Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

Sicherheit für die digitale Transformation der Produktion

Wien, 2020

Inhalt

1 Einleitung 4

2 Ausgangssituation in Österreich: Analyse des Sicherheitsbewusstseins 6

2.1 Bewusstsein zum Thema Security 6

2.2 Reifegrad im Bereich Security 12

2.3 Security-Investitionen 15

2.4 Bedrohungsszenarien 16

3 Steigende Sicherheitsanforderungen als Herausforderung für die Industrie 20

3.1 Neue Sicherheitsanforderungen 20

3.1.1 Differenzierung von IT und OT als wichtige Herausforderung für Industrial Control Systems Security 20

3.1.2 Referenzarchitekturmodell RAMI 4.0 21

3.1.3 Die Normenreihe IEC 62443 23

3.1.4 Sicherheitsanforderungen 25

3.1.5 Organisatorische Anforderungen 25

3.1.6 Technische Anforderungen 27

3.2 Industrielle Praxis und Herausforderungen 30

3.3 Bedeutung von Security-Fachkräften 31

3.4 Good-Practice-Beispiele 32

4 Security als Standortfaktor 39

4.1 Spezifika österreichischer Industrieunternehmen 39

4.2 Vorhandene Kompetenzen, Lösungen und Produkte 41

4.3 Kommunikation und Zusammenarbeit bei Sicherheitsvorfällen 43

4.4 Handlungsempfehlungen für Industrieunternehmen 45

4.5 Handlungsempfehlungen für die Politik 47

4.5.1 Forschung und Entwicklung 47

4.5.2 Aus- und Weiterbildung 48

4.5.3 Standardisierung und Zertifizierung 50

4.5.4 Bewusstseinsbildung und Kommunikation 51

5 Zusammenfassung 53

Abbildungsverzeichnis 57

Literaturverzeichnis 58

Abkürzungen 60

Impressum 63

1 Einleitung

Information Technology (IT)-Systeme sind bereits gegenwärtig das Herzstück vieler Produktionssysteme. Informationssicherheit ist dabei eine wichtige und erfolgskritische Herausforderung: Aufgrund der Verbindung von IT und OT (Operational Technology) entsteht in der Industrie 4.0 jedoch eine neue Qualität von Abhängigkeiten und Risiken für Produktionssysteme sowie sensible Personen- und Unternehmensdaten. Zentral ist hier die Entwicklung integrierter Sicherheitskonzepte und -architekturen sowie eine sichere Migration von Altsystemen zu Industrie-4.0-Lösungen. Ohne eine Gewährleistung geeigneter Sicherheitsstandards ist eine weitreichende Realisierung von Industrie 4.0 fragwürdig. Die Informationssicherheit steht dabei in Verbindung mit Fragen der BenutzerInnenfreundlichkeit, Akzeptanz und Wirtschaftlichkeit. Ein entsprechendes Problembewusstsein bei Führungspersonal und MitarbeiterInnen ist dabei ein erster Schritt auf dem Weg zur Gewährleistung der IT-Security.

Diese Studie hat das Ziel, ein Bewusstsein für die zentrale Rolle von Security in der Industrie 4.0 zu schaffen und Security als wesentlichen Standortfaktor für Österreich zu etablieren. Dazu wird zunächst in Abschnitt 2 die aktuelle Sicherheitslage in österreichischen Produktionsbetrieben analysiert. Sodann werden in Abschnitt 3 die neuen Sicherheitsanforderungen, die mit der Vernetzung und Automatisierung einhergehen, dargestellt. Schließlich werden in Abschnitt 4 Chancen, Barrieren und Potenziale für den Standort Österreich aufgezeigt, die sich dadurch ergeben.

Eine wichtige Datenbasis für diese Studie stellt der European Manufacturing Survey 2018 dar. Diese Erhebung ist die größte Studie zum Einsatz von industriellen Technologien in Österreich. Sie wurde im Herbst 2018 vom Austrian Institute of Technology (AIT) in Abstimmung mit einem internationalen Konsortium durchgeführt. Aufgrund der großen Bedeutung des Sicherheitsthemas wurde der international standardisierte Fragebogen für Österreich um einige spezifische Sicherheitsfragen erweitert, so dass eine zuverlässige empirische Datenbasis für diese Studie vorhanden ist. Darüber hinaus wurden Interviews mit unterschiedlichen Akteuren auf Nachfrage- und Angebotsseite durchgeführt sowie ein Workshop mit österreichischen ExpertInnen sowie Mitgliedern der ExpertInnengruppe Security und Safety des Vereins Industrie 4.0[1] organisiert.

[1] https://plattformindustrie40.at/

Auf Basis der breiten und validen empirischen Befunde werden in Abschnitt 4.4 Handlungsempfehlungen formuliert, die für Unternehmen der Industrie und des Sicherheitssektors konkrete Anhaltspunkte geben, wie die Informations- und Kommunikationssicherheit erhöht werden kann. Für die öffentliche Hand gibt die Studie in Abschnitt 4.5 Hinweise zur Gestaltung von Rahmenbedingungen und zeigt einen möglichen FTI-politischen Bedarf auf.

2 Ausgangssituation in Österreich: Analyse des Sicherheitsbewusstseins

2.1 Bewusstsein zum Thema Security

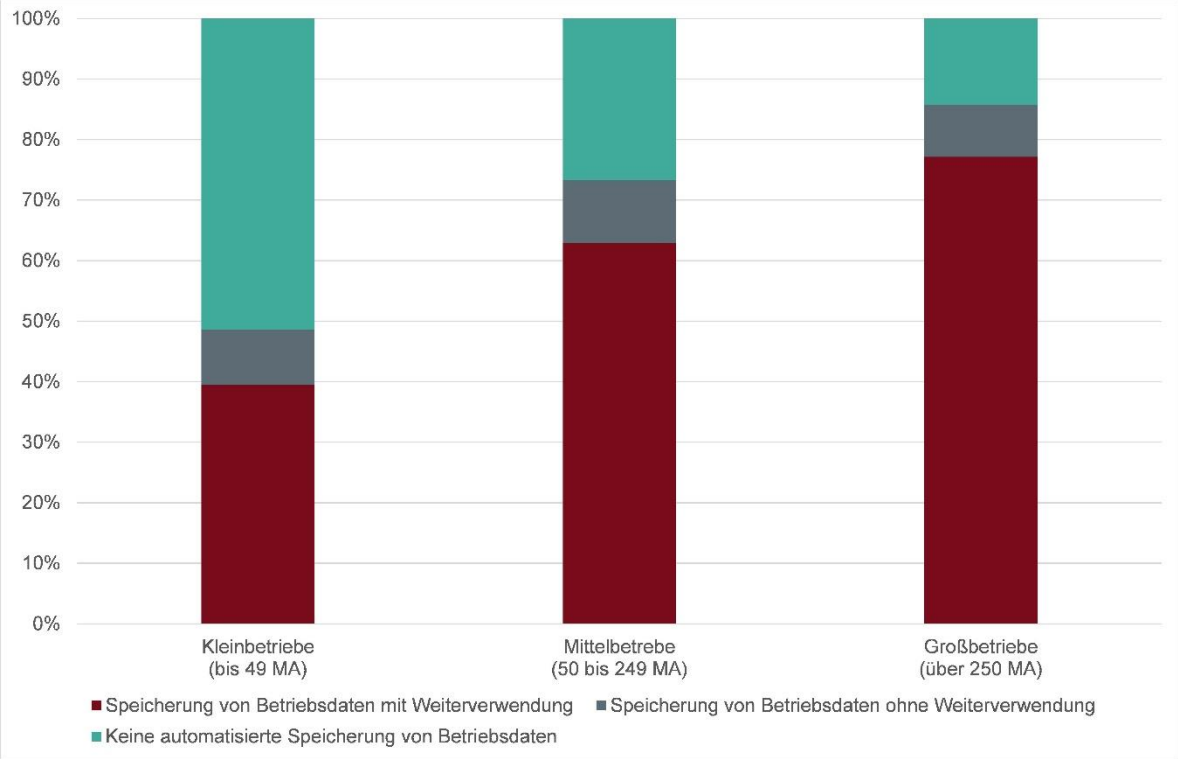
Mangelndes Sicherheitsbewusstsein gilt als eine wichtige Ursache für Sicherheitsrisiken. Bislang gab es in Österreich keine empirischen Befunde über das Thema Security im produzierenden Bereich. Mit dem European Manufacturing Survey (EMS) wurden 2018 einige spezifische Fragen zur Bedeutung von Security gestellt.[2] Das Bewusstsein zum Thema Security in der Produktion wird im EMS durch drei Fragen erfasst:

1. Wie viele Betriebe in der Produktion haben Maschinen oder Anlagen, die automatisiert Betriebsdaten speichern;
2. Wie wird das Bedrohungspotential durch die Betriebe selber eingeschätzt;
3. In welchen Umfang werden etwaige Sicherheitsmaßnahmen regelmäßig intern und/oder extern überprüft.

Die Ergebnisse des EMS zeigen, dass die automatisierte Speicherung von Betriebsdaten mittlerweile weit verbreitet ist und mit der Betriebsgröße steigt. Bei Großbetrieben mit über 250 MitarbeiterInnen ist dies bereits die Regel, fast 90% dieser Betriebe geben an, automatisiert Betriebsdaten zu speichern und auch über 80% der Betriebe nutzen in der Folge diese Daten zur Optimierung der Produktionsabläufe, der Einsatz- bzw. Auslastungsplanung, der Planung von Wartung und Instandhaltung sowie zur Erstellung von Produktivitäts- oder Leistungskennzahlen. Auch drei von vier Mittelbetrieben mit 50 mit 249 MitarbeiterInnen speichern automatisiert Betriebsdaten, die Verbreitung bei Kleinbetrieben mit 20 bis 49 MitarbeiterInnen ist mit rund der Hälfte der Betriebe geringer.

[2] Mit dem European Manufacturing Survey (EMS), der in Österreich vom Austrian Institute of Technology durchgeführt wird, werden in einem dreijährigen Zyklus Entwicklungstrends und Strategien österreichischer Industrieunternehmen untersucht. Die Befragung wurde in allen Branchen des produzierenden Sektors durchgeführt und umfasst Betriebe mit mehr als 20 MitarbeiterInnen. 2018 haben an der Befragung insgesamt 258 Betriebe teilgenommen, womit ein, was die Branchen und Größenklassen betrifft, repräsentatives Sample zur Verfügung steht.

Abbildung 1: Speicherung von Betriebsdaten nach Betriebsgrößen



Quelle: EMS 2018, eigene Berechnungen
Frage: „Haben Sie in Ihrer Produktion Maschinen oder Anlagen, die automatisiert Betriebsdaten speichern?"
Anmerkung: n=250 Betriebe der österreichischen Sachgütererzeugung ab 20 MitarbeiterInnen (MA)

Obwohl der Anteil der Betriebe, die automatisiert Betriebsdaten speichern, mit der Betriebsgröße steigt, ist die absolute Anzahl dieser Betriebe im Bereich der Klein- und Mittelbetriebe am größten. Legt man die Grundgesamtheit der produzierenden Betriebe laut der Leistungs- und Strukturerhebung der Statistik Austria zu Grunde[3], sammeln jeweils etwa 1.100 Klein- bzw. Mittelbetriebe automatisiert Betriebsdaten, während die absolute Anzahl der entsprechenden Großbetriebe mit unter 450 Betrieben deutlich geringer ist.

