IT-Risiken in der vernetzten Produktion

Gregor Schlingermann

IT-Risiken in der vernetzten Produktion

Gefahren technisch und finanziell bewerten

Mit einem Geleitwort von Prof. Ing. Peter Markovič, PhD

Springer Gabler

Dr. Gregor Schlingermann
Düsseldorf, Deutschland

OnlinePlus Material zu diesem Buch finden Sie auf
http://www.springer.com/978-3-658-18346-2

ISBN 978-3-658-18345-5 ISBN 978-3-658-18346-2 (eBook)
DOI 10.1007/978-3-658-18346-2

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Gabler

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Gabler ist Teil von Springer Nature
Die eingetragene Gesellschaft ist Springer Fachmedien Wiesbaden GmbH
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Geleitwort

Die IT-Risiken gehören in der gegenwärtigen globalen Welt zu der meist gefürchteten Risikoart. Den Grund dafür liefern zum Ersten die Digitalisierung des alltäglichen Lebens, zum Zweiten die schwer rückverfolgbaren Angriffe und zum Dritten die niedrige Informationskenntnis von Kunden. Dies führt zu höheren Anforderungen an das Risikomanagement von Unternehmen, ohne Rücksicht auf die Branche, den Produkttyp oder die Größenordnung des Unternehmens.

Im Rahmen der Produktion gibt es diverse Situationen, in denen der Einsatz von IT-Instrumenten zu großen zeitlichen und finanziellen Einsparungen führen kann. Positive Beispiele zeigen uns, dass wir dank guter Vernetzung von Inputs und Prozessen wesentlich schlanker produzieren können, und zum Einsatz können somit auch moderne Managementinstrumente wie z. B. Lean Production, Kanban, Kaizen, Quality Circles kommen. Durch den Ersatz menschlicher Tätigkeit durch Maschine und Technologie erreichen wir einen bestimmten Grad der Innovation und üben Wettbewerbsdruck auf einzelne Marktteilnehmer aus. Aus Sicht der Aktionäre (Eigentümer) ist diese Entwicklung positiv und wünschenswert, Manager begrüßen die bessere Informationsversorgung, und Kunden haben die Möglichkeit, die Produkte während der Erzeugung zu verfolgen. Die Industrie 4.0 kann die individuelle Nachfrage problemlos befriedigen und den Kunden eine höhere Nutzqualität des Produkts anbieten. Das, was nur wenige Stakeholder interessieren wird, ist die Sicherheit der gesamten Kommunikationskette, wo sie sich voll auf den Unternehmensstandard verlassen werden.

Die vorgelegte Publikation befasst sich komplex mit den IT-Risiken, mit rechtlichen Anforderungen, der Etablierung eines IT-Risikomanagements und hauptsächlich mit der Produktionsvernetzung. Die wesentliche Botschaft würde ich mithilfe des vorliegenden Textes verbreiten:

> „Mit dem IT-Grundschutz wurden anschließend die im deutschsprachigen Raum relevantesten Methoden als Basis für die Entwicklung einer Bewertungsmethode für das IT-Risikomanagement zur Bewertung der Risiken durch die Vernetzung

> in der Produktion ausgewählt und mit dem Modell der Automatisierungspyramide verknüpft. Für die Bewertung selbst wurde eine Vorgehensweise ausgewählt, wie sie für die Zertifizierung nach ISO 27001 auf Basis von IT Grundschutz genutzt wird. Die genannten Überlegungen bilden das Grundgerüst der Bewertungsmethode. Um dem Anspruch der durchgängigen Transparenz bis zur Ebene des Geschäftsberichtes gerecht werden zu können, wurden Geschäftsberichte gesichtet, um Rückschlüsse auf die festzulegenden Risikokategorien gewinnen zu können. Die entwickelte Bewertungsmethode kombiniert also die Risikoaggregation von unten nach oben mit der Ausdifferenzierung der Risikokategorien von oben nach unten."[1]

Es bleibt allen Lesern zu wünschen, dass sie das notwendige Gehör für die Meinungen des Autors finden und seinen Gedankenfluss im praktischen Leben applizieren.

Prof. Ing. Peter Markovič, PhD
Fakultät für Betriebsmanagement der Wirtschaftsuniversität in Bratislava

[1] Vgl. S. 139 in dieser Arbeit.

Abstract

This dissertation aims at developing an assessment method for IT risk management that allows by using various data to assess the risks that arise in production due to connectivity in the logical as well as physical sense. Due to advanced automation of manufacturing technologies, there are many network interconnections in production today at all manufacturing stages. As network interconnection, not just interconnection in terms of the sequences of operations is referred to but also the actual physical network interconnections that facilitate data transmission within production. Current production facilities largely are permeated by Ethernet networks or at times even wireless networks already. The uses range from individual programmable logic controllers, in the field of which bus systems have been replaced by network system, through individual robots and production equipment up to whole production stages, comprising almost the entire production process. Though the connected production on the one hand facilitates optimised process and production control, it also causes even minor and sporadically occurring irregularities to add up to a major failure. The network failures may be caused either by failures of the network components, but also by virus attacks or targeted sabotage. The tasks of identifying the risks and taking proactive measures as appropriate are a part of IT safety management / IT security management. Typical sources of hazards in these contexts include the lack of virus scanners in production lines, inadequate firewall configurations or poor concepts of practical interventions.

The target output of this paper should be to provide in IT risk management via a newly devised assessment method identification of connectivity-related technical risks implied by existing interconnections, summarisation of the risks and financial evaluation thereof.

Abstract

In dieser Dissertationsarbeit soll eine Bewertungsmethode für das IT-Risikomanagement entwickelt werden, die es ermöglicht, auf Basis verschiedener Daten das Risiko zu bewerten, das sich durch die Vernetzung – sowohl logisch als auch physikalisch – innerhalb der Produktion ergibt. Die heutige Produktion ist durch die stark automatisierte Fertigungstechnik hochgradig in den einzelnen Produktionsschritten miteinander vernetzt. Vernetzt bedeutet in diesem Zusammenhang nicht nur die im Ablauf optimierte Vernetzung, sondern die tatsächliche physische Verbindung, die eine Datenübertragung innerhalb der Produktion ermöglicht. So sind heutige Produktionsstätten zu einem hohen Grad durch Ethernet- oder teilweise bereits Funknetzwerke miteinander verbunden. Dies betrifft von einzelnen speicherprogrammierbaren Steuerungen (SPS) – hier wurden die Bussysteme durch Netzwerke abgelöst – über einzelne Roboter und Produktionsanlagen bis hin zu kompletten Produktionsabschnitten nahezu die ganze Produktion. Die Vernetzung ermöglicht zum einen zwar optimierte Prozess- bzw. Produktionssteuerung, sorgt aber auch dafür, dass bereits kleinere, vereinzelte Störungen sich zu einer Großstörung verketten können. Die Störungen des Netzwerkes können zum einen durch den Ausfall von Netzwerkkomponenten bedingt sein, zum anderen durch Virenbefall oder gezielte Sabotage. Diese Risiken aufzuzeigen und ggf. proaktiv tätig zu werden, ist Teil des IT-Sicherheitsmanagements. Typische Gefahrenquellen sind hier der Mangel von Virenscannern in den Produktionsanlagen, unzureichende Konfigurationen von Firewalls oder mangelnde Zugriffskonzepte.

Als Ergebnis der Arbeit soll es mithilfe einer neu entwickelten Bewertungsmethode möglich sein, die durch Vernetzungen implizierten technischen Risiken der Vernetzung im IT-Risikomanagement explizit zu machen, diese zu konsolidieren und eine monetäre Bewertung durchzuführen.

Inhaltsverzeichnis

Abbildungsverzeichnis 13

Tabellenverzeichnis 15

Abkürzungsverzeichnis 17

Einleitung 19

1 Gegenwärtiger Stand der gelösten Problematik 23

1.1 Risiko, Risikomanagement und Zusammenhänge mit IT-Management .. 23
1.1.1 Definition von Risiken 24
1.1.2 Risikokategorien 25
1.1.3 Der Umgang mit Risiken – das Risikomanagement 33
1.1.4 Etablierung des Risikomanagements im Unternehmen 37
1.1.5 Besonderheiten des IT-Risikomanagements 41

1.2 IT-Risiken – eine Kategorie für sich 41
1.2.1 Rechtliche Anforderungen an das IT-Risikomanagement 46
1.2.2 Etablierung des IT-Risikomanagements in Unternehmen 48

1.3 Das Wesen der Risiko-Bewertungsmethoden 84
1.4 Aktuelle Problemstellungen – Produktion, Infrastruktur und Gefahren 87
1.4.1 Vernetzung in der Produktion – Aufbau einer Produktion und technische Infrastruktur 87
1.4.2 Informationstechnische Gefahren für Produktionsanlagen und deren Vernetzung 91

2 Ziel der Arbeit 97

3 Methodik der Arbeit und wissenschaftliche Methoden ... 99

3.1 Angewandte Methoden ... 99
3.2 Vorgehensweise ... 100

4 Die Ergebnisse der Arbeit ... 101

4.1 Vernetzung in der Produktion – Facetten eines Risikos ... 101
4.2 Was ist und gebraucht wird – Methoden und Modellauswahl ... 102
4.3 Vernetzung in der Produktion neu bewertet – die VIP-Bewertungsmethode ... 103

5 Diskussion ... 137

5.1 Beitrag für die Lehre ... 137
5.2 Beitrag für die Wissenschaft/Forschung ... 138
5.3 Beitrag für die Praxis ... 139
5.4 Ausblick ... 140

Schlusswort ... 143

Literaturverzeichnis ... 147

Anhang ... 155

Abbildungsverzeichnis

Abbildung 1: Rahmenbedingungen Risikomanagement 24
Abbildung 2: Risikodimensionen 26
Abbildung 3: Rechtsnormen zum Risikomanagement 36
Abbildung 4: Einflussfaktoren der Unternehmensumwelt auf das Unternehmen als System 38
Abbildung 5: Strategisches und Operatives Risikomanagement 39
Abbildung 6: Bekanntheit und praktische Bedeutung von Kriterienwerken zur Informations-Sicherheit 48
Abbildung 7: Übersicht über BSI-Publikationen zum Sicherheitsmanagement 51
Abbildung 8: Bestandteile eines Managementsystems für Informationssicherheit 58
Abbildung 9: Gliederung des BSI-Standards 100-2 63
Abbildung 10: Wiederanlaufparameter 74
Abbildung 11: Schadensverlauf und Kosten für Wiederanlauf 77
Abbildung 12: PDCA-Modell des ISO 27001-Standards 80
Abbildung 13: Methoden zur Quantifizierung von IT-Risiken 85
Abbildung 14: Werkstruktur Einzelkonzept 88
Abbildung 15: Werkstruktur Zentralkonzept 89
Abbildung 16: Automatisierungsstruktur einer Rohbauzelle 90
Abbildung 17: Automatisierungspyramide 91
Abbildung 18: OSI-Referenzmodell 92
Abbildung 19: Aufbau eines Produktionsleitsystems 94
Abbildung 20: Vorgehensweise und Aufbau der Arbeit 100
Abbildung 21: Bestandteile der Bewertungsmethode 104
Abbildung 22: IT-Risiken in der Produktion 109

Abbildung 23: Aufbau der Risikobewertungsmethode 110
Abbildung 24: Zuordnung Bausteine der IT-Grundschutz-Kataloge zu Aufbau Produktionsleitsystems 114
Abbildung 25: Zuordnung IT-Grundschutz Risiken Allgemeiner Client zu IT-Risiken in der Produktion 116
Abbildung 26: Ablauf Risikobewertung pro Baustein 121

Tabellenverzeichnis

Tabelle 1: Risikoarten 32
Tabelle 2: Schadenseintritt nach Gefahrenbereich 43
Tabelle 3: IT-relevante Strafbestände im StGB 46
Tabelle 4: Phasenaufbau Bausteine-Kataloge mit Beispiel 54
Tabelle 5: Schichten der Bausteine-Kataloge 56
Tabelle 6: Aufbau Kataloge und Verweise 57
Tabelle 7: Rollenübersicht der IS-Organisation 64
Tabelle 8: Zusätzliche Gefährdungen 69
Tabelle 9: Schadenskategorien und Schadensszenarien 72
Tabelle 10: Gesamtüberblick exemplarische Schadensbewertung 73
Tabelle 11: Entscheidungshilfe Kontinuitätsstrategie Rechenzentrum 78
Tabelle 12: Übersicht ISO/IEC 2700x-Standards 79
Tabelle 13: Kapitel mit Sicherheitskategorien ISO 27002 82
Tabelle 14: IT-Risiken in Geschäftsberichten 106
Tabelle 15: Zuordnung der Qualifizierungsstufen zu Risikostufen ... 113
Tabelle 16: B 3.201 Allgemeiner Client – Zuordnung von kontrollierten Maßnahmen zu Gefahren 118
Tabelle 17: Beispielhafte Risikobewertung der Prozessleitebene 124
Tabelle 18: Beispielhafte Risikobewertung des Geschäftsprozesses Karosseriebau 128
Tabelle 19: Beispielhafte Bewertung aller Geschäftsprozesse 129
Tabelle 20: Beispielhafte Bewertung aller Produktionsstätten 133
Tabelle 21: Darstellung im Geschäftsbericht 135
Tabelle 22: Zuordnung IT-Grundschutz-Risiken ausgewählter Bausteine zu IT-Risiken 155

Abkürzungsverzeichnis

AktG	Aktiengesetz
BCM	Business Continuity Management
BDSG	Bundesdatenschutzgesetz
BIA	Business Impact Analyse
BSI	Bundesamt für Sicherheit in der Informationstechnik
CEO	Chief Executive Officer
CFO	Chief Financial Officer
COSO	Committee of Sponsoring Organizations of the Treadway Commission
COSO ERM	Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management
DAX	Deutscher Aktien Index
DCGK	Deutscher Corporate Governance Kodex
DoS	Denial of Service
DRS	Deutscher Rechnungslegungs Standard
DRSC	Deutsches Rechnungslegungs Standard Committee
EBIT	Earnings Before Interest and Taxes
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
FMEA	Failure Mode and Effects Analysis
HGB	Handelsgesetzbuch
HTTP	Hypertext Transfer Protocol
IC	Internal Control
ISMS	Managementsysteme für Informationssicherheit
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITIL	IT Infrastructure Library
JIS	Just-in-Sequenz
JIT	Just-in-Time

KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KWG	Gesetz über Kreditwesen
LAN	Local Area Network
MES	Manufacturing Execution System
MTA	Maximal tolerierbare Ausfallzeit
OSI	Open System Interconnection
PDA	Personal Digital Assistant
PDCA	Plan-Do-Check-Act
PDF	Portable Document Format
PWC	PricewaterhouseCoopers
RFID	Radio-frequency Identification
SCADA	Supervisory Control and Data Acquisition
SOX	Sarbanes-Oxley Act
SLA	Service Level Agreement
SPS	Speicherprogrammierbare Steuerungen
StGB	Strafgesetzbuch
TCP/IP	Transmission Control Protocol/Internet Protocol
USB	Universal Serial Bus
USV	Unterbrechungsfreie Stromversorgung
VIP	Vernetzung in der Produktion
VoIP	Voice over Internet Protocol
VPN	Virtual private Network
WAZ	Wiederanlaufzeit
WLAN	Wireless Local Area Network

Einleitung

Der wohl bekannteste Vorfall einer gehackten Industrieanlage ereignete sich 2011, als durch professionelle ‚Hacker' erheblicher Schaden in einer Atomanlage im Iran angerichtet wurde. Der hierfür verwendete Computerwurm wurde unter dem Namen Stuxnet bekannt und zeigte deutlich die Schwachstellen von sogenannten SCADA (Supervisory Control and Data Acquisition)-Anlagen auf. Hatte man bis dahin geglaubt, es sei zu aufwendig, individuell programmierte und konzeptionierte Anlagen zu analysieren, deren Schwachstellen aufzudecken und auszunutzen, um damit fatale Schäden anzurichten, wurde man eines Besseren belehrt.

Besonders die Standardisierung zum einen und die Komponentenbauweise zum anderen ermöglichen es, bekannte Schwachstellen einzelner Komponenten immer wieder zu nutzen, um verschiedene Anlagen zu manipulieren. Im Fall des Stuxnet-Wurms wurde eine weitverbreitete Speicherprogrammierbare Steuerung (SPS) der Firma Siemens genutzt, um manipulierte Steuerungsbefehle abzuschicken.

Neben gezielten Angriffen sieht sich die Industrie auch mit der Unachtsamkeit ihrer eigenen Mitarbeiter konfrontiert. So erscheint es zunächst nachvollziehbar, dass Mitarbeiter, wie sie es vom heimischen PC kennen, auch in der Firma Musik abspielen. Welche Auswirkungen es allerdings haben kann, wenn sich neben den Musikdateien auch infizierte Dateien auf dem externen Datenträger befinden, musste nach Medienangaben ein deutscher Autohersteller erfahren. Ein Mitarbeiter hatte einen infizierten USB-Stick in einen Kontrollrechner eingesteckt, über den sich der ‚Virus' im ganzen Werk verbreitete und zum Stillstand des betroffenen Werkes führte. 2005 gab es einen weiteren Vorfall, von dem erneut die Automobilindustrie betroffen war. So musste die DaimlerChrysler AG, als eines von 175 betroffenen Unternehmen, in insgesamt 13 Werken für eine Stunde die Produktion ruhen und das Unternehmen und somit 50.000 Mitarbeiter unbeschäftigt lassen. Grund dafür war die Attacke eines ‚Wurms' Namens Zotob.[2]

---

[2] Vgl. heise (2013)

Die aufgeführten Beispiele zeigen deutlich, wie hoch das Gefährdungspotenzial ist, das sich durch den Einsatz von Informationstechnologie speziell im produzierenden Bereich ergibt. Anders als bei einem Ausfall der IT in der Verwaltung ist der Schaden, der sich in der Produktion ergibt, unmittelbar durch die nicht produzierte Menge darstellbar. Da die IT aus den Geschäfts- und Produktionsprozessen der modernen Wirtschaft nicht mehr wegzudenken ist, besteht eine wesentliche informationstechnologische Aufgabe darin, sich den Gefahren, die sich durch die ‚Vernetzung in der Produktion' ergeben, zu stellen. Dazu bedarf es im Wesentlichen zweier Dinge: zum einen der Risikoanalyse und -bewertung, zum anderen der Risikominimierung, wenn nicht sogar des Risikoausschlusses bzw. der -vermeidung durch geeignete Maßnahmen.

In einem großen Unternehmen entsteht hier oftmals das erste organisatorische Problem. Während die finanziellen Risiken oftmals im Bereich Finance und Controlling bewertet werden, sind die Analyse und Beseitigung konkreter technischer Risiken meist Aufgabe des IT-Bereichs. Diese Diskrepanz wird besonders deutlich, wenn man sich die Geschäftsberichte im Jahr der geschilderten Wurmattacke und im Jahr nach der Wurmattacke am Beispiel der DaimlerChrysler AG anschaut:

> „Darüber hinaus könnten unsere betrieblichen Abläufe durch Unterbrechungen in den Rechenzentren beeinträchtigt werden. Hierzu wurden Sicherheitsmaßnahmen und Notfallpläne erstellt. Andere IT-Risiken aus dem Netzwerk-, Applikations- und System-Management sowie Outsourcing-/Lieferanten-Management haben zwar eine sehr niedrige Eintrittswahrscheinlichkeit, könnten sich aber im Falle des Risikoeintritts ebenfalls spürbar negativ auf das Ergebnis auswirken."[3]

> „Darüber hinaus könnten unsere betrieblichen Abläufe durch Unterbrechungen in den Rechenzentren beeinträchtigt werden. Hierzu wurden Sicherheitsmaßnahmen und Notfallpläne erstellt. Andere IT-Risiken aus dem Netzwerk-, Applikations- und System-Management sowie Outsourcing-/Lieferanten-Management haben zwar eine sehr niedrige Eintrittswahrscheinlichkeit, könnten sich aber im Falle des Risikoeintritts ebenfalls spürbar negativ auf das Ergebnis auswirken."[4]

[3] DaimlerChrysler AG (2006, S. 60)
[4] DaimlerChrysler AG (2007, S. 70)

Sowohl im Geschäftsbericht aus 2005 als auch aus 2006 wird das IT-Risiko im Besonderen auf Rechenzentren bezogen. Andere IT-Risiken, wie z. B. ein Viren- oder Wurmbefall, werden mit einer sehr niedrigen Eintrittswahrscheinlichkeit bewertet. Der Unterschied zwischen Berichtssicht und Tatsachen ist hier deutlich zu erkennen und lässt vermuten, dass technische Aspekte bei der Risikobewertung eine untergeordnete Rolle spielen. Eine abgestimmte Vorgehensweise zwischen beiden Disziplinen zu etablieren bzw. eine Bewertungsmethode zu entwickeln, die auch die konkreten technischen Risiken berücksichtigt, ist der Gegenstand der vorliegenden Dissertation.

Zur Entwicklung einer Bewertungsmethode für das IT-Risikomanagement zur Bewertung der Risiken durch die Vernetzung in der Produktion wird sich die vorliegende Dissertation folgendermaßen gliedern: Im ersten Schritt wird der gegenwärtigen Stand zur Lösung der aufgezeigten Problematik darlegt. Dies beinhaltet zunächst einen Blick auf die verschiedenen Methoden zur Risikobewertung. Im Fokus stehen hier die für die unterschiedlichen Unternehmensformen gesetzlich vorgeschriebenen Methoden, aber auch über diesen Standard hinausgehende Methoden. Es folgt eine genaue Definition des Begriffs Produktion und des typischen Aufbaus eines Produktionsbetriebes und seiner Merkmale. In diesem Zusammenhang wird auch die Vernetzung der Produktion sowohl im prozessualen als auch im technischen Sinn aufzuzeigen sein. Die technischen Gegebenheiten werden genau erläutert und auf die Risiken einzelner Komponenten, wie beispielsweise Speicherprogrammierbare Steuerungen (SPS), konkret eingegangen. An dieser Stelle werden auch die unterschiedlichen Formen der Sabotage beleuchtet. Auf Basis der aktuellen Forschung werde ich dann ein eigenes Vorgehen zur Risikobewertung entwickeln.