die z.T. auch über die Vermittlung von Grundlagen der IT-Sicherheit und der ICS-Abläufe hinausgehen. Die Autoren des Kompendiums versuchen auch die bereits existierenden BSI IT-Grundschutzkataloge mit den darin enthaltenen technischen und organisatorischen Sicherheitsmaßnahmen soweit anzupassen bzw.

P. Schartner · P. Lipp (Hrsg.) · D•A•CH Security 2014 · syssec (2014) 105-112.

zu nutzen, sodass sie für die ICS-Security anwendbar werden. Zudem wird eine Übersicht über die für ICS relevanten nationalen und internationalen Normen und Standards gegeben - wobei das Kompendium auch den Anspruch hat, eine Sammlung von bewährten Sicherheitsmaßnahmen (Best Practices) zusammenzustellen. Darüber hinaus soll mit einer Auditmethodik eine Möglichkeit der Prüfung und Verbesserung gegeben werden. Schlussendlich möchte das Kompendium den momentanen Handlungsbedarf aufzeigen und auf notwendige Themen für Forschung und Entwicklung hinweisen.

Dieser Beitrag möchte eine Einordung des Kompendiums für das aktuelle Themengebiet Sicherheitsmanagement für ICS vornehmen. Der Leser bekommt eine Aussage, inwieweit dieses Kompendium für die ICS-Sicherheit geeignet ist, bzw. zeigt Aspekte auf, was für die Praxis noch fehlt. Zudem werden die darin enthaltenen Vorgehensweisen und Best Practices einer kritischen Betrachtung unterzogen.

2 Management der Informationssicherheit

Informationssicherheit hat zum Ziel Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherzustellen. Das Management der Informationssicherheit besteht nun darin, organisatorische Rahmenbedingungen zu schaffen, Sicherheitsmaßnahmen zu planen und umzusetzen sowie die Wirksamkeit der Aktivitäten zu kontrollieren. Eine typische Maßnahme hinsichtlich Vertraulichkeit von Informationen auf einem IT-System wäre z.B. das Einrichten eines Zugriffsschutzes mittels Authentisierung per Passwort.

Diese Anforderungen kommen aus dem klassischen IT-Bereich von Unternehmen und Behörden. In diesem Bereich gibt es eine umfassende Auswahl an Best Practices, wie z.B. die BSI IT-Grundschutz-Kataloge. In vielen Organisationen haben sich im Laufe der Jahre erprobte Vorgehensweisen etabliert. Das Ziel ist immer der Schutz vor wirtschaftlichen Schäden, indem man die Risiken, die aus einer Vielzahl von Gefährdungen entstehen können, durch ein Sicherheitsmanagement minimiert. Die Verantwortung ist bei der Organisationsleitung verankert und entspricht somit dem Top-Down-Ansatz.

Da gerade der IT-Dienstleistungssektor stark durch das Auslagern von Anwendungen und Prozessen IT-Betrieb geprägt ist, gibt es eine Motivation die organisationseigene Informationssicherheit durch eine Zertifizierung der nachzuweisen. Laut ISO Survey hatten im Jahre 2012 in Deutschland ganze 499 Organisationen eine ISO 27001-Zertifizierung.

Mit der zunehmenden Vernetzung von ICS über öffentlich zugängliche Netze wie dem Internet erscheint es nur logisch, dass ICS immer größeren Risiken ausgesetzt sind. ICS wird immer mehr durch moderne Informationstechnik durchdrungen. Hinzu kommt, dass Hard- und Software zu einer Zeit entwickelt wurden, in der noch niemand an eine weltweite Vernetzung gedacht hat.

3 Standards und Normen

Sehr unübersichtlich sind momentan die für ICS geltenden Standards und Normen. Das Kompendium gibt einen ausführlichen Überblick mit Erläuterungen und der dazugehörigen Organisationen und Verbände. Hierbei spielen nur die sicherheitsrelevanten Vorgaben eine Rolle, da Standards und Normen zur Betriebssicherheit (engl. safety) laut BSI explizit nicht Betrachtungsgegenstand des ICS-Security-Kompendiums sind.

An erster Stelle sind die Standards der ISO 27000-Familie zum Informationssicherheitsmanagement der International Standards Organisation für Normung (ISO) zu nennen. Dieses typische Managementsystem nach standardisierter ISO-Art ist sehr universell einsetzbar. Es ist jedoch aufgrund des niedrigen technischen Detaillierungsgrad in erster Linie als eine Art Überbau zusehen.