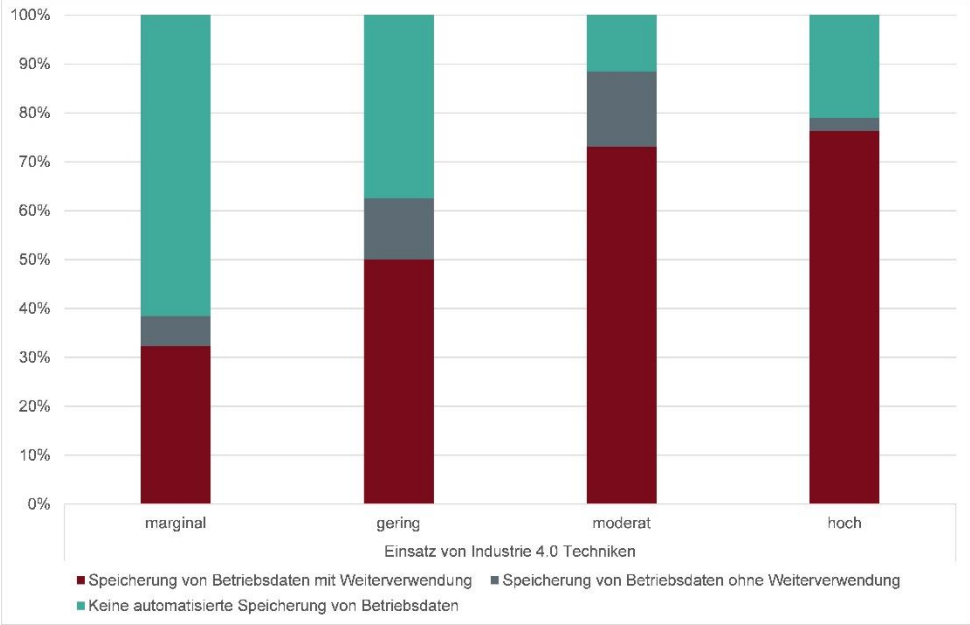
Die automatisierte Speicherung, und in der Folge auch Nutzung von Betriebsdaten steigt nicht nur mit der Betriebsgröße deutlich an, sondern auch mit dem Einsatz moderner, digitaler Produktionstechniken. Im Rahmen des EMS und der darin abgefragten Bedeutung unterschiedlicher Produktionstechnologien kann der Reifegrad von Industrie 4.0 erfasst werden. Dabei wird der Einsatz von 13 Produktions- und Prozesstechniken herangezogen, um den Reifegrad zu bestimmen. Der Schwerpunkt liegt hier auf der technologischen Ausstattung, die notwendig ist, um in weiterer Folge Industrie 4.0 verwirklichen zu können. Berücksichtigt werden Prozesstechniken, digitale Techniken, künstliche Intelligenz, der

[3] 2161 Betriebe mit 20 bis 49 MitarbeiterInnen, 1469 Betriebe mit 50 bis 249 MitarbeiterInnen sowie 465 Betriebe ab 250 MitarbeiterInnen

Einsatz von 3D-Druck sowie unterschiedliche Formen flexibler Robotiklösungen. Da Industrie 4.0 unter anderem auch geänderte Anforderungen an die MitarbeiterInnenqualifikation bedingt, wurden Weiterbildungsmaßnahmen in Bezug auf den Umgang mit Big Data ergänzend für den Industrie-4.0-Reifegrad berücksichtigt. Das Ausmaß des aktuellen und geplanten Einsatzes dieser Techniken ist ein robuster Indikator für die technologische „Readiness" in Bezug auf Industrie 4.0.[4]

Der EMS illustriert, dass die Speicherung von Betriebsdaten mit dem Industrie-4.0-Reifegrad zunimmt (vgl. Abbildung 2). 75% der Unternehmen, die als Industrie-4.0-Frontrunner bezeichnet werden können (Reifegrad hoch), speichern Betriebsdaten, während dies bei der Gruppe der Betriebe, die Industrie-4.0-Techniken nur vereinzelt einsetzen lediglich rund ein Drittel ist. Interessant ist auch der Befund, dass bei den Frontrunner-Unternehmen kaum Betriebe dabei sind, die Daten nur speichern, aber nicht nutzen.

Abbildung 2: Speicherung von Betriebsdaten und Industrie 4.0 Reifegrad

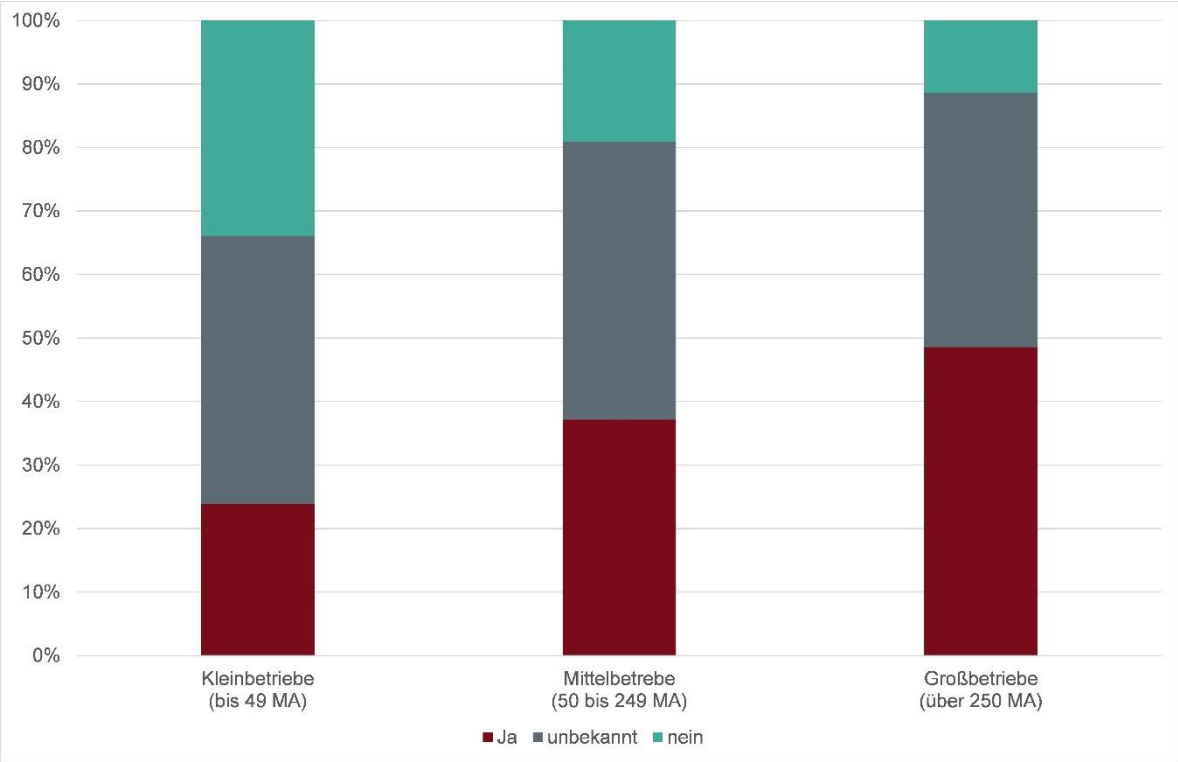


Quelle: EMS 2018, eigene Berechnungen
Frage: Haben Sie in Ihrer Produktion Maschinen oder Anlagen, die automatisiert Betriebsdaten speichern?
Anmerkung: n=250 Betriebe der österreichischen Sachgütererzeugung ab 20 MitarbeiterInnen
Klassifikation des Industrie 4.0 Reifegrad auf Basis des Einsatzes von 13 spezifischen Techniken.

[4] Der EMS zeigt dabei allgemein, dass im Schnitt im Jahr 2018 drei Techniken eingesetzt werden (nicht dargestellt). Es zeigen sich beim Reifegrad starke Unterschiede zwischen den Betrieben. 27% aller Betriebe der Sachgütererzeugung ab 20 MitarbeiterInnen setzen maximal eine relevante Technik ein und weitere 36% nur zwei bis drei Techniken. Im Gegensatz dazu setzen 37% der Betriebe vier oder mehr dieser Techniken bereits ein, 16% sogar sechs und mehr Techniken. Dabei zeigt sich ein deutlicher Unterschied beim Technikeinsatz nach Größenklassen. Während Betriebe mit 20-29 MitarbeiterInnen im Schnitt nur knapp zwei Techniken einsetzen, steigt ihre Zahl bei Betrieben mit über 250 MitarbeiterInnen auf vier an.

Was das eingeschätzte Bedrohungspotenzial betrifft, zeigt der EMS, dass dieses mit der Betriebsgröße steigt (vgl. Abbildung 3). Gleichzeitig kann konstatiert werden, dass über alle Größenklassen hinweg rund ein Drittel der Betriebe nicht abschätzen kann, ob Cyberangriffe eine relevante Bedrohung für den Betrieb darstellen.

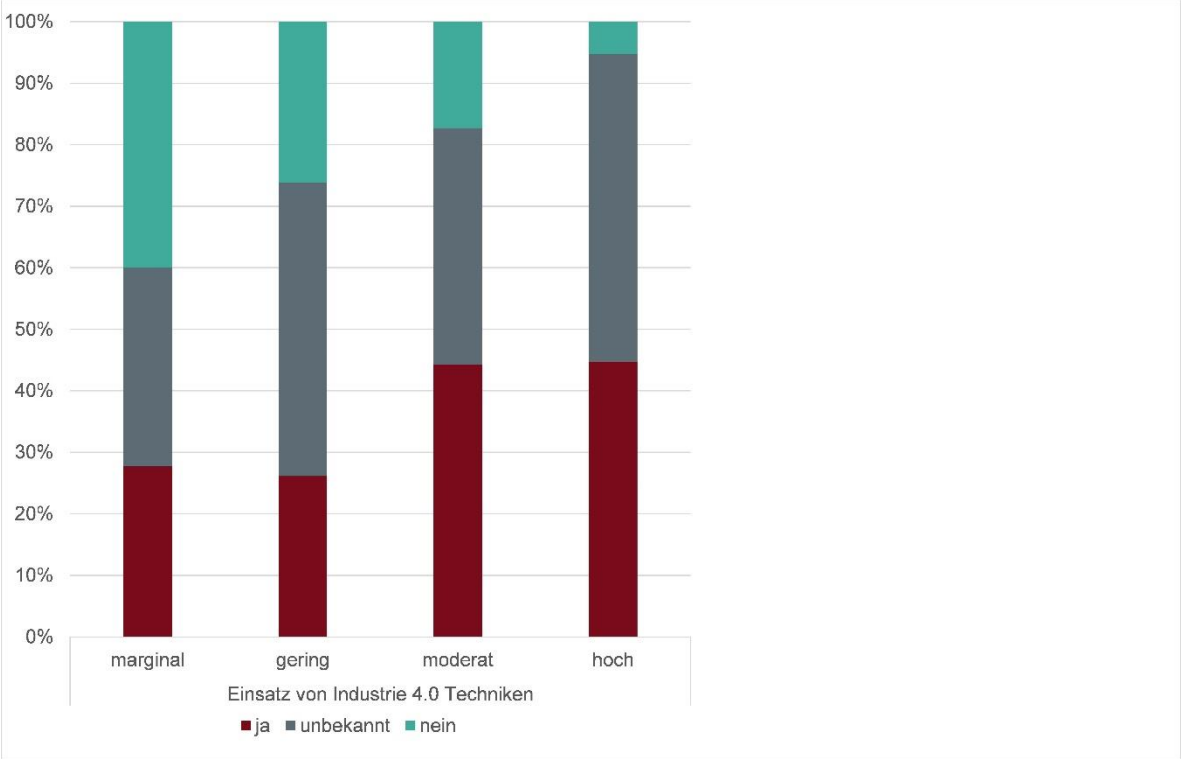
Abbildung 3: Bedrohungspotential von Cyberangriffen nach Betriebsgrößen



Quelle: EMS 2018, eigene Berechnungen
Frage: „Stellen Cyber-Angriffe eine relevante Gefährdung Ihres Betriebes dar?"
Anmerkung: n=250 Betriebe der österreichischen Sachgütererzeugung ab 20 MitarbeiterInnen

Für die Analysen des Zusammenhangs zwischen Industrie-4.0-Reifegrad und Security kann ebenfalls wieder nach vier Stufen von Industrie-4.0-Reifegrad differenziert werden. Die Ergebnisse zeigen, dass mit steigender Industrie-4.0-Ausstattung der Anteil der Betriebe, die Bedrohungspotenziale von Cyberangriffen als relevante Gefahr betrachten, steigt (vgl. Abbildung 4). Gleichzeitig kann quer über alle Betriebstypen ein beträchtlicher Anteil das Potenzial nicht einschätzen.

