

Inhaltsverzeichnis

1	Einführung	11
2	Zum Begriff Security im Zusammenhang mit Industrie 4.0	18
2.1	Paradigmenwechsel in der Produktion	18
2.1.1	Industrie gestern und heute	18
2.1.2	Paradigmenwechsel in der Produktion	19
2.2	Security meets Safety	20
2.3	Aus Erfahrung lernen	21
2.3.1	Klassische IT	21
2.3.2	Produktions-IT	22
2.3.3	Bestandssysteme	23
2.4	Warum Konzepte aus der Office-IT nicht einfach auf Industrie 4.0 übertragen werden können	24
2.5	Wie sicher ist sicher?	26
2.5.1	Wieso es keine absolute Sicherheit gibt	26
2.5.2	Sicherheit ist eine momentane Bestandsaufnahme	28
2.5.3	Sicherheit und Risiko	28
2.5.4	Funktionale und nichtfunktionale Sicherheitsaspekte	29
2.5.5	Was bedeutet also nun Sicherheit?	30
2.6	Sicherheit und RAMI	30
2.7	Schutzziele der IT-Sicherheit	33
2.7.1	Was sind also die Schutzziele der IT-Sicherheit für Industrie 4.0?	34
2.7.2	IP-Schutz der Produktionsdaten (Datenvor-Vertraulichkeit)	35
2.7.3	Authentizität von Komponenten und Daten	36
2.7.4	Piraterieschutz (Daten- und Objekt-Integrität)	36
2.7.5	Verfügbarkeit der Produktion (Daten- und Objekt-Verfügbarkeit)	36
2.8	Betrachtungsumfang von Security	37
2.8.1	Security	37
2.8.2	Security by Design	37
2.8.3	Security at Large	38

3	Angriffe – Szenarien und Vorfälle	39
3.1	Angriffe gegen das Schutzziel Verfügbarkeit	40
3.2	Angriffe gegen das Schutzziel Vertraulichkeit	43
3.3	Angriffe gegen das Schutzziel Authentizität	44
3.4	Angriffe gegen das Schutzziel Integrität	45
4	Bedrohungsmodellierung	47
4.1	Die IUNO-Methode zur Bedrohungs- und Risikobewertung ...	48
4.2	Anwendungsbeispiel zur Bedrohungs- und Risikobewertung...	51
4.3	Informationsgewinnung	53
4.3.1	Erfassung der Funktionen und Annahmen	53
4.3.1.1	Identifizierung und Beschreibung der Funktionen des Untersuchungsgegenstands	54
4.3.1.2	Erfassung vorhandener Sicherheitsmechanismen und ihrer Abhängigkeiten	54
4.3.1.3	Erfassung von vertrauenswürdigen Akteuren und Umgebungen	54
4.3.1.4	Erfassung von Annahmen auf Organisationsebene	55
4.3.2	Erfassung der Architektur	56
4.3.2.1	Tabellarische Erfassung der Schlüsselmerkmale	57
4.3.2.2	Tabellarische Erfassung von Informationen und Begründungen zur Architektur	57
4.3.2.3	Erfassung des internen Aufbaus auf Basis eines Datenflussdiagramms	58
4.3.2.4	Erfassen bekannter Schwachstellen und Verwundbarkeiten aus Vorversionen	64
4.3.3	Erfassung der Angriffsfläche, Akteure und Drittanbieter-Komponenten	64
4.3.3.1	Erfassung der Akteure	65
4.3.3.2	Erfassung exponierter Entitäten	66
4.3.3.3	Erfassung der Sicherheitseigenschaften von Drittanbieter-Komponenten	66
4.4	Schutzbedarfsermittlung	68
4.4.1	Definition eines Angreifermodells	68
4.4.1	Erstellung eines Wertekatalogs	70
4.4.1.1	Erfassung von Stakeholdern	70
4.4.1.2	Erfassung von Werten (Assets)	71
4.4.1.3	Erfassung von Werten auf Basis von Asset-Klassen nach Common Criteria	72
4.4.1.4	Erfassung von Assets und Stakeholdern auf Basis von CORAS Asset-Diagrammen	72

4.4.1.5	Erfassung von Datenrepräsentationen der Assets	75
4.4.2	Identifizierung und Bewertung der Schutzziele	78
4.5	4.5.1 Analyse der Bedrohungen	80
	4.5.2 Identifikation der Bedrohungen	80
	4.5.3 Erfassung von Bedrohungen mittels STRIDE durch Ableitung aus Datenflussdiagrammen	80
	4.5.3 Erfassung von Bedrohungen auf Basis von CORAS-Bedrohungsdiagrammen	82
5	5. Risikomanagement für Industrie 4.0	87
5.1	Der Risikomanagementprozess	87
5.2	Risikomodellierung und Risikoanalyse	88
5.3	5.3 Die IUNO-Methode als Vorgehensweise zur Risikobewertung	90
5.4	5.4 Ablauf der Risikoanalyse	95
5.5	5.5 Berechnung der Verlustfrequenz	101
	5.5.1 Bedrohungs frequenz bestimmen	102
	5.5.2 Verwundbarkeit bestimmen	103
	5.5.3 Verlustfrequenz aus Bedrohungs frequenz und Verwundbarkeit ableiten	106
5.6	5.6 Berechnung der erwarteten Verlusthöhe anhand von Verlustformen und Aktionen	108
	5.6.1 Verlustformen und Aktionen erfassen	108
	5.6.1.1 Produktivität	109
	5.6.2.2 Reaktion	109
	5.6.2.3 Wiederbeschaffung	110
	5.6.2.4 Wettbewerbsvorteil	110
	5.6.2.5 Bußgelder und Rechtsurteile	111
	5.6.2.6 Ruf schädigung	111
	5.6.2.7 Safety	112
	5.6.2.8 Erwartete Verlusthöhe berechnen	114
	5.6.3 Erwartete Verlusthöhe bei Safety-Verlusten berechnen	117
	5.6.3.1 Bestimmung der Verlusthöhe bei Safety-Verlusten	118
	5.6.4 Berechnung des resultierenden Risikos aus Verlustfrequenz und erwarteter Verlusthöhe	118
	5.6.5 Verluste messen und abschätzen	120
	5.6.5.1 Indikatoren	121
	5.6.5.2 Einbettung der Risikoanalyse in das Risikomanagement	130

6	Elemente eines Sicherheitskonzepts	132
6.1	Architekturen für IT-Sicherheit in Industrie 4.0	132
6.1.1	IT-Sicherheit bei der Herstellung von Komponenten...	133
6.1.2	IT-Sicherheit bei der Konfiguration von Komponenten	135
6.1.3	IT-Sicherheit der zum Zugang benutzten Anwendungen	138
6.1.3.1	Sicherheit bei der Auslagerung von Funktionalität auf externe Systeme	139
6.1.3.2	Best Practices Kryptographie	140
6.1.3.3	Weitere Aspekte	141
6.2	Digitale Identitäten	143
6.3	Digital Rights Management	144
6.4	Piraterieschutz	147
6.5	Normen, Standards und Best Practices	148
6.6	SIEM	161
6.7	Künstliche Intelligenz und Machine Learning in der Industrie 4.0	166
6.7.1	Begriffsklärung	166
6.7.2	Lernverfahren	167
6.7.2.1	Überwachtes Lernen	167
6.7.2.2	Uniüberwachtes Lernen	168
6.7.2.3	Teilüberwachtes Lernen	168
6.7.2.4	Bestärkendes Lernen	169
6.7.2.5	Deep Learning	169
6.7.3	Anwendung von Machine Learning in der Industrie 4.0	171
6.7.3.1	Produktivitätssteigernde KI	172
6.7.3.2	Angriffserkennung in industriellen Anlagen....	173
6.7.4	IT-Sicherheit bei der Verwendung von KI und ML in der Industrie 4.0	176
6.8	Organisationsanforderungen für IT-Sicherheit in Industrie 4.0	179
6.9	Mitarbeiter als Risiko – Qualifikation und Schaffung von Sicherheitsbewusstsein	183
7	Ein Blick auf das Recht	186
7.1	Die Datenschutz-Grundverordnung in der Industrie 4.0	187
7.1.1	Begriffsbestimmungen	187
7.1.2	Datenschutz ist Menschenschutz	189
7.1.3	Relevanz des Datenschutzrechts für die Industrie 4.0	189
7.1.4	Anforderungen der Datenschutz-Grundverordnung	191
7.1.4.1	Datenschutz-Grundsätze	191

7.2	Das IT-Sicherheitsgesetz	209
7.2.1	Betreiber von Webangeboten	209
7.2.1.1	Telekommunikationsunternehmen	210
7.2.1.2	Betreiber kritischer Infrastrukturen	210
7.2.1.3	Ausblick	211
8	Ausblick	212
8.1	Neue Faktoren in der Sicherheitsbetrachtung	213
8.2	Ausblick Post-Quantum	214
8.3	Die Plattform Industrie 4.0	216
9	Glossar und Abkürzungsverzeichnis	217
10	Literaturverzeichnis	229