Inhalt

Teil 1 9

1 Einleitung 9
1.1 Was ist überhaupt Cybersicherheit? 11
1.2 Ist Cybersicherheit gleich IT-Sicherheit? 12
1.2.1 Fall 1 „Vertrauliche Papiere im Drucker“ 12
1.3 Cybersicherheit, wie sie bis heute verstanden wird 12

2 Derzeitige betriebliche Praxis 15
2.1 NIS2-Richtlinie – was kommt neu? 18
2.2 Interessante Normen für Cybersicherheitsmaßnahmen 22
2.2.1 Vergleich TRBS 1115 und TRBS 1115 Teil 1 23

3 Aufgaben von IT-Sicherheit, Elektrosicherheit und Arbeitssicherheit 27
3.1 Aufgaben und Grenzen der IT-Sicherheit 27
3.2 Die Top 5 IT-Sicherheitsmaßnahmen, die jedes Unternehmen ergreifen sollte 28
3.3 Aufgaben und Grenzen der Elektrosicherheit 29
3.4 Aufgaben und Grenzen der Arbeitssicherheit 37
3.5 Gemeinsame Aufgaben der IT-Sicherheit, Elektrosicherheit und Arbeitssicherheit 40
3.6 Integrierte Sicherheitspraxis: Arbeitssicherheit, Elektrosicherheit und IT-Sicherheit effektiv vereinen für größere Unternehmen 42
3.6.1 Einsatz von Technologie 42
3.6.2 Integrierte Sicherheitsrichtlinien und -verfahren 43
3.6.3 Interdisziplinäres Sicherheitsteam 43
3.6.4 Compliance-Management 43
3.6.5 Notfall- und Krisenmanagement 43
3.6.6 Fazit 43
3.7 Kleinere Unternehmen und deren integrierte Sicherheitspraxis 44
3.8 Inhalte und Abgrenzung von IT-Sicherheit, Elektrosicherheit und Arbeitssicherheit 46
3.9 Was beinhaltet IT-Sicherheit? 48
3.9.1 Was beinhaltet IT-Sicherheit kombiniert mit Arbeitssicherheit? 50
3.9.2 Was beinhaltet IT-Sicherheit kombiniert mit Elektrosicherheit? 51

3.9.3 Was verbindet die IT-Sicherheit mit Elektrosicherheit und Arbeitssicherheit? 52

4 Die VEFK und die Cybersicherheit 55
4.1 Verantwortlichkeiten 55
4.2 Hauptaufgabe ist die Klärung der Informationsschnittstelle 56
4.3 Was kommt auf die VEFK bei vernetzten Arbeitsmitteln neu hinzu? . . . 57
4.3.1 Vorgehensweise 57

5 Wer kann in der Praxis die Cybersicherheit unterstützen? 61
5.1 Was kann eine Elektrofachkraft unternehmen, damit in seinem Bereich keine Cyberangriffe stattfinden könnten? 61
5.1.1 Beispiel Aufzug 62
5.1.2 Aber wie macht das ein Hacker? 64
5.1.3 Beispiel Produktionsmaschine 65
5.2 Was kann eine Sicherheitsfachkraft unternehmen, damit in ihrem Bereich keine Cyberangriffe verhindert werden? 66
5.2.1 Beispiel Zugangsberechtigung 67
5.2.2 Fazit 69

6 Was kann passieren, wenn man seine Cybersicherheit in der Produktion nicht im Griff hat? 71
6.1 Idee eines Leitfadens zur Einführung „Cybersicherheit“ 73
6.2 Was kann ein OTler in der Produktion unternehmen, damit in seinem Bereich keine Cyberangriffe stattfinden könnten? 75
6.2.1 Wie könnte so ein Sicherheitsplan aussehen? 76
6.3 Checklisten und Arbeitshilfen zur Grobanalyse 78
6.3.1 Checkliste „Allgemein“ 79
6.3.2 Checkliste „Maschinen mit Datenschnittstelle“ 81
6.3.3 Checkliste „Haus- und Gebäudetechnik mit IP-Schnittstellen“ 82
6.3.4 Checkliste „Produktionsmaschinen mit IP-Schnittstelle“ 83
6.3.5 Checkliste „Updates“ 84
6.3.6 Checkliste „Netzwerkinfrastruktur“ 85
6.3.7 Checkliste „Prozesse“ 86
6.3.8 Checkliste „Software Security“ 87
6.3.9 Checkliste „Rechtliche normative Vorgehensweise/Grundlage“ 88

Teil 2 89

7 Ziele des zweiten Teils des Buches 89
7.1 Zielgruppen 89
7.2 Themenschwerpunkte 90

8 Cybersicherheit im Maschinen- und Anlagenbau 93
8.1 Klassisches Verständnis von Cybersicherheit für KMUs 93
8.2 Der Dreiklang von Cybersicherheit in KMUs 94
8.3 Cybersicherheit in der Praxis 96
8.3.1 Gefahrenquellen im operativen Betrieb 97
8.4 Zusammenfassung 100

9 Ertüchtigung ihrer Organisation 101
9.1 Sicherheitsmanagement – ein erster Ansatz 101
9.2 Cybersicherheitsmanagement – die TOPI-Methode als Leitfaden 103
9.3 Messung und Kontrolle von Cybersicherheitszielen 106
9.3.1 Zielformulierung auf Basis einer Risikoanalyse 106
9.3.2 Wirksamkeit einer Cybersicherheitsstrategie 107
9.4 KVP – Der „ewige Kreislauf“, ein dynamischer Ansatz 110

10 „How-to“-Anleitungen für zentrale Werkzeuge und Methoden des Cybersicherheitsmanagements 127
10.1 Risikoanalyse und -bewertung 127
10.1.1 Kontext einer Risikoanalyse erfassen 127
10.1.2 System abgrenzen und verstehen 128
10.1.3 Gefährdungen identifizieren 129
10.1.4 Schwachstellen identifizieren 130
10.1.5 Gefährdungen entschärfen 131
10.2 Notfall-/Krisenmanagement und Notfallpläne 133