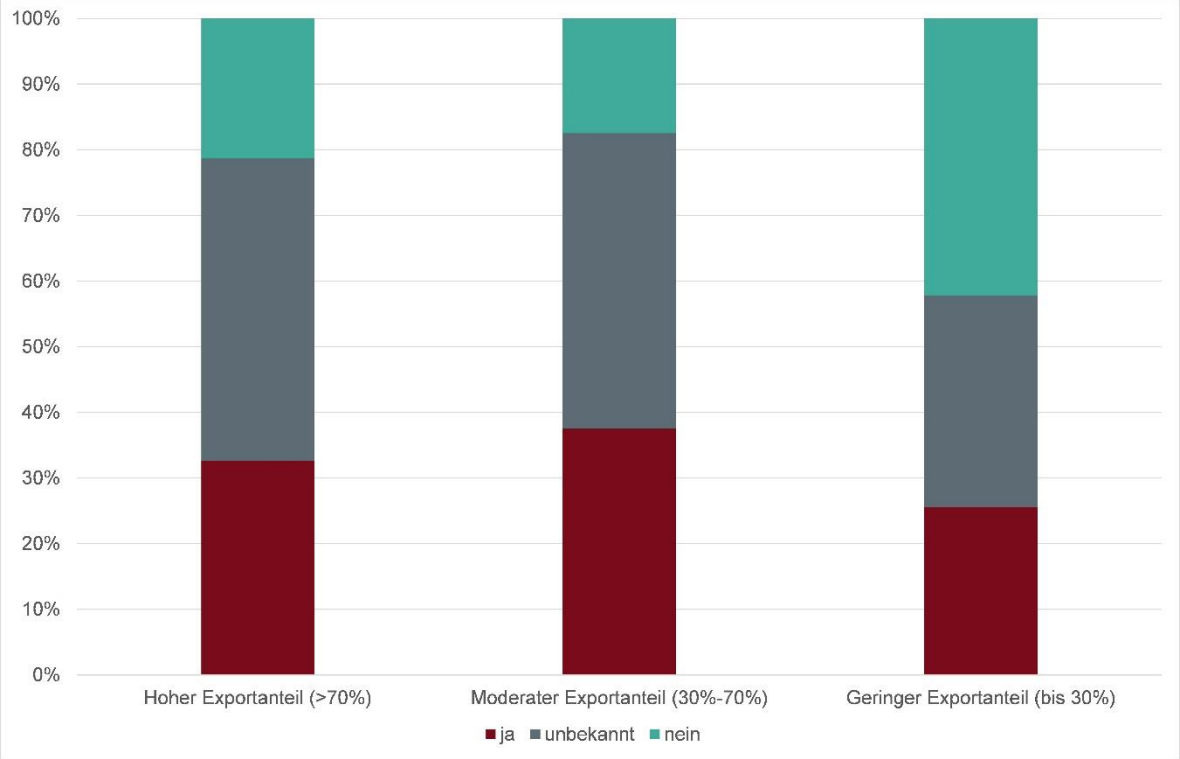
Abbildung 4: Bedrohungspotenzial von Cyberangriffen und Industrie-4.0-Reifegrad



Quelle: EMS 2018, eigene Berechnungen
Frage: „Stellen Cyber-Angriffe eine relevante Gefährdung Ihres Betriebes dar?"
Anmerkung: n=250 Betriebe der österreichischen Sachgütererzeugung ab 20 Mitarbeitern
Klassifikation des Industrie 4.0 Reifegrad auf Basis von 13 Techniken

Auch in Bezug auf die internationale Orientierung der Betriebe zeigt sich ein Zusammenhang mit dem wahrgenommenen Bedrohungspotenzial. Betriebe mit einem Exportanteil von mehr als 30% behaupten öfter, möglichen Gefahren für Cyberangriffe ausgesetzt zu sein. Bei Betrieben, die vorwiegend nationale Märkte bedienen, ist der Anteil, derer, die kein Bedrohungspotenzial sehen, deutlich geringer (45% vs. 20%).

Abbildung 5: Bedrohungspotenzial von Cyberangriffen und Exportanteil



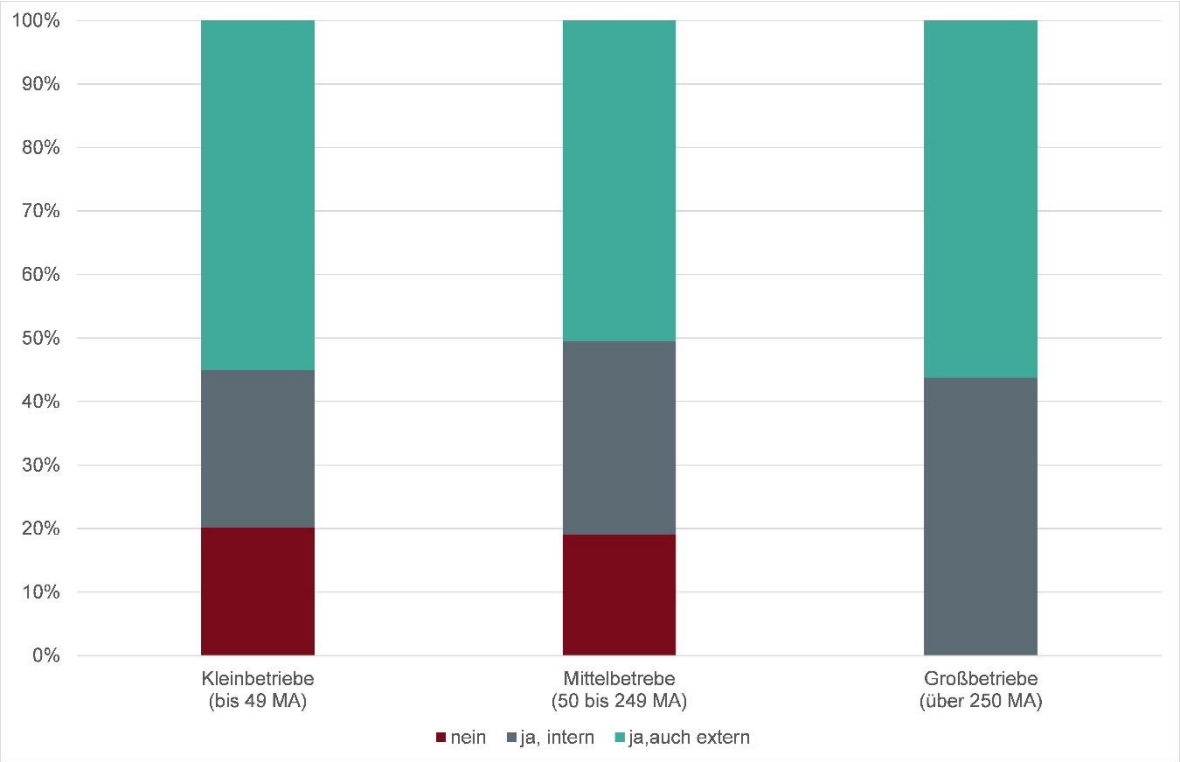
Quelle: EMS 2018, eigene Berechnungen
Frage: „Stellen Cyber-Angriffe eine relevante Gefährdung Ihres Betriebes dar?"
Anmerkung: n=250 Betriebe der österreichischen Sachgütererzeugung ab 20 MitarbeiterInnen

Das wahrgenommene Bedrohungspotenzial hängt überdies auch von der Position in der Wertschöpfungskette ab. So zeigt sich, dass Betriebe, die als Zulieferer tätig sind, häufig bekunden, möglichen Cyberangriffen ausgesetzt zu sein (hier nicht dargestellt).

Die Überprüfung von Sicherheitsmaßnahmen durch die Betriebe ist ein weiterer Indikator zur Einschätzung des Sicherheitsbewusstseins. Eine Auswertung nach der Betriebsgröße zeigt, dass Großbetriebe mit mehr als 250 Beschäftigten ausnahmslos die Effektivität der Sicherheitsmaßnahmen regelmäßig überprüfen. Mehr als die Hälfte dieser Betriebe lassen diese Maßnahmen auch extern überprüfen. Aber auch 80% der Betriebe mit weniger als 250 Beschäftigten überprüfen regelmäßig die Effektivität der Sicherheitsmaßnahmen.

Im Rahmen des EMS können die Unternehmen auch nach der Technologieintensität der Branchen untersucht werden („Low-Tech versus High-Tech"). Dabei zeigen sich keine klaren Muster, was die regelmäßige Überprüfung der Sicherheitsmaßnahmen betrifft (hier nicht dargestellt). Ebenso wenig hat die Position in der Wertschöpfungskette (Zulieferer versus Hersteller von Endprodukten) eine Auswirkung auf die Überprüfung von Sicherheitsmaßnahmen (hier nicht dargestellt).

Abbildung 6: Überprüfung von Sicherheitsmaßnahmen nach Betriebsgrößen



Quelle: EMS 2018, eigene Berechnungen
Frage: „Wird die Effektivität der Sicherheitsmaßnahmen sowie die Angemessenheit und Umsetzung Ihres Sicherheitskonzeptes regelmäßig überprüft?"
Anmerkung: n=250 Betriebe der österreichischen Sachgütererzeugung ab 20 MitarbeiterInnen

2.2 Reifegrad im Bereich Security

Für die Bewertung des Entwicklungsstands der Unternehmen im Umgang mit Security werden in der Praxis häufig sogenannte Reifegrad-Modelle genutzt, beispielsweise das Cybersecurity Capability Maturity Model (C2M2) des US Department of Energy[5]. Auf Basis der Daten des EMS und in Anlehnung an die in der Literatur für unterschiedliche Branchen vorgestellten Modelle[6] wurde für diese Studie ein einfaches Reifegradmodell entwickelt (siehe Abbildung 7).

[5] https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf
[6] Vgl. z.B. ISA 2009, ISO 2009, Caralli et al. 2011, DOD und DHS 2014.