Grundsätzlich eignet sich dafür, ICS-Betreibern ein System an die Hand zu geben um Informationssicherheitsmanagement mit den wichtigsten Aspekten einzuführen. Darin enthaltene Themengebiete geben eine gute Struktur vor, in der Themen, wie z.B. Risikobehandlung, Personalsicherheit, Zugangskontrolle oder Einhaltung von Vorgaben (engl. compliance) behandelt werden.

Für einige Branchen, wie z.B. Energieversorgung (ISO 27019 - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry) oder die Branche der Cloud-Anbieter (ISO 27017 - Code of practice for information security controls based on ISO/IEC 27002 for cloud services), gibt es bereits ganz aktuell spezifische ISO-Standards und Guidelines für Informationssicherheit.

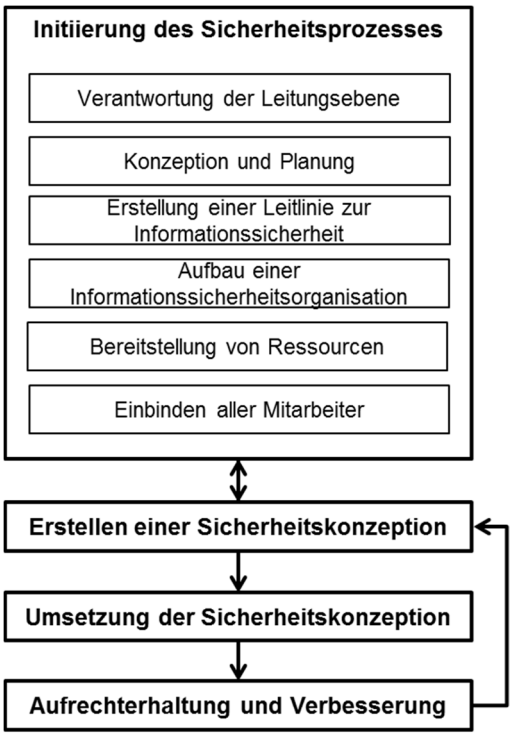

Abb. 1: Informationssicherheitsmanagement nach BSI IT-Grundschutz ist ein fortlaufender Prozess.

Der eigene deutsche BSI-Standard 100-1 bzw. 100-2 mit dem Zertifikat „ISO 27001 auf Basis von BSI IT-Grundschutz“ wird ebenfalls als Möglichkeit zum Aufbau eines ICS-Sicherheitsmanagements vorgestellt. Dieser Standard bietet eine in vielen Behörden und auch in privaten Organisationen eine praxiserprobte Vorgehensweise (siehe **Abb. 1**) zum Informationssicherheitsmanagement.

Des Weiteren werden die beiden technischen Normenreihen IEC 62443 (Industrial communication networks – Network and system security) und IEC 62351 (Power systems management and associated information exchange – Data and communication security) vorgestellt. IEC 62443 beschreibt ein prozessorientiertes Vorgehensmodell zur Herstellung von IT-Sicherheit

für die industrielle Automatisierung und Kontrollsysteme (IACS). Es werden Hinweise bezüglich eines Cybersicherheitsmanagementsystem (CSMS) für Hersteller, Integratoren und Betreiber von IACS gegeben. IEC 62351 hingegen ist eher technisch und macht Vorgaben für Entwickler in der Energietechnik zur Absicherung der eingesetzten Kommunikationsprotokolle.

Als weitere Standards und Normen deutscher Organisationen, wie dem Deutschen Institut für Normungen (DIN), den Branchenverbänden VDI, VDE und DKE sowie weiteren branchenspezifischen Vorgaben wie vom Bundesverband der Energie- und Wasserwirtschaft, sowie dem Verband der Großkraftwerksbetreiber (VGB) vorgestellt.

Auf internationaler Ebene werden hauptsächliche US-amerikanische und angelsächsische Standards und Normen als Informationsquelle vorgestellt. Eine weitere gute Übersicht über die verschiedenen Standards bietet auch der Kompass IT-Sicherheit der BITKOM [BIT10] oder auch Guidelines auf eher technischer Ebene die Webseite ICS-Cert des Department of Homeland Security [DHS14].

4 Rahmenbedingungen

Traditionell haben IT-Sicherheit und ICS keine oder nur sehr wenige Berührungspunkte. Die fehlende Sicherheitskultur ist durch die bisher isolierte Einsatzumgebung von ICS und dem oft aufkommenden Zielkonflikt von Sicherheit versus Funktionalität begründet. Proprietäre Software und Protokolle haben viele Schwachstellen und in der Regel keine Sicherheitsfeatures, die im Zuge der heutigen Vernetzung notwendig wären. Viele Sicherheitsexperten konstatieren der Sicherheit in ICS einen enormen Nachholbedarf und sehen einen Sicherheitsstand wie in der klassischen IT vor 15 Jahren [Weis10].

Die Rahmenbedingungen von ICS erschweren laut ICS-Security-Kompendium die Umsetzung der Informationssicherheit. Während die Systeme immer häufiger mit Fremdsystemen vernetzt sind gibt es kaum Sicherheitsmechanismen gegen absichtliche Manipulation. Zunehmend werden aber auch hier klassische IT-Systeme im Verbund mit industriellen Steuerungssystemen eingesetzt. Diese werden dann direkt mit ICS verbunden, auf denen Updates und Patches nicht ohne weiteres eingespielt werden können. Eine andere Problematik stellt das Alter der Systeme dar – oft haben ICS eine Lebensdauer von über 20 Jahren. Dies steht ganz im Gegensatz zur dynamischen Entwicklung von klassischen IT-Systemen. Zudem gibt es strenge Vorgaben zum Betrieb der Anlagen, die Änderungen am System ohne ausführliche Prüfungen nicht erlauben. Zusammen mit häufigen Wartungen kann das Einspielen von Updates oder Patches hohe Kosten verursachen. ICS haben in der Regel auch sehr hohe Verfügbarkeitsanforderungen.

5 Gefährdungen bei ICS

Mit zunehmender Vernetzung, Kommunikation und Fernsteuerung sind ICS immer häufiger einer Vielzahl von Gefährdungen ausgesetzt, die erst seit einigen Jahren mit dem Siegeszug des Internets aufgekommen sind. Diese für ICS-Betreiber neu aufgekommenen Gefährdungen können zu erheblichen Risiken für Betreiber führen. Das Kompendium des BSI nennt hierbei an erster Stelle die Betriebssicherheit. Zudem kommen aber Produktionsausfälle, Umweltverschmutzung, Schäden an Betriebsmitteln, Informationsdiebstahl und Beschädigung der Reputation eines Betreibers hinzu.

Das Kompendium stellt eine Auswahl an möglichen Gefährdungen zusammen, die im Rahmen eines Informationssicherheitsmanagements unbedingt beachtet und analysiert werden sollten. Hierin besteht auch ein wesentlicher Mehrwert des ICS-Kompendiums. Die Einteilung der Gefährdungen, wie sie auch im BSI IT-Grundschutz vorgenommen werden, gibt dem verantwortlichen Sicherheitsmanagement eine grobe Orientierung für die Risikoanalyse und den umzusetzenden Sicherheitsmaßnahmen.

Die Gefährdungen werden in folgende Gruppen eingeteilt:

- organisatorische Gefährdungen (z.B. unzureichende Regelungen zur IT-Sicherheit, unzureichende Dokumentation, mangelnde Awareness bezüglich IT-Sicherheit)
- menschliche Fehlhandlungen (z.B. Mangelhafte Konfigurationen von Komponenten, Fehlende Backups, unzureichende Validierung von Eingaben und Ausgaben) und
- vorsätzliche Handlungen (z.B. Brute-Force-Angriffe, Denial-of-Service-Angriffe (DoS), Schadsoftware).

Hierbei wird deutlich, dass vorsätzliche Handlungen zwar die prominentesten sind, wie z.B. Brute-Force-Attacken, Schwachstellenscans oder DoS-Attacken, jedoch wird auch herausgestellt, dass organisatorische Gefährdungen und Fehlhandlungen ebenso zu schwerwiegenden Risiken führen können.

Dies ist eine gute Basis zum Identifizieren von möglichen Risiken bei der Durchführung einer Risikoanalyse. Nutzt man beispielsweise die 46 elementaren Gefährdungen und die Methodik zur Risikoanalyse aus dem BSI-Standard 100-3, so kann man gut spezifische ICS-Gefährdungen diesen allgemeinen elementaren Gefährdungen zuordnen. Das stellt eine enorme Vereinfachung bei der Risikoanalyse dar. Zudem gibt es eine Übersicht im Kompendium, die für jeden Best Practice die Referenzen auf die Vorgaben in den Standards ISO 27001, IT-Grundschutz und IEC 62443 aufzeigt.

6 Best Practices

Kern des ICS-Security-Kompendiums sind die architektonischen, technischen und organisatorischen Sicherheitsmaßnahmen für Betreiber. Diese 73 Best Practices sind hauptsächlich aus ISO 27001 bzw. ISO 27002 und den BSI IT-Grundschutzkatalogen abgeleitet. Darin sind auch Hinweise auf die Best Practices enthalten, die initial umgesetzt werden müssen. Das Kompendium erachtet den Aufbau und das Etablieren eines Sicherheitsmanagements, die Pflege der Dokumentation, das Erstellen eines Netzplanes sowie das Auflisten aller IT-Systeme und installierten Anwendungen als essentiell für den Einstieg. Im nächsten Schritt gilt es, die Security-spezifischen Prozesse und Richtlinien zu entwickeln. Anschließend folgen Best Practices zur Auswahl von Systemen, Komponenten und Dienstleistern. Die Best Practices zur baulichen und physischen Absicherung sowie die technischen Maßnahmen ähneln sehr den Maßnahmen der IT-Grundschutzkataloge – sie sind aber speziell für den ICS-Kontext überarbeitet.

In zwei umfassenden Tabellen ist im Kompendium eine Gegenüberstellung der Best Practices ausgearbeitet. Diese Tabellen zeigen auf, welche der vorgestellten Normen und Standard diese Best Practices voll, teilweise oder gar nicht abdecken. Das ICS-Security-Kompendium stellt 73 Best Practices zu den in der Tabelle aufgeführten Aspekten der ICS-Sicherheit vor.

Tab. 1: ICS-Security-Kompendium

Prozesse und Richtlinien	Auswahl Systeme und Komponenten	Bauliche und phys. Absicherung	Technische Maß-nahmen
Security Management	Vertrauenswürdigkeit	Zutrittsschutz	Absicherung der Netze
Technische Dokumentation	IT-Security-Merkmale von ICS-Komponenten	Zugangsschutz	Absicherung von Diensten und Protokollen
Durchgängiges Management aller ICS-Komponenten	Kompatibilität einge-setzter Technologien zu Standards	Zugriffsschutz	Härtung der IT-Systeme
Notfallmanagement	Inbetriebnahme in sicherer Konfiguration	Protokollierung und Auswertung / Überwachung	Patchmanagement
Personal	Soft- und Hardware Support		Authentisierung
Revision & Tests	Fernwartung durch Hersteller und Integrator		Zugriffskontrolle
	Absicherung von Feldgeräten		Schutz vor Schadprogrammen
			Mobile Datenträger
			Datensicherung
			Protokollierung und Auswertung

7 Anwendung und Ausblick

Das vollständige Auflisten und Umsetzen von Best Practices ist nicht empfehlenswert, ohne eine adäquate Vorgehensweise beim Sicherheitsmanagement anzuwenden, wie es z.B. der BSI-Standard 100-2 [BSI08] vorschlägt.

Es bietet sich an, die IT-Grundschutz-Vorgehensweise zu implementieren:

- Definition des Geltungsbereiches
- Durchführen der Strukturanalyse (Erhebung Anwendungen, IT-Systeme, Netze und Räume)
- Durchführen der Schutzbedarfsanalyse (für erhobene Objekte aus der Strukturanalyse)
- Auswahl und Anpassung der Maßnahmen (aus den IT-Grundschutz-Katalogen)
- Durchführen des Basis-Sicherheitschecks (Durchführen eines Soll-Ist-Vergleichs)

- Durchführen der ergänzenden Sicherheitsanalyse (Entscheidung über Durchführung von Risikoanalysen bei nicht vorhandenem Baustein oder höherem Schutzbedarf)

Da es für die einzelnen ICS-Objekte keine IT-Grundschutzbausteine (Sammlung von Gefährdungen und Maßnahmen) gibt, ist immer eine Risikoanalyse durchzuführen. Als Ergebnis der Risikoanalyse kann man zur Risikobehandlung die Best Practices als Risiko minimierende Maßnahmen identifizieren, zuordnen und anwenden.

Bei dieser Zusammenstellung der Best Practices ist der Zusammenhang zwischen Gefährdung und der dazu passenden Sicherheitsmaßnahmen nicht ersichtlich. Eine solche Zuordnung von Gefährdungen und Maßnahmen wird in den IT-Grundschutzkatalogen mit Hilfe der Kreuzreferenztabellen (siehe Tab. **2**) zusammengestellt. [BSI14]. Ein Allgemeiner Server ordnet den Gefährdungen Maßnahmen zu.

Tab. 2: Die Kreuzreferenztabelle für den BSI IT-Grundschutz-Baustein B 3.101

	Schutz-bedarf	G 1.1 Personalausfall	G 1.2 Ausfall von IT-Systemen	G 2.7 Unerlaubte Ausübung von Rechten
M 1.28 Lokale unterbrechungsfreie Stromversorgung	normal		X	
M 2.314 Verwendung von hochverfügbaren Architekturen für Server	höher		X	
M 2.316 Festlegen einer Sicherheitsrichtlinie für einen allg. Server	normal	X		
M 4.239 Sicherer Betrieb eines Servers	normal	X		
M 5.1 Restriktive Rechtevergabe	normal			X

Die Umsetzung der Best Practices des Kompendiums ist zwar zu empfehlen, jedoch kann von einem Grundschutz für ICS nicht die Rede sein. Der IT-Grundschutz für das normale Sicherheitsniveau ermöglicht mit seinen Bausteinen ein gutes Sicherheitsniveau, denn die Bausteine beinhalten eine allgemeine Risikoanalyse für sogenannte Zielobjekte (z.B. Gebäude, Server, WLAN oder Anwendungen), da sie auf einer Zuordnung von Gefährdungen und Maßnahmen basieren. [LaFu13] schlagen dazu vor, die standardisierten Bausteine für verschiedene Objekte in ICS anzupassen bzw. ganz neu zu entwickeln. Beispielsweise könnten laut den Autoren neue Bausteine wie z.B. Werkshalle, Leitstand oder SCADA-System für normalen Schutzbedarf erstellt werden und bereits vorhandene Bausteine neu angepasst bzw. ergänzt werden, wie z.B. die Bausteine Patch- und Änderungsmanagement oder Netz- und Systemmanagement.

Bei fehlenden Bausteinen zu ICS muss mit Hilfe der Gefährdungen aus dem Kompendium in jedem Fall eine individuelle Risikoanalyse für alle speziellen ICS-Objekte (ICS-Applikationen, Systeme, Komponenten, Netze, etc.) vorgenommen werden. Risikoanalysen, wie es z.B. der BSI Standard 100-3 vorschlägt, sind sehr aufwendig und kaum vollständig durchführbar. Der Mehrwert des ICS-Kompendiums besteht nun darin, dass eine Art Baukas-

ten von Gefährdungen und Sicherheitsmaßnahmen zur Verfügung gestellt wird. Bisher fehlt leider der Bezug von Gefährdung zu Best Practices-Maßnahmen (z.B. mit Hilfe von Kreuzreferenztabellen), die dem Sicherheitsmanagement helfen würde, relativ einfach adäquate Maßnahmen zu identifizieren. In diese Richtung sollte zukünftig im Bereich ICS-Sicherheit weiter gearbeitet werden.

Literatur

[BITK10] BITKOM: Kompass der IT-Sicherheitsstandards – Leitfaden und Nachschlagewerk, Bundesverband Informationswirtschaft, Berlin: Telekommunikation und neue Medien e. V. (2010).

[BSIn08] Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI-Standard 100-2 – IT-Grundschutz-Vorgehensweise, Version 2.0. Bonn, BSI (2008)

[BSIn13] Bundesamt für Sicherheit in der Informationstechnik (BSI): Das ICS-Security-Kompendium. Bonn, BSI (2013).

[BSIn14] Bundesamt für Sicherheit in der Informationstechnik (BSI): Kreuzreferenztabellen der IT-Grundschutz-Kataloge 13. Ergänzungslieferung, Bonn, BSI (2013). https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html.

[DoHS14] The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): Standards and References, Online: http://ics-cert.us-cert.gov/Standards-and-References.Washington: Department of Homeland Security (2014).

[LaFu02] S. Lass, D. Fuhr: IT-Sicherheit in der Fabrik, In: Productivity Management 2/2013, GITO-Verlag (2013) 29-32.

[Weis10] Joseph Weiss: Protecting Industrial Control Systems from Electronic Threats. New York: Momentum Press (2010) 206.