H. Langweg, M. Meier, B.C. Witt, D. Reinhardt (Hrsg.): Sicherheit 2018,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2018 249

Ein integriertes Vorgehensmodell zur Planung und Umsetzung eines ISMS am Beispiel der Pharmaproduktion

Robert Geiger[1], Sabrina Krausz[2], Holger Mettler[3]

Abstract: Der Beitrag stellt ein integriertes Vorgehensmodell zur Planung und Umsetzung eines Informationssicherheitsmanagementsystems (ISMS) für KRITIS Betreiber im pharmazeutischen Produktionsumfeld vor. Es soll Betreibern kritischer Infrastrukturen helfen diese zu schützen und kann einen Beitrag zu einem branchenspezifischen Sicherheitsstandard (B3S) für den Sektor Gesundheit leisten. Es soll mögliche Synergien zu vorhandenen Systemen und Prozessen der pharmazeutischen Qualitätssicherung aufzeigen und zusätzliche Anforderungen der automatisierten Produktion berücksichtigen.

Keywords: IT-Sicherheitsgesetz, Informationssicherheitsmanagementsystem (ISMS), KRITIS Infrastrukturen, Risikomanagement, Risikobehandlung, Industrial Control Systems (ICS)

1 Einleitung

Die zunehmende Vernetzung und Anbindung von automatisierten Produktionsanlagen an komplexe IT-Systeme stellen neue Anforderungen an die Sicherheit von Maschinen und Anlagen. Informationstechnisch vernetzte Anlagen in und außerhalb der Produktion müssen daher hinsichtlich Cyber Security Anforderungen und Maschinensicherheit von den Betreibern und Hersteller von Automationslösungen neu überdacht werden. Hinzu kommen neue gesetzliche Anforderungen durch das IT-Sicherheitsgesetz, welches auch Teile der Pharmaindustrie verpflichtet den Stand der Technik umzusetzen um die kritischen Infrastrukturen zu schützen. Ein umfassendes Sicherheitskonzept betrifft in der Pharmaindustrie nicht nur die IT-Systeme sondern auch automatisierte, computerisierte Produktionssysteme. Da technische Sicherheit nur in Verbindung mit organisatorischen und personellen Maßnahmen wirkt, benötigt jede Organisation ein System von Verfahren, Prozeduren und Regeln zum Management der betrieblichen Informationssicherheit, ein ISMS. [Al16] Aus unserer Sicht ist es notwendig, beim Aufbau dieser Systeme die heterogenen Richtlinien und speziell, die oft schon vorhandenen technischen und organisatorischen Maßnahmen aus den (IT)–Qualitätssicherungsprozessen mit einzubeziehen. Insbesondere gängige Modelle zur Computer System Validierung (CSV) wie ISPE GAMP 5 [IS08] müssen hier integriert werden.

[1] M+W Central Europe GmbH, CSV & Cyber Security, Loewentorbogen 9b, 70376 Stuttgart, robert.geiger@mwgroup.net
[2] Hochschule Neu-Ulm, Wileystraße 1, 89231 Neu-Ulm, sabrina.krausz@student.hs-neu-ulm.de
[3] M+W Central Europe GmbH, CSV & Cyber Security, Loewentorbogen 9b, 70376 Stuttgart, holger.mettler@mwgroup.net

doi:10.18420/sicherheit2018_19

2 KRITIS - Absicherung der automatisierten Produktion

Zur Automation von Herstellungsprozessen und der Überwachung in der pharmazeutischen Produktion kommen industrielle Steuerungssysteme (engl. Industrial Control Systems - ICS) zum Einsatz. ICS haben neben den klassischen Schutzzielen Verfügbarkeit, Integrität und Vertraulichkeit noch andere Anforderungen. Dies äußert sich beispielsweise in längeren Betriebszeiten und seltenen Wartungsfenstern, z.B. für das Einspielen von Software-Updates oder -Patches. Zudem sind insbesondere die Echtzeitanforderungen zu nennen, die für die Steuerung häufig unerlässlich sind. Etablierte Schutzmaßnahmen aus dem Büroumfeld (z. B. Virenscanner) sind dabei nur bedingt auf ICS übertragbar. Auch wird der Lebenszyklus von ICS in der Regel aus dem Zyklus der zugehörigen Produktionsanlagen abgeleitet. Die Laufzeit, im Gegensatz zu typischer Office-IT, beträgt zehn bis sogar 20 Jahre. Echtzeit und Security sind also divergierende Anforderungen für ICS Systeme im Vergleich mit Office-Systemen.

2.1 ISO 27001 mit PDCA-Zyklus als Referenzprozess

Bis es einen KRITIS-konformen Standard für die Medizintechnik, Arzneimittelproduktion und weitere Unternehmen der pharmazeutischen Industrie gibt, kann der im IT-Sicherheitsgesetz geforderte Stand der Technik durch etablierte Methoden eines ISMS umgesetzt werden. Da die Implementierung nach ISO 27001 [DI17] Betreibern Kritischer Infrastrukturen empfohlen wird [KP16], wird im Modell diese Norm für den Referenzprozess genutzt. Auch die internationale Anerkennung und höhere Flexibilität sprechen für diese Norm. Die PDCA-Zyklen, die nicht nur implizit in der ISO 27001, sondern auch explizit integraler Bestandteil der Norm IEC 62443 [Ko16] sind, ermöglichen neben der Aufrechterhaltung und Verbesserung der Informationssicherheit auch die Möglichkeit der kontinuierlichen Überprüfung und Verbesserung der GMP-Praxis. Unter GMP (engl. Good Manufacturing Practice, dt. Gute Herstellungspraxis) versteht man internationale Richtlinien und Gesetze zum Qualitätsmanagement der Produktionsabläufe und -umgebung in der Produktion von Arzneimitteln und Wirkstoffen. [Eu11]

2.2 Integratives Vorgehen

Ausgangspunkt des integrierten Vorgehensmodells ist die Erstellung einer Cyber Sicherheitsstrategie speziell für automatisierte Produktionssysteme. Auf deren Basis können die oft schon zahlreich in der regulierten Pharmaindustrie vorhandenen IT Sicherheitsmaßnahmen, Leitlinien, Standard Operation Procedures (SOPs) und organisatorischen Maßnahmen für alle relevanten IT-Systeme abgefragt und berücksichtigt werden und an die Anforderungen eines modernen gesetzeskonformen ISMS angepasst werden. Unser Vorgehensmodell setzt die Anforderungen und Elemente der ISO 27001 mit den Maßnahmen der klassischen pharmazeutischen Qualitätssicherung und gesetzlichen Anforderungen (EU-GMP Leitfaden Anhang 11 [Eu11], FDA 21 CFR Part 11), CSV gemäß ISPE GAMP 5 [IS08] und Infrastrukturqualifizierung mit technischen, sowie organisato-

rischen Sicherheitsmaßnahmen im Produktionsbereich (IEC 62443) in Beziehung, siehe Abb. 1. Die Grundlage bildet ein Modell, das sich am ISPE GAMP Lebenszyklus orientiert und Überschneidungen der ISO 27001, GAMP 5 und IEC 62443 aufzeigt. [MG17]

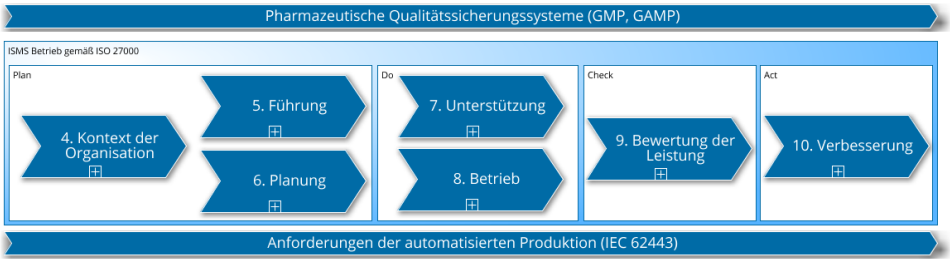

Abb. 1: Integratives Vorgehen am Referenzprozess der ISO 27001

2.3 Das Modell

Das kontrollflussorientierte, integrierte Vorgehensmodell soll die Planung und Umsetzung eines ISMS für KRITIS-Betreiber im Pharmaumfeld unterstützen. Es werden Prozesslandkarten und Unterprozesse auf Basis von Elementen der Business Process Modeling and Notation (BPMN) genutzt. Das Modell zeigt die Abfolge der Prozessschritte des Referenzprozesses aus ISO 27001, deren obligatorische und sinnvolle Dokumentation und die Zuordnung der Controls aus Anhang A, die direkt das ISMS betreffen. Überschneidungen zwischen Anforderungen der ISO 27001 und vorhandenen Systemen und Prozessen der pharmazeutischen Qualitätssicherung sind kenntlich gemacht. Diese werden bei der Implementierung durch Fragebögen und Checklisten analysiert. Tätigkeiten, die in ISO 27001 gefordert werden, wie etwa die Risikoanalyse bzw. Risikobehandlung bauen dann auf vorhandenen GMP-Analysen und Bewertungen auf und können durch neue Sicherheitsanforderungen ergänzt werden. Überschneidungspunkte des Modells mit vorhandenen Prozessen und Dokumentationen sind unter anderem folgende Themenbereiche: Asset-Management, Sicherheitsrichtlinien und Sicherheitsstrategie, Gefährdungsübersichten, Festlegung des Schutzbedarfs von Assets, Konzeption und Implementierung eines Identitäts- und Zugriffs-Managements, Sicherheitsvorfallmanagement, siehe auch Tab. 1.
Das integrierte Modell zeigt, dass durch die pharmazeutischen Qualitätssicherungsprozesse bereits eine starke Grundlage für die Einführung und Verwendung der Informationssicherheitsstandards ISO 27001 und IEC 62443 in der Pharmaindustrie besteht. Damit bietet sich für alle Unternehmen die nach diesen Richtlinien arbeiten wollen eine Möglichkeit kostengünstig und effizient Synergien auszunutzen.

Das integrierte Vorgehensmodell (Work-in-Progress), soll weiter entwickelt werden, mit der wissenschaftlichen Gemeinschaft und Partnern aus der Praxis diskutiert werden und innerhalb eines Industrieprojekts bewertet werden.

ISO 27001		In Pharmaindustrie vorhandene Prozesse/Dokumente
Kontext der Organisation	4.1	Sicherheits-Politik; IT-Sicherheits-SOPs; operative IT-Betriebsrichtlinien; IT-Betriebshandbücher; EHS (Environment-Health-System)
	4.2	bestehende Kontakte zu Zulassungsbehörde, Überwachungsbehörde, Aufsichtsbehörde
	4.3	Inventarisierungsliste; Systeminventarisierung; System Topologien; Site Master File und Validierungsmasterplan (EU-GMP-Leitfaden Kapitel 4 und Anhang 15); Zulassungsantrag; QM-Handbuch
Planung	6.1	Risikomanagement und -Bewertung nach EU-GMP Leitlinie Anhang 11; GAMP 5; ICH Q9
	6.2	IT-Sicherheitsrichtlinie, IT-Betriebsrichtlinie

Tab. 1: Beispiele für Synergien mit vorhandenen Prozessen/Dokumente der Pharmaindustrie

3 Literaturverzeichnis

[Al16] Altrhein, Adrian et.al.: Handreichung zum "Stand der Technik" im Sinne des IT-Sicherheitsgesetzes (ITSiG) (TeleTrusT - Bundesverband IT-Sicherheit e.V Hrsg.), Berlin, 2016.

[DI17] DIN-Normenausschuss Informationstechnik und Anwendungen (NIA) Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015). Beuth Verlag GmbH, Berlin, 2017.

[Eu11] European Commission: EudraLex Volume 4 - EU Guidelines for Good Manufacturing Practice Medicinal Products for Human and Veterinary Use - Annex 11: Computerised Systems, Brussels, 2011.

[IS08] GAMP 5. A risk-based approach to compliant GxP computerized systems (German version). ISPE, Chicago Ill., 2008.

[Ko16] Kobes, P.: Leitfaden Industrial Security. IEC 62443 einfach erklärt. VDE Verlag, Berlin, 2016.

[KP16] Kipker, D.-K.; Pfeil, D.: IT-Sicherheitsgesetz in Theorie und Praxis. In Datenschutz und Datensicherheit - DuD, 2016, 40; S. 810–814.

[MG17] Mettler, H.; Geiger, R.: Sicherstellung der Cyber Security bei automatisierten Produktionssystemen. In Die Pharmazeutische Industrie, 2017, 79; S. 1164–1171.