Abbildung 7: Reifegradmodell

Quelle: Eigene Darstellung

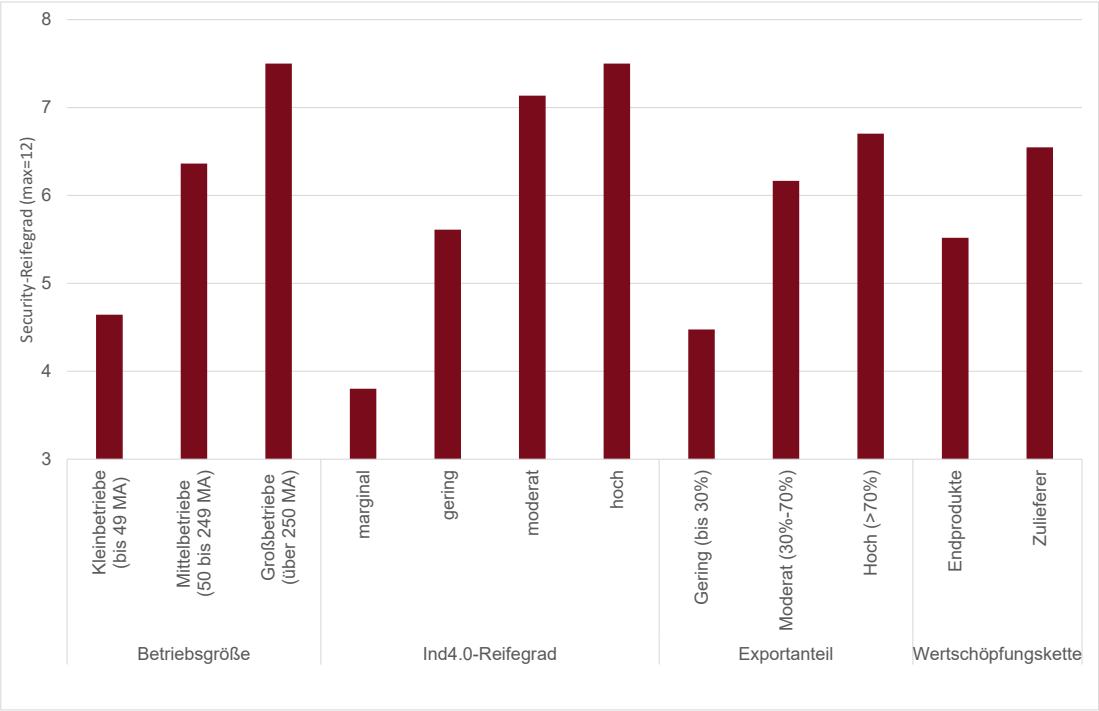
Auf Basis der im EMS abgefragten Inhalte zum Umgang mit Security wird die Nutzung von insgesamt 12 verschiedenen Security-Maßnahmen in fünf Bereichen herangezogen, um einen Index (max. 12 Punkte) zu bilden. Dabei werden berücksichtigt:

- Maßnahmen für die Sicherung der Betriebsdaten
  - Regelmäßige Sensibilisierung der Beschäftigten
  - Einsatz spezieller Softwarelösungen
  - Einsatz spezieller Hardwarelösungen
  - Spezielle organisatorische Maßnahmen
- Maßnahmen für den Schutz sensibler Entwicklungs- und Vertriebsdaten
  - Passwortrichtlinien
  - Verschlüsselung
  - Analyse-Tools zur Angriffserkennung
  - Räumliche Zugangsbeschränkungen

- Überprüfung der Effektivität dieser Sicherheitsmaßnahmen sowie die Angemessenheit und Umsetzung Ihres Sicherheitskonzeptes
    - Ja, intern
    - Ja, auch extern
- Risikoanalyse für die in der Produktion anfallenden Betriebsdaten
- Weiterbildungsmaßnahmen in Bezug auf Datenschutz/Privacy und/oder den sicherheitsbewussten Umgang mit Daten

Abbildung 8 zeigt die Ergebnisse des EMS-basierten Security-Reifegrads differenziert nach Betriebsgröße, Industrie-4.0-Reifegrad, Exportanteil und Stellung in der Zulieferkette. Dabei zeigt sich, dass ein klarer Zusammenhang zwischen dem Ausmaß der Nutzung von Industrie-4.0-Technologien und dem Security-Reifegrad besteht: Unternehmen, die viele Industrie-4.0-Technologien einsetzen, haben auch deutlich mehr Security-Maßnahmen implementiert. Ebenso haben größere Unternehmen einen höheren Security-Reifegrad. Unternehmen, die im Export tätigt sind und als Zulieferer agieren, setzen im Durchschnitt ebenfalls mehr Security-Maßnahmen ein.

Abbildung 8: Security-Reifegrad (0-12) nach Betriebsgröße, Einsatz von Industrie 4.0 Techniken (Industrie 4.0-Reifegrad), Exportanteil und Stellung in der Zulieferkette

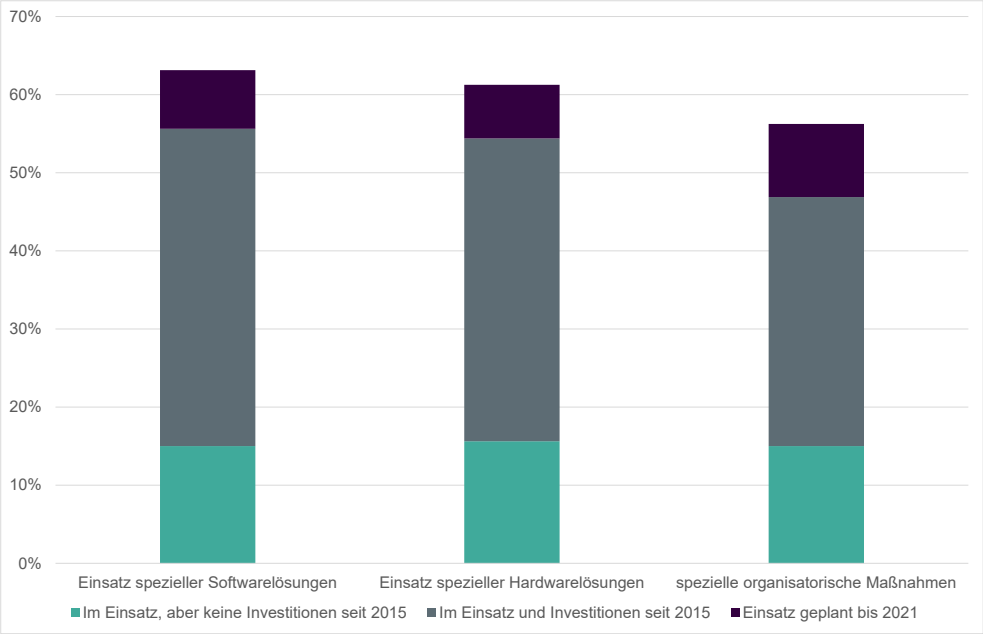


Quelle: EMS 2018, eigene Berechnungen
Anmerkung: n=250 Betriebe der österreichischen Sachgütererzeugung ab 20 MitarbeiterInnen

2.3 Security-Investitionen

Für die Frage der Investitionen in Security können Befunde des EMS herangezogen werden, die untersuchen, ob Investitionen durchgeführt wurden oder geplant sind. Dabei zeigt sich, dass jeweils rund 40-50% der befragten Unternehmen seit 2015 in Softwarelösungen, Hardwarelösungen bzw. spezifische organisatorischer Maßnahmen investiert haben (vgl. Abbildung 9). Rund 10-15% planen jeweils bis 2021 derartige Lösungen erstmalig einzusetzen. Rund 15% der befragten Betriebe haben zwar die jeweiligen Security-Maßnahmen im Einsatz, jedoch seit 2015 keine Folgeinvestitionen getätigt.

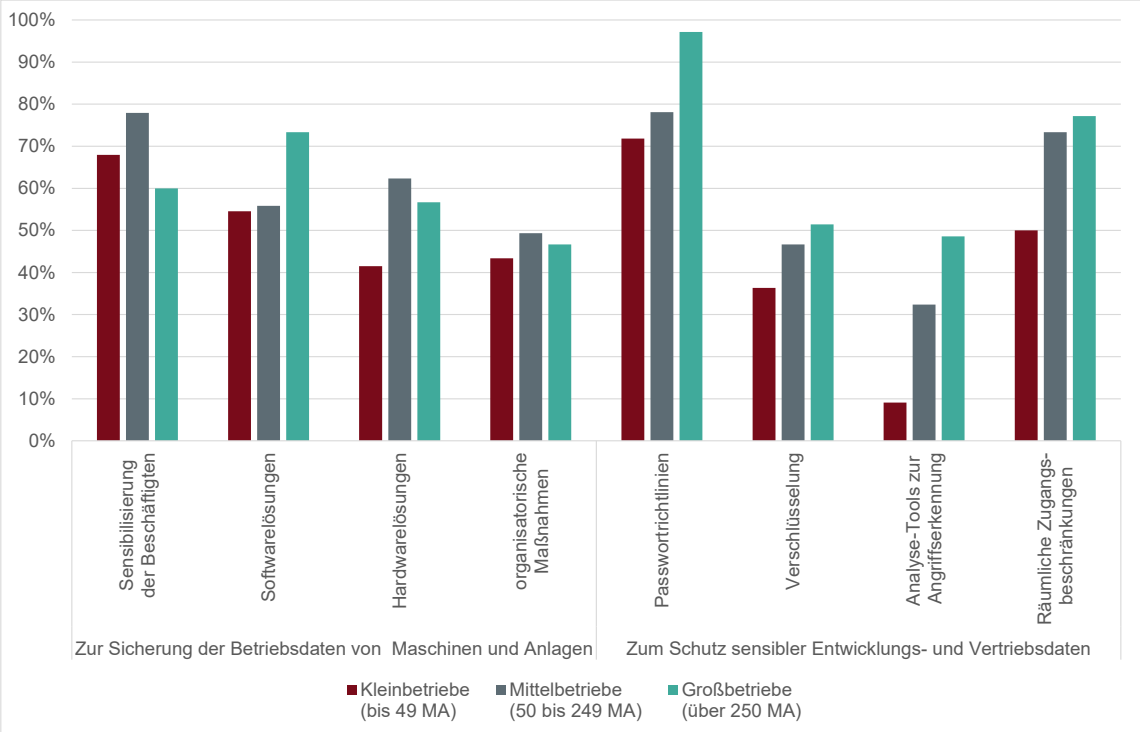
Abbildung 9: Investitionen in Security



Quelle: EMS 2018, eigene Berechnungen
Frage: „Der Einsatz welcher Maßnahmen für die Sicherung der Betriebsdaten ist bis 2021 geplant und in welche bestehenden Maßnahmen gab es Folgeinvestitionen seit 2015?"
Anmerkung: n=250 Betriebe der österreichischen Sachgütererzeugung ab 20 MitarbeiterInnen

Im EMS wurden auch konkrete Maßnahmen zum Schutz von unterschiedlichen Daten erfasst. Auch diese Frage erlaubt Rückschlüsse auf das Sicherheitsbewusstsein in der österreichischen Industrie. Abbildung 10 zeigt den Einsatz von Security-Maßnahmen differenziert nach Betriebsgröße. Die Ergebnisse zeigen, dass das Ausmaß der Aktivitäten mit der Betriebsgröße steigt. Nur bei organisatorischen Maßnahmen und bei der Sensibilisierung der Beschäftigten ist der Zusammenhang nicht klar ausgeprägt. Insgesamt spielen Passwortrichtlinien die größte Rolle, gefolgt von räumlichen Zugangsbeschränkungen und der Sensibilisierung der Beschäftigten.

Abbildung 10: Einsatz von Security-Maßnahmen



Quelle: EMS 2018, eigene Berechnungen
Frage: „Welche der folgenden Maßnahmen setzen Sie für die Sicherung der Betriebsdaten Ihrer Maschinen und Anlagen ein?"
Anmerkung: n=250 Betriebe der österreichischen Sachgütererzeugung ab 20 MitarbeiterInnen

2.4 Bedrohungsszenarien

Vertraulichkeit der Produktionsdaten und die Zuverlässigkeit des Produktionssystems sind zwei Beispiele für die verschiedenartigen Herausforderungen, mit denen Produktionsunternehmen durch Industrie 4.0 konfrontiert sind. Die Teilnahme an Wertschöpfungsnetzwerken erfordert das Vertrauen zwischen den teilnehmenden Organisationen. Vertrauliche Produktionsdaten müssen vor dem Zugriff unbefugter Dritter geschützt werden. Die weitreichende Vernetzung von Produktionsanlagen und Systemen zur Prozesssteuerung, die auch als Operational Technology (OT) bezeichnet werden, und deren Integration mit der Informationstechnologie (IT) führen jedoch dazu, dass Industrielle Steuerungssysteme (ICS) sich heute ähnlichen Bedrohungen gegenübersehen wie klassische IT-Systeme.

Die gezielte Störung oder Zerstörung von Systemen durch Manipulation von außen, die z.B. zu Betriebsausfällen oder -verzögerungen führen können, sind ein Teil dieser Gefahren.

Jedoch sind Unternehmensinformationen (Industriespionage und Piraterie) ebenso gefährdet wie sensible Daten von Beschäftigten und Kunden.

Gerade in der jüngeren Vergangenheit musste durch verschiedene Vorfälle erkannt werden, dass diese Bedrohungen sehr real sind. So musste beispielsweise der französische Automobilkonzern Renault im Mai 2017 seine Produktion an mehreren Standorten einstellen, nachdem er Opfer eines Cyberangriffs mit dem Erpressungstrojaner WannaCry geworden war. Das Deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) berichtet von einem Angriff auf ein deutsches Stahlwerk. Über einen Spear-Phishing-Angriff erlangten die Angreifer Zugriff auf die IT-Systeme des Unternehmens, von wo aus sie sich bis zur Steuerung des Hochofens vorarbeiteten. Die Folge war eine erhebliche Beschädigung der Anlage durch ein unkontrolliertes Herunterfahren des Hochofens.

Nachfolgende Tabelle 1 stellt eine Auswahl aktueller Bedrohungen für ICS dar, die besonders relevant sind. Für weiterführende Informationen sei auf die Top 10 Bedrohungen und Gegenmaßnahmen des BSI und den Cyber-Security-Leitfaden für Produktionsbetriebe des Vereins Industrie 4.0 Österreich verwiesen.[7]

Bedrohung für Industrie 4.0

- **Schadsoftware:** Regelmäßig werden neue Schwachstellen bekannt, die Angreifer für das Einschleusen von Schadsoftware nutzen können. Angreifer können dadurch an unternehmenskritische Informationen gelangen oder den Betrieb sabotieren. Durch die zunehmende Vernetzung kann es Angreifern gelingen, sich vom Office-Netz aus in das ICS einzudringen. Die Infektion des Office-Netzes geschieht dabei primär über das Internet, kann sich aber auch über das Intranet verteilen. Selbst wenn das ICS physikalisch vom Office-Netz getrennt ist, so besteht immer noch die Gefahr des Einschleusens von Schadsoftware über Wechseldatenträger und externe Hardware. Neben gezielten Angriffen auf das Unternehmen stellen Ransomware und in letzter Zeit auch Cryptojacking eine Bedrohung für die IT-Infrastruktur dar. Dabei werden die Rechenressourcen eines Computers genutzt, um Cryptowährungen zu „minen".
- **Angriff auf vernetzte Komponenten:** Mit dem Internet verbundene Komponenten stellen eine potenzielle Bedrohung für ein Unternehmen dar, da sie von Angreifern ausgenutzt werden können, um Zugriff auf das Unternehmensnetzwerk zu bekommen. Dabei muss man zwischen temporären und permanenten Verbindungen unterscheiden. Wartungszugänge, die zur Wartung von Maschinen durch externe Dienstleister genutzt werden, um Maschinen zu warten, stellen einen der möglichen Angriffsvektoren dar.

[7] Siehe Verein Industrie 4.0 Österreich – die Plattform für intelligente Produktion (2018).

Obwohl sie nur temporär für den Zeitraum der Wartungsarbeiten zur Verfügung stehen sollten, kann ein Angreifer beispielsweise versuchen, sich durch einen Brute-Force-Angriff auf das Passwort Zugriff auf das Unternehmensnetz zu verschaffen. Darüber hinaus kann auch der verwendete Wartungsrechner mit Schadsoftware infiziert sein, die den vorhandenen Kanal ausnutzt. Obwohl im Allgemeinen davon abgeraten wird, kommt es immer wieder vor, dass ICS-Komponenten direkt mit dem Internet verbunden und von außen auffindbar sind. Dies kann sowohl absichtlich als auch versehentlich geschehen. Die Komponenten sind dafür jedoch nicht ausgelegt und somit anfällig für Angriffe. Angriffsvektoren können in diesem Zusammenhang nicht geänderte Standardpasswörter oder nicht zeitnah beseitigte Schwachstellen sein.

- **Advanced Persistent Threats (APT):** Zielgerichtete Angriffe und Advanced Persistent Threats (APT) stellen für viele Unternehmen eine große Herausforderung dar. APTs erfolgen stufenweise über einen längeren Zeitraum. Ziel ist es, möglichst ungedeckt zu bleiben und damit möglichst viele sensible Informationen zu erhalten. Es sind allerdings auch Fälle bekannt geworden, die die Sabotage von Produktionsanlagen zum Ziel hatten.
- **Spionage:** In der letzten Zeit wurden vermehrt staatlich gesponserte Angriffe aufgedeckt, die insbesondere die Industrie und die Betreiber kritischer Infrastruktur zum Ziel hatten. Diese Angriffe zielen auf die Beschaffung von Informationen über Geschäftsgeheimnisse, geistiges Eigentum oder andere schutzwürdige Informationen ab. Dabei wird häufig auch das vermeintlich niedrigere Sicherheitsniveau in der Supply-Chain ausgenutzt. Die Angreifer nutzen dabei auch Fernwartungszugänge von ICS, aber auch APT.
- **Social Engineering und Phishing:** Social Engineering ist eine Technik, mit der Personen dazu gebracht werden, sicherheitskritische Informationen wie beispielsweise Passwörter preiszugeben. Diese Informationen können anschließend dazu verwendet werden, ansonsten sichere Systeme anzugreifen. Phishing ist ein typischer Vertreter dieser Kategorie. Der Angreifer versucht über gefälschte E-Mails, Passwörter zu erlangen oder Malware zu installieren. Die wichtigste Maßnahme gegen Social Engineering im Allgemeinen und Phishing im Besonderen sind Awareness-Maßnahmen und die Schulung der Mitarbeiter.
- **(D)DoS Angriffe:** „(Distributed) Denial of Service"-Angriffe zielen darauf ab, die Ressourcen eines Systems durch Überlast aufzubrauchen. Diese Angriffe richten sich gegen die Rechenressourcen eines Systems oder gegen die Netzwerkressourcen durch das Fluten des Kommunikationskanals mit einer großen Anzahl von Nachrichten. ICS-Komponenten, die häufig nur über geringe Rechenkapazität verfügen, sind nicht dafür ausgelegt, derartige Angriffe zu überstehen.
- **Technische Fehler:** In der industriellen Fertigung herrschen zum Teil extreme Umgebungsbedingungen, die eine Herausforderung für die eingesetzte Hardware und Software in IT und OT darstellen. Obwohl in diesen Systemen in der Regel entsprechend

ausgelegte Komponenten zum Einsatz kommen, ist die Wahrscheinlichkeit für den Ausfall oder die Fehlfunktion einzelner Komponenten erhöht. Fehler in Hard- oder Software können zum Ausfall kompletter Systeme führen. Durch effiziente organisatorische Maßnahmen können die Auswirkungen von technischen Fehlern jedoch minimiert werden.

- **Beabsichtigtes und unbeabsichtigtes menschliches Fehlverhalten:** Eine besondere Rolle kommt im industriellen Umfeld den MitarbeiterInnen zu. Bedrohungen können sowohl durch beabsichtigte als auch unbeabsichtigte Handlungen entstehen, wie beispielsweise eine Fehlkonfiguration wichtiger Komponenten oder das unbeabsichtigte Einschleusen von Malware.
- **Angriffe auf Cloud-Komponenten:** Cloud-Computing ist einer der IT-Trends, der jetzt auch die ICS-Domäne erreicht hat. Oft handelt es sich dabei um Applikationen zur Datenanalyse, da zeitkritische Aktionen in der Produktion wegen der längeren Laufzeiten nicht möglich sind. Es darf dabei jedoch nicht vergessen werden, dass sich daraus neue Bedrohungen ergeben. Das Unternehmen hat keinen direkten Einfluss auf die Sicherheit des Cloud-Anbieters, so dass eine zusätzliche Gefahr von Datendiebstahl oder -manipulation besteht. Falls die Daten, die bei einem Cloud-Anbieter liegen, für den Produktionsprozess benötigt werden, ergibt sich durch die mögliche Störung der Kommunikation, z.B. durch einen DoS-Angriff, ein zusätzliches Bedrohungspotenzial.

3 Steigende Sicherheitsanforderungen als Herausforderung für die Industrie

3.1 Neue Sicherheitsanforderungen

3.1.1 Differenzierung von IT und OT als wichtige Herausforderung für Industrial Control Systems Security

Im Rahmen von Industrie 4.0 kommt es zu einer weitreichenden Vernetzung von Produktionsanlagen und Systemen zur Prozesssteuerung, die auch als Operational Technology (OT) bezeichnet werden, und deren Integration mit Systemen der klassischen Informationstechnologie (IT). Im direkten Vergleich sind wesentliche Unterschiede die hohen Anforderungen an die Verfügbarkeit von OT-Komponenten, deren vergleichsweise lange Lebenszyklen und häufig eingeschränkte Prozessorleistungs- und Speicherkapazitäten. Die folgenden drei Sachverhalte werden daher gemeinhin als zentrale Herausforderungen bei der Absicherung von industriellen Steuerungssystemen (Industrial Control Systems, ICS) betrachtet:

1. **Vernetzung und Komplexität**: Der Paradigmenwechsel weg von isolierten, proprietären Systemen hin zu Vernetzung von OT und IT und Nutzung von Komponenten aus der Office-Welt führt dazu, dass OT den gleichen Gefährdungen ausgesetzt ist wie IT bzw. Office-Welt, mit potenziell gefährlichen Folgen u.a. auch für die Safety (Betriebssicherheit).
2. **Unterschiedliche Anforderungen bzw. Prioritäten bei IT und OT** in Bezug auf Verfügbarkeit, Latenz, Lebensdauer der Komponenten und Systeme – bekannte Security-Maßnahmen aus der IT sind somit nicht 1:1 in der OT anwendbar. Die Security hat bei industriellen Anlagen oft einen geringeren Stellenwert als die Funktionalität und wird eher im Nachhinein „aufgepfropft" statt von Beginn an („by design") mitgedacht zu werden, was die Komplexität der Lösung weiter erhöht.
3. **Interdisziplinarität und mangelnde Kommunikation**: IT- und OT-ExpertInnen sprechen (im übertragenen Sinn) oft eine andere Sprache und verstehen einander nicht, was auch mit dem vorab genannten Punkt zusammenhängt. Generell haben nur wenige ExpertInnen fundierte Kenntnisse in beiden Bereichen. Diese Problematik wird noch

verstärkt durch die häufig vorhandene organisatorische Trennung von Produktion/OT und Security/IT in den Betrieben.

Um die IT-Sicherheit in klassischen IT-Systemen zu realisieren und entsprechende Anforderungen zu definieren, gibt es heute eine Fülle von etablierten Ansätzen. Die größte Bedeutung hat dabei die Normenreihe ISO/IEC 27000. Die Reihe enthält Best-Practice-Empfehlungen zum Informationssicherheitsmanagement im Kontext eines allgemeinen Informationssicherheitsmanagementsystems (ISMS). Spezifische Anforderungen an die IT-Sicherheit industrieller Steuerungssysteme sind dort zwar nicht berücksichtigt, aber im Allgemeinen daran angelehnt.

Auch durch gesetzliche Regelungen wie das NIS-Gesetz[8] oder den EU-Rechtsakt zur Cybersicherheit[9] können völlig neue Anforderungen an Produkte und Dienstleistungen entstehen. Das NIS-Gesetz verlangt von den Betreibern wesentlicher Dienste die Einführung geeigneter Sicherheitsmaßnahmen, die gegebenenfalls auch von deren Lieferanten unterstützt werden müssen. Der EU-Rechtsakt zur Cybersicherheit hat dahingehend noch weitreichendere Auswirkungen. Durch ihn soll ein EU-weites System zur Zertifizierung von Cybersicherheit von Produkten, Verfahren und Dienstleistungen geschaffen werden. Das Ziel ist es, dass Sicherheitsmerkmale bereits während des Entwicklungsprozesses berücksichtigt werden und der Anwender durch eine unabhängige Überprüfung ein hohes Maß an Vertrauen in die betroffenen Produkte haben kann.

3.1.2 Referenzarchitekturmodell RAMI 4.0

Nachfolgend soll näher auf die Differenzierung zwischen IT und OT eingegangen werden und wie diese in Zukunft immer mehr verschwimmt. Ein Ansatz für künftige Automatisierungssysteme ist das dreidimensionalen Referenzarchitekturmodell RAMI 4.0, das Lebenszyklus bzw. Wertschöpfungskette aus IEC 62890 (Life-cycle management for systems and products used in industrial-process measurement, control and automation) mit den Hierarchiestufen aus IEC 62264 (Enterprise-control system integration) kombiniert. Es stellt einen strukturierten Ansatz für die Definition von Industrie-4.0-Konzepten dar. Gegenüber der aus IEC 62264 abgeleiteten Automatisierungspyramide wurde RAMI 4.0 um die Stufen „Produkt" und die über den einzelnen Produktionsstandort hinausgehende

[8] Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG), Fassung vom 10.03.2020.
[9] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").

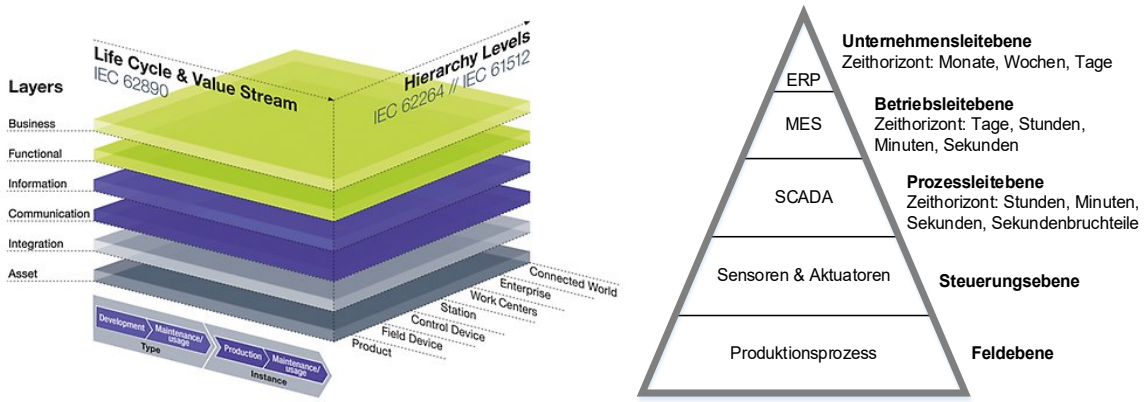
„Connected World" erweitert. Jede dieser Ebenen ist durch bestimmten Arten von Informationen, Systemen, Funktionen und Zeithorizonten gekennzeichnet. Bei den Hierarchiestufen handelt es sich, anders als bei der Automatisierungspyramide, jedoch nur um die Einordnung von Funktionalitäten und nicht um eine räumliche Zuordnung zu Geräteklassen.

Die Unternehmensleitebene befasst sich mit der Unternehmensplanung und Logistik und wird häufig in einem ERP-System (Enterprise Resource Planning) verwaltet. Die darunterliegende Betriebsleitebene steuert die Fertigungsabläufe, wie z. B. welche Prozesse in welcher Reihenfolge ausgeführt werden sollen. Diese Systeme werden als Manufacturing Execution Systems (MES) bezeichnet. Darunter ist die Prozessleitebene angeordnet, auf der die Geräte über Mensch-Maschine-Schnittstellen überwacht werden (HMI) und die über eine Überwachungs- und Datenerfassungsfunktionalität (SCADA) verfügt. Die Steuerung der Maschinen findet auf der Steuerungsebene statt, die üblicherweise durch speicherprogrammierbare Steuerungen (SPS) realisiert ist. Der Produktionsprozess selbst wird schließlich durch die Feldebene repräsentiert.

Die Schnittstelle zwischen OT und IT bildet das Produktionsleitsystem, das auch als Manufacturing Execution System (MES) bezeichnet wird. Das MES verfügt jeweils über eine Schnittstelle zur Prozessautomatisierung und zum Enterprise Resource Planning (ERP).

Die Anforderungen an die Verfügbarkeit auf den verschiedenen Hierarchieebenen lassen sich auch aus den Zeithorizonten der Entscheidungen ableiten, die in IEC 62246-3 definiert sind: Während in den IT-Systemen der Zeitrahmen für Entscheidungen bei Tagen und Wochen liegt, umfasst er auf Betriebsleitebene Tage bis Sekunden. Auf Prozessleitebene und darunter sind Entscheidungen teilweise innerhalb von Mikrosekunden (d.h. Tausendstel Sekunden) zu treffen.

Abbildung 11: Referenzarchitekturmodell RAMI 4.0 und Automatisierungspyramide



Quelle: ZVEI

In der Industrie 4.0 wird sich die streng hierarchische Struktur der Automatisierungspyramide insofern auflösen, als die I4.0-Komponenten einer Ebene mit beliebigen Endpunkten kommunizieren können. Daher wird in Zukunft eine klare Abgrenzung zwischen OT und IT schwieriger, wobei die Echtzeitanforderung in der Feld- und Steuerungsebene weiterhin als unterscheidendes Merkmal herangezogen werden kann.

3.1.3 Die Normenreihe IEC 62443

Die europäische Standardisierung zur Industrie 4.0 befasst sich u.a. mit Apekten der Security, Safety, Verlässlichkeit bzw. Ausfallsicherheit und Interoperabilität. Besonders aktiv in diesem Bereich sind die europäischen Normungsorganisationen CEN und CENELEC. Die „CEN-CENELEC-ETSI Coordination Group on Smart Manufacturing" (CEN-CLC-ETSI SMa-CG) verfolgt das Ziel, die Erfordernisse und Aktivitäten im Bereich Standardisierung zu koordinieren und über die Grenzen der einzelnen Normungsorganisationen hinweg kohärente Lösungen voranzutreiben. International ist die IEC 62443 „Industrial communication networks – Network and system security" eine branchenunabhängige Normenreihe zur IT-Sicherheit im Bereich der industriellen Automatisierung. Aufgrund ihrer zentralen Bedeutung und hohen Akzeptanz wird sie im Folgenden kurz erläutert.

Die IEC 62443 unterstützt AnwenderInnen darin, Sicherheitslücken ihrer Steuerungs- und Leittechnik zu identifizieren und geeignete Schutzmaßnahmen zu entwickeln. AnwenderInnen können dabei einer oder mehreren der drei wesentlichen Stakeholdergruppen angehören, welche die IEC unterscheidet: **Geräte- und Maschinenhersteller, Systemintegratoren und Anlagenbetreiber.**

Die Normenreihe differenziert zwischen dem technischen Sicherheitslevel („Security Level") der Systeme bzw. Komponenten und dem Reifegrad („Maturity Level") der organisatorischen Prozesse und deren Einhaltung. Die Kombination technischer und organisatorischer Aspekte ergibt ein umfassendes Sicherheitskonzept, das „weitaus mehr Schutzpotenzial bietet als die rein technische Betrachtung"[10]. Auf Basis einer Architektur des betrachteten Gesamtsystems werden auf mehreren Ebenen Sicherheitsmaßnahmen für alle betrachteten Systeme und Komponenten definiert („Defense-in-depth"-Prinzip, siehe technische Anforderungen in Abschnitt 3.1).

Die IEC 62443 ist in vier Bereich unterteilt, die Sicherheit jeweils aus unterschiedlicher Perspektive betrachten: Allgemein (Teil 1), aus Policy-Sicht (Teil 2), aus System- (Teil 3) sowie Komponentensicht (Teil 4). Der **Betreiber** („Asset owner") bestimmt mittels Risikoanalyse (Teil 3-2) den Schutzbedarf seines Systems („Target security level", SL-T). Der **Hersteller** gibt seinem Produkt inhärente Sicherheitseigenschaften („Security capabilities", SL-C) mit, indem er Sicherheitsanforderungen bereits bei der Entwicklung berücksichtigt (Teil 4). Der **Systemintegrator** entwirft ein System, welches den Schutzbedarf SL-T des Betreibers erfüllt, indem er Herstellerkomponenten mit gewissen Sicherheitseigenschaften („Security capabilities", SL-C) verwendet (Teil 3-3). Die Komponente kann dabei die Capability selbst aufweisen oder aber mit einer anderen Komponente, die dies leistet, integriert werden. Das Schutzniveau, welches letztendlich erreicht wird („Security level achieved", SL-A), ergibt sich erst in der konkreten Implementierung der Hersteller-Komponente durch den Systemintegrator beim Betreiber.

IEC 62443 definiert verschiedene Anforderungsebenen: Die **Basisanforderungen** ("Foundational requirements", FR, Teil 1-1) werden unterteilt in Systemanforderungen ("System requirements", SR, Teil 3-3), welche weiter verfeinert werden in Anforderungen für einzelne Komponenten ("Component requirements", CR, Teil 4-2). Jede Anforderung hat ein "Baseline requirement" sowie optionale "Enhancements"; diese werden auf die jeweiligen Capability-Sicherheitslevel SL-C abgebildet (z.B. muss für eine hohe Sicherheitsstufe SL 4 das Baseline requirement plus Enhancement x und y erfüllt werden, für SL 1 reicht hingegen bereits das Baseline requirement).

In der Praxis wird die Normenreihe IEC 62443 eher von großen Unternehmen angewendet; dies gilt insbesondere für eine Zertifizierung nach IEC 62443. Bei KMU ist der Gebrauch aufgrund der Komplexität und des Umfangs der Normenreihe weniger stark verbreitet, wobei in den letzten Jahren einige Leitfäden als Hilfestellung erarbeitet wurden[11]. Daher können

[10] Siehe https://www.sichere-industrie.de/iec-62443-diese-grundlagen-sollten-betreiber-einer-automatisierungsloesung-kennen/

[11] Kobes, Pierre: Leitfaden Industrial Security. IEC 62443 einfach erklärt, VDE-Verlag 2016.

sich insbesondere KMU durch den folgenden Katalog von Sicherheitsanforderungen einen ersten Überblick verschaffen.

3.1.4 Sicherheitsanforderungen

Vor dem Hintergrund der in Abschnitt 3.1.1 beschriebenen Herausforderungen werden im Folgenden die neuen Sicherheitsanforderungen gelistet.

Anmerkung zu den Auswahlkriterien: Viele Sicherheitsanforderungen gelten für IT ebenso wie für OT, beispielsweise das regelmäßige Erstellen von Datensicherungen (Backups). Solche Anforderungen werden im Weiteren nicht genannt, da es das explizite Ziel der Studie ist, *neue* Anforderungen zu beschreiben, die sich für industrielle Steuerungssysteme – zusätzlich zu den klassischen IT-Security-Anforderungen – ergeben oder aber für diese aufgrund der OT-Spezifika besonders relevant sind. Die Anforderungen wurden gemäß Aufgabenstellung in technische und organisatorische Anforderungen gegliedert, wobei einige Anforderungen nicht eindeutig einer der beiden Kategorien zugeordnet werden können bzw. Aspekte aus beiden Kategorien beinhalten (siehe z.B. die Anforderung „Monitoring" und die Anmerkungen im Text). Eine detaillierte, vollständige Auflistung sämtlicher Sicherheitsanforderungen inkl. Zuordnung zu den verschiedenen Stakeholdern (Betreiber, Integrator, Hersteller) würde den gegebenen Rahmen sprengen; wir verweisen hierfür auf die Normenreihe IEC 62443.

3.1.5 Organisatorische Anforderungen

Wichtige organisatorische Anforderungen für die Erhöhung der Security können wir folgt beschrieben werden:

- **Ganzheitliche Betrachtung** von Security, d.h. Technik UND Prozesse
    - Security by Design: Sicherheitsanforderungen müssen **von Anfang an** mitbetrachten werden, insbesondere bereits bei der Beschaffung bzw. bei Ausschreibungen.
      Der **gesamten Lebenszyklus** der Assets von Beschaffung bzw. Entwicklung über Betrieb und Wartung bis hin zu Außerbetriebnahme & Entsorgung sollte bei den Sicherheitserwägungen in Betracht gezogen werden.

- **Awareness und Kommunikation**, „menschliche Komponente"
    - Es müssen **klare Rollen und Zuständigkeiten** für Sicherheit in ICS definiert werden.

    - Security muss im **Management** verankert sein, damit ihr ein hoher Stellenwert sowie die nötigen finanziellen & personellen Ressourcen zuteilwerden.
    - **Auf die Kommunikation zwischen IT-Abteilung und Produktionsleitung** sollte ein besonderes Augenmerk gelegt werden, um Missverständnisse, unterschiedliche bzw. teils inkompatible Anforderungen und „Reibungsverluste" zu vermeiden.
    - Durch **regelmäßige Schulungen und Kommunikation** der Sicherheitsmaßnahmen **an die MitarbeiterInnen** (z.B. Schutz vor Phishing) sollten diese für IT-Sicherheit sensibilisiert werden.
    - Es sollte ein regelmäßiger Austausch mit externen Wissens- und Erfahrungsträgern wie Nutzerverbänden, Standardisierungsinitiativen und anderen Netzwerken (z.B. zur Definition & Durchsetzung von Sicherheitsanforderungen an Hersteller von ICS) stattfinden.

- Die aktuelle **Dokumentation** aller Komponenten, Dienste, Verbindungen und Berechtigungen ist unter mehreren Gesichtspunkten erforderlich:
    - Für die Prävention, Detektion & Reaktion auf Sicherheitsvorfälle ist ein vollständiges Bild aller Assets erforderlich, ebenso ist dies Grundlage für **Risikoanalysen** (siehe „Risikomanagement" weiter unten).
    - Auch die **Definition, Umsetzung & stetige Revision von Prozessen** zur Absicherung von ICS erfordert eine vollständige Dokumentation.
    - Das **Change & Configuration Management** beinhaltet die vollständige Dokumentation der Systemkonfiguration (inklusive aller Komponenten) einschließlich der Anpassungen, die im Laufe der Zeit erfolgt sind (siehe auch technische Anforderung „Minimalprinzip"). In diesem Zusammenhang ist auch anzumerken, dass in der IT eine separate Umgebung für Entwicklung, Test und Operation üblich ist, in der OT bislang eher nicht.
    - Im Rahmen des **Risikomanagements** werden kritische Bereiche bzw. Komponenten identifiziert, relevante Schwachstellen & Bedrohungen erkannt, Maßnahmen gesetzt und das Restrisiko definiert.
    - **Monitoring, Anomalieerkennung & Incident Management** beinhalten die konsequente Überwachung der Infrastruktur auf ungewöhnliche Vorgänge und Störungen, die ggf. auf Angriffe hindeuten können, und die Vorgehenwseise bei akuten Sicherheitsvorfällen. Dies umfasst auch die Dokumentation und Aufarbeitung vergangener Sicherheitsvorfälle (möglichst auch anderer Organisationen, siehe auch letzten Punkt bei „Awareness & Kommunikation" oben).

- Nicht zuletzt muss auch eine konsequente **Dokumentation von Sicherheitsmaßnahmen** und organisatorischen Sicherheitsprozessen erfolgen (z.B. Vorschriften für Vergabe & Wechsel von Passwörtern, Vorgehensweise bei Verlust, etc.). Die Sicherheitsmaßnahmen müssen allerdings nicht nur dokumentiert, sondern auch durchgesetzt und kontrolliert werden (z.B. kein Deaktivieren von Sicherheitsfunktionen).

3.1.6 Technische Anforderungen

Folgende technische Anforderungen stellen sich:

- **Monitoring der IT-Infrastruktur & Intrusion Detection**
    - Die IT-Infrastruktur muss kontinuierlich auf ungewöhnliche Vorgänge hin überprüft werden. Nur durch die Analyse von fehlgeschlagenen Anmeldungen, Netzwerkauslastung, etc. ist es möglich **Angriffe und Angriffsversuche rechtzeitig zu erkennen** und analysieren zu können (in der OT ist die kontinuierliche Überprüfung von Messwerten und Parametern bereits Standard).
    - Der Einsatz von **Intrusion Prevention Systemen (IPS)**, die automatisiert Netzwerkverkehr blockieren, ist nicht empfehlenswert, da möglicherweise auch legitime Verbindungen unterbrochen werden (für Industrial Control Systems inakzeptabel); Intrusion Detection Systeme (IDS) sollten im oberen Teil der Architektur eingesetzt werden (siehe dazu auch Abschnitt 3.1.2).
    - Um potenzielle Sicherheitslücken rechtzeitig zu erkennen und schließen zu können, ist ein aktives Vulnerability- und Patchmanagement unerlässlich (siehe z.B. die herstellerunabhängigen ICS-CERT Advisories[12]).
    - **Sicherheitsvorfälle** (in der eigenen sowie in anderen Organisationen) sollten Anlass sein, das eigene Risiko neu zu bewerten und Verbesserungsmaßnahmen einzuführen. Ein **Trendmonitoring** in Verbindung mit einem internen Monitoring in der eigenen Organisation ermöglicht die **Abschätzung der Bedrohungslage aufgrund neuer Angriffsmuster oder Exploits**)

- Das **Minimalprinzip** ist eine wichtige Strategie, um die Sicherheit eines Unternehmens zu erhöhen. Dazu gehören:
    - **Vermeiden unnötiger Anbindungen / Kommunikationskanäle** (und damit auch von Schwachstellen und Abhängigkeiten), z.B. Internetanbindung eines ICS, Nutzung externer Clouds, Verbindungen Office- und Produktionsnetz

[12] https://www.us-cert.gov/ics/advisories

- **Vermeiden unnötiger Programme und Dienste**; Entfernen von nicht benutzten, unnötigen oder unbekannten Softwarekomponenten
- **Vermeiden unnötiger Berechtigungen** (Least Privilege)
- Anmerkung: das Minimalprinzip hängt eng zusammen mit der Anforderung „sichere Konfiguration und Härtung des ICS"

– Maßnahmen zur sicheren **Konfiguration und Härtung des ICS**
Anmerkung: Hierbei handelt es sich zwar um eine klassische IT-Security-Anforderung. Für OT ist sie aber besonders relevant, da hier besonders häufig Standard-Passwörter verwendet und Sicherheitsfunktionen zum Zwecke der unbeeinträchtigten Funktionalität deaktiviert werden, was die Angriffsoberfläche vergrößert (siehe auch Anforderung „Benutzermanagement und Zugriffskontrolle"

  Zu den Maßnahmen gehört:

  - Vermeidung von **Standard-Zugangsdaten** (wie z.B. „admin")
  - Auswahl von Softwarekomponenten und -konfigurationen, die höhere Sicherheit unterstützen
  - **Validierung von Ein- und Ausgaben** zum Schutz vor Buffer Overflow und Injection-Angriffen (muss bereits bei Entwicklung und Beschaffung berücksichtigt werden)
  - Bei Einsatz von Standard-IT-Komponenten aus der Office-Welt (COTS, v.a. Bedienoberflächen und Netzwerkkomponenten) sollte besondere Vorsicht gewaltet lassen werden. Um **Schwachstellen** zu schließen und diese **nicht aus der Office-Umgebung in die ICS-Umgebung einzuschleppen sind** regelmäßige Updates unumgänglich.
  - Die Installation von **Sicherheitsupdates** sollte immer unter Beachtung von Safety- und Verfügbarkeitsanforderungen erfolgen.

– Es sollten **sichere Kommunikationsverbindungen** eingerichtet werden und insbesondere ein Augenmerk auf die **sichere Übertragung von Mess- und Steuerwerten** gerichtet werden. Dazu gehört unter anderem
  - Die Sicherstellung von **Vertraulichkeit, Authentizität und Integrität**, d.h. der Schutz vor unberechtigtem Mitlesen und vor Manipulation (Einspielen / Unterdrücken / Verändern von Daten sowie Replay-Angriffe)
  - Die direkten Auswirkungen der Kommunikationssicherheit auf **Safety-Anforderungen** (z.B. Auslösen eines Überdruckventils durch kompromittierte Sensordaten)

    - Der besonderer Schutz von Programmable Logic Controllers (PLC) und Remote Terminal Units (RTU) und deren Kommunikationsschnittstellen wie WLAN oder Ethernet.
    - Die Erkennung & Vermeidung von **physischen Manipulationen** bzw. Angriffen „zur Provokation administrativer Eingriffe" und absichtlichem Auslösen von Fehl-Alarmen

- Eine **Defense-in-Depth-Strategie** sollte implementiert werden
    - Sicherheitsmaßnahmen sollten dabei auf **verschiedenen (unabhängigen) Ebenen der Netzarchitektur** realisiert werden, so das bei Versagen einer Maßnahme greifen die weiteren Maßnahmen auf den anderen Ebenen greifen.
    - Das ICS sollte in Abhängigkeit des jeweiligen Schutzbedarfs in **verschiedene Zonen** unterteilt werden.
    - In Übereinstimmung mit der vorgenannten Anforderung sollte eine **Segmentierung des Netzwerks** durchgeführt werden, so dass zumindest das **Office-vom ICS-Netz getrennt** ist.

- **Benutzermanagement und Zugriffskontrolle**
    - Es sollten Maßnahmen zur **sichere Authentifizierung** getroffen werde (siehe auch „sichere Konfiguration"), da der physischer Zugriff auf eine Komponente es dem Angreifer maßgeblich erleichtert, auch logischen Zugriff auf das ICS zu erhalten.
    - **Administrator-Zugängen** und die zur Wartung verwendeten mobilen Datenträgern & Geräte sollten wegen der Gefahr der Ausbreitung von Schadsoftware besonders geschützt sein.
    - **Fernwartungszugängen** sollten besonders abgesichert sein. Wirksamen Schutz bietet beispielsweise eine Kombination aus Call-Back, limitierter Verbindungszeit und starker Authentisierung.
    - **Engineering Workstations**, über welche die Konfiguration und Programmierung von ICS-Komponenten erfolgt sollten besonders geschützt sein.

- **Regelmäßige technische Sicherheitsaudits** des ICS
    - Um ein realistisches Bild des Sicherheitsniveaus zu erhalten sollten **praktische Sicherheitstests** durchgeführt werden.
    - Vorsicht: **Systemstabilität und Verfügbarkeit** darf dabei nicht negativ beeinflusst werden! In produktiver Umgebung sind daher nur passive Tests

und keine Netzwerkscans zulässig. Letztere könnten das System überlasten und zu Ausfällen führen.

3.2 Industrielle Praxis und Herausforderungen

Der Industrie-4.0- und Security-Reifegrad in österreichischen Industrieunternehmen ist höchst unterschiedlich und entsprechend sind es auch die eingesetzten Maßnahmen und Strategien, die von den Betrieben eingesetzt werden. Alle befragten Unternehmen nutzen Firewalls und setzen auf die gezielte Vergabe von Rechten in der Produktion. Wenngleich im Kontext der Diffusion von Industrie 4.0 die Komponenten, Anlagen und Systeme zunehmend vernetzt werden, erfolgt dies nur dort, wo es nach Angaben der Unternehmen erforderlich ist. Nach wie vor ist daher die Trennung von Produktions-IT und Verwaltungs-IT verbreitet.

Die Schulung von MitarbeiterInnen (inkl. Anwendung der Prinzipien von Social Engineering) ist ein wichtiges Thema bei den Betrieben und auch ein zentrales Instrument zur Erhöhung des Sicherheitsbewusstseins. MitarbeiterInnen sind etwa dadurch angehalten, verdächtige Mails an die IT-Abteilung zu melden.

Unternehmen, die bzgl. Security noch am Anfang stehen, bekunden, dass die fehlende Klarheit über Sicherheitsmaßnahmen eine Barriere für die weitere Investition in Industrie 4.0 und vor allem die Vernetzung von Systemen ist. Gerade bei kleinen Unternehmen kommen die Informationen häufig von externen BeraterInnen, die tlw. bei der Auswahl der Maschinen involviert sind.

Welche Unternehmensbereiche und Ebenen treiben den Wandel voran? Die im Projekt involvierten VertreterInnen von Unternehmen argumentieren, dass die Geschäftsführung und die IT-Abteilung das Thema Security forcieren. Die Geschäftsführungen agieren dabei häufig vor dem Hintergrund von Haftungskalkülen und Complianceverpflichtungen. Darüber hinaus spielt auch die DSGVO und ISO 27000 eine Rolle. Ferner sind Kunden wichtige Proponenten für das Thema Security, etwa indem sie selbst ISO-Zertifizierungen (IEC-27000-Reihe) einfordern.

Insgesamt wird die Markttransparenz in Österreich als gering eingestuft und vor allem kleinere Unternehmen sind mitunter gar nicht in der Lage, die Anforderungen überhaupt zu definieren, um dann einen geeigneten Anbieter zu suchen.

Wenngleich viele Unternehmen bestrebt sind, Standardlösungen zu suchen, ist der Tenor der befragten ExpertInnen, dass vielfach angepasste Lösungen notwendig sind. Spezifische Anforderungen müssen durch ein „Customizing" erfüllt werden. Systemanbieter bzw. Berater beobachten hier auch bisweilen, dass Kunden häufig Standard-Security-Lösungen kaufen und sich in Sicherheit wiegen. Teilweise handelt es sich hierbei jedoch um IT-Lösungen, die nicht für den Automatisierungsbereich ausgelegt sind oder nicht adäquat integriert und betrieben werden. „Es gibt keine Security von der Stange", sagt ein Anbieter von Sicherheitslösungen in diesem Zusammenhang – Kunden müssen ihre individuelle Situation betrachten und ihre „Hausaufgaben" machen, d.h. ihr Netzwerk analysieren und absichern und langfristige Konzepte entwickeln. Darüber hinaus betonen die Industrieunternehmen, dass die permanente Herausforderung darin besteht, die Lösungen auch konsequent umzusetzen und zu „leben".

Von Seiten der befragten Anlagenlieferanten und BeraterInnen wird vor allem bei der Steuerungssoftware in der Fertigung erhebliches Verbesserungspotential gesehen. Ein Vertreter eines Unternehmens bringt dies auf den Punkt: *„Sie können die Anlagen nicht von einem auf den anderen Tag tauschen, sonst haben Sie monatelang Stillstand. Es stehen ja vielfach noch uralte Anlagen, die tun, was sie tun sollen und die in der Vergangenheit durch Netztrennung isoliert waren. Dann kommt irgendjemand und legt die Netze zusammen und plötzlich kann man die Steuerung erreichen. Damit ist Tür und Tor offen, für alles, was man tun kann."*

3.3 Bedeutung von Security-Fachkräften

In den ExpertInneninterviews wurde immer wieder betont, dass Aus- und Weiterbildung eine essenzielle, aber oft unterschätzte Maßnahme zur Erhöhung von Safety und Security ist. Bei großen Unternehmen wird das Thema Security (und damit auch Security-Training) eher systematisch angegangen (teilweise auf Druck der IT-Abteilung), bei kleinen Unternehmen ist dies stark abhängig von der Initiative der handelnden Personen bzw. EntscheidungsträgerInnen.

In der IT wurde der hohe Stellenwert von Security-Aus- & Weiterbildung bereits erkannt, zunehmend gilt das in Österreich auch für OT (Studiengänge FHs, Lehrplan HTLs). Speziell im OT-Bereich herrscht allerdings nach wie vor ein Mangel an qualifiziertem Personal. Dies gilt vor allem auch in der Ausbildung: In der Automatisierungstechnik kommen auch die AusbilderInnen aus der „klassischen Schiene" und kennen sich wenig bis gar nicht mit Security aus. Umgekehrt ist reines Security-Wissen alleine zu wenig, da sodann unter

Umständen Maßnahmen vorgeschlagen werden, die mit den Anforderungen der Automatisierungstechnik nicht vereinbar sind. TechnikerInnen reagieren in derartigen Fällen häufig abweisend. Es ist folglich fundiertes Wissen auf beiden Seiten notwendig, d.h. Security *und* Automatisierungstechnik, und man muss bei der Ausbildung der TrainerInnen beginnen („Train the Trainer"), damit diese das interdisziplinäre Wissen anschließend weitergeben können.

Die interviewten Schulungsanbieter schätzen das Security-Vorwissen vor allem bei Automatisierungstechnikern als eher gering ein: Die Personen, welche die Systeme bauen, hätten systematisch zu wenig Ahnung von Security, so der Tenor der befragten ExpertInnen. In der Automatisierungstechnik-Ausbildung lerne man Automatisierung und Elektrotechnik, aber wenig bis nichts von IT und noch weniger über Security. Aber auch in der IT sollte das Thema Security viel stärker in die Ausbildung integriert werden: Jede(r) ProgrammiererIn muss sich zwingend mit Security-Anforderungen auseinandersetzen. Security-Themen sollten folglich integraler Bestandteil der Ausbildung (IT und OT) sein, statt nur als ergänzende oder gar optionale Zusatzveranstaltung konzipiert zu sein. In diesem Zusammenhang argumentiert etwa ein befragter Experte: *„Wenn die Systeme sicherer werden sollen, müssen die Leute, die sie bauen, Ahnung von Security haben!"*

Statt nur auf Weiterbildungskurse zu setzen, deren Inhalte man schon bald wieder vergessen hat, sollten Security-Themen stärker in den Arbeitsalltag integriert und durch konkrete Hinweise und Tipps gefestigt werden, z.B. analog zu Safety-Piktogrammen (man denke an allgemeinverständliche Sicherheitshinweise auf Baustellen, die beispielsweise auf Helmpflicht hinweisen).

Positiv wurde genannt, dass Österreich im Bereich der sicherheitsspezifischen Ausbildung an Fachhochschulen und Universitäten international sehr gut aufgestellt sei, vor allem auch im Vergleich zu Deutschland. Die Ausbildung sollte allerdings herstellerunabhängig und stärker praxisbezogen sein. Viele Studierende müssten neben dem Studium arbeiten, um sich Praxiswissen anzueignen; besser wäre es, den Praxisbezug direkt ins Studium zu integrieren. Dabei betont ein befragter Experte einer Organisation, die Ausbildungen anbietet: *„In der Security sind Theorie und Praxis besonders weit voneinander entfernt."*

3.4 Good-Practice-Beispiele

Im Folgenden werden (teilweise anonymisiert) einige Beispiele aus der industriellen Praxis bzw. von der Anbieter-Seite (Technologien/Schulungen) vorgestellt, die aufzeigen sollen, wie

Unternehmen bereits heute auf die hohen Security-Anforderungen reagieren und in welche Richtung umgesetzte Maßnahmen gehen.[13]

Good Practice: Stiwa Group

Security spielt eine große Herausforderung für Unternehmen, die Automatisierungsanlagen entwickeln und produzieren. Da Steuerungssysteme zunehmend vernetzt sind, müssen zeitgemäße Lösungen gefunden werden. Das Unternehmen hat den Trend und die neuen Anforderungen früh erkannt und bereits Anfang der 2000er Jahre begonnen, eine eigene Abteilung zu gründen, die sich mit der Softwareentwicklung befasst. Diese Abteilung hat von Beginn an eng mit dem Maschinenbau und den Betreibern der Maschinen interdisziplinär zusammengearbeitet. Softwareprodukte werden heute nicht nur als Teil der eigenen Automatisierungsanlagen entwickelt und vertrieben, sondern auch als unabhängige Lösung angeboten. Mittlