Inhaltsverzeichnis

Geleitworte 5

Vorwort 9

1 Einleitung 15
1.1 Zweck und Zielgruppe 15
1.2 Aufbau des Buches 16
1.3 Abgrenzung 17

2 Organisationsanforderungen für den Aufbau einer Industrial IT Security 19
2.1 Abgrenzung Office IT–Produktion 20
2.2 Organisation und Industrial IT Security 23
2.3 Policies, Standards, Leitlinien und deren Anwendbarkeit 24
2.4 Gefährdung der Industrial IT Security und abgeleitete Anforderungen 25
2.4.1 Problemfeld «Fehlende Awareness der Mitarbeiter» 25
2.4.2 Unzureichende Dokumentation der Anwendungen und Systeme («Graue IT») 26
2.4.3 Fehlende Überwachung der Infrastruktur und Anwendungen 27
2.5 Organisatorische Maßnahmen 27
2.5.1 Dedizierte IT-Security-Organisation für die Produktion 28
2.5.2 Sicherheitsleitlinie für die Produktion 30
2.5.3 Aufgaben, Kompetenzen, Verantwortlichkeiten und Prozesse 30
2.6 Prozesse und Prozess-Management in der Produktions-IT 31
2.6.1 Basisprozess Asset-Management 32
2.6.2 Incident-Management und Service Desk 33
2.6.3 Problem-Management 33
2.6.4 Change-Management 34
2.7 Basisprozesse für das Management der Industrial IT Security 34

3 Automatisierte Produktionssysteme 37
3.1 Abgrenzung 37
3.2 Nutzung von Client-Rechnern in der Produktion 37
3.2.1 Härtung von Windows-Rechnern 38
3.2.2 Altlasten: Veraltete Client-Betriebssysteme 40
3.2.3 Umstieg auf eine aktuelle Betriebssystemversion 41
3.2.4 Whitelisting, Application Control und Embedded Security Systems 41
3.2.5 Trennung mittels Firewall und Netzwerkzonen 42
3.2.6 Strikte Abtrennung kritischer Systeme vom Netzwerk 43
3.3 Erstellung angemessener Dokumentation 43
3.3.1 Komplette Übersicht der IT für Anlagen (IT Asset-Inventory) 43
3.3.2 Kontext-Diagramm für Anlagen 44
3.3.3 Betriebshandbuch für Maschinen und Anlagen 44
3.4 Nutzung von Fremdhardware in der Produktion 44

4 (IT-) Netzwerktechnik in der Produktion 47
4.1 Einleitung 47
4.2 Bedrohungen und bekannte Angriffsmuster 48
4.3 Abgrenzung zu anderen behandelten Themen 50
4.4 Spezielle Anforderungen aus der Produktion 50
4.5 Netzwerk-Zonierung 50
4.5.1 Analyse der Kommunikationswege (Anlagenkomponenten) 50
4.5.2 Zonierungsbeispiel 53
4.5.3 Gerätetypen und Betriebssystem-Versionen im Anlagennetz 54
4.5.4 Netzwerktypen und Bustechnologien im Produktionsnetz 55
4.5.5 Betrachtung möglicher Bedrohungen 56
4.5.6 Betrachtung von Schutzmaßnahmen beim Netz-Zonenübergang 56
4.5.7 Sicherheitselemente am Netz-Zonenübergang 57
4.5.8 Netz-Zonen und Adressierung (IPv4) 58
4.5.9 Redundante Auslegung von Sicherheitselementen am Übergang 59
4.5.10 Verschlüsselung in den Produktionsnetzen 59
4.6 Anforderungen an den sicheren Netzwerkbetrieb 60
4.6.1 Remote Access 60
4.6.2 Stand der Software und Aktualisierungen 60
4.6.3 Zugelassene Geräte und Systeme 60

5 Sicherheit von SCADA-/ICS-Komponenten 63
5.1 Einführung 63
5.2 Produktionsdaten vs. Steuerungsinformationen 63
5.3 Schutz von Steuerungsinformationen und Kommunikation 64
5.4 Absicherung der Steuerungs-Infrastruktur 65
5.5 Absicherung der Steuerungskomponenten 65

6 Verzeichnisdienste in der Produktion 67
6.1 Allgemeines 67
6.2 Abgrenzung 67
6.3 Einfluss der Netzwerkplanung und Architektur 68
6.4 Nutzen von Verzeichnisdiensten in der Produktion 68
6.4.1 Nutzungsarten und Modelle 69
6.4.2 Spezifische Anforderungen der Produktion 72
6.4.3 Nutzung des Active Directory 72
6.4.4 Vertrauensmodelle für Produktions-ADs im Vergleich 73
6.5 Namenskonventionen: Anforderungen an die Namensräume 74
6.6 Domain Controller mit eindeutigen IP 75
6.7 Zonenkonzepte und AD 76
6.8 AD und IPv4 77
6.9 AP und IPv6 77
6.10 Kerberos im AD 78
6.11 Härtung und Monitoring 79
6.11.1 Härtung von AD-Servern 79
6.11.2 Härtung des ADs und seiner Komponenten 79
6.11.3 Monitoring und Überwachung des ADs 80
6.11.4 Administrative Zugriffe über PAM-Systeme 80

6.12 Administrations- und Betriebskonzept ... 81
6.12.1 Domänen und Organisationseinheiten (OUs) ... 81
6.12.2 Rollen im AD ... 81
6.12.3 Namenskonzept und Namensräume ... 82
6.13 Administrationsmodell ... 82
6.14 Richtlinien und Group Policy Objects (GPOs) ... 84
6.15 Datensicherheit im Verzeichnisdienst ... 85
6.15.1 Domain Controller (DC) – Ausfallsicherheit und Redundanz ... 85
6.15.2 Physische oder virtuelle Domain Controller ... 86
6.15.3 Backup und Recovery des ADs ... 87
6.16 Lizenz-Aktivierung durch Key Management Server (KMS) ... 88

7 Sicherheit von Anwendungen ... 89
7.1 Einführung ... 89
7.2 Risikobewertung für Industrial-IT-Anwendungen ... 89
7.3 Software-Auswahlverfahren ... 91
7.4 Kryptografie im Rahmen der Software-Akquise ... 93
7.5 Aspekte der sicheren Software-Entwicklung ... 93
7.5.1 Funktionstrennung (Segregation of Duties, SoD) ... 93
7.5.2 Secure Software Development Lifecycle (SDL) ... 93
7.6 Sichere Integration in die Produktionslandschaft ... 96
7.6.1 Mindestanforderungen für die sichere Integration ... 96
7.6.2 Integration der Software in das bestehende Security-Management ... 97
7.6.3 Applikations-Integration über eine DMZ / Service-Zone ... 97
7.7 Sicherer Betrieb von Industrial-IT-Anwendungen ... 97
7.7.1 Verfügbarkeit von Applikationen in Produktionsanlagen ... 98
7.7.2 Integrität von Applikationen in Produktionsanlagen ... 98
7.8 Absicherung der (Fern-) Wartung ... 99
7.9 Schwachstellen-Management durch den Hersteller ... 99
7.10 Patch-Management ... 100
7.11 Zugriffsschutz für Software ... 100
7.12 Notwendigkeit eines dauerhaften Internet-Zugriffs ... 101
7.13 Dokumentation ... 101

8 Risikomanagement und die industrielle IT-Sicherheit ... 103
8.1 Einführung ... 103
8.2 Risiko – Was ist das eigentlich? ... 103
8.2.1 Erste Risikoanalyse – Eine Standortbestimmung ... 105
8.2.2 Erweiterte Risikoanalyse – Risikomanagement ... 107
8.2.3 Tool-Unterstützung für das ISMS ... 108

9 Ausblick Industrie 4.0 ... 109
9.1 Basis der Industrie 4.0 im Rahmen der Digitalisierung ... 109
9.2 Netz-Zonen und Industrie 4.0 ... 113
9.3 I4.0 und Kommunikation ... 114
9.4 Neue I4.0-Kommunikation – Über APIs in die Cloud ... 116

Abkürzungen 119

Glossar 123

Literaturverzeichnis 133

Quellenverzeichnis 135

Stichwortverzeichnis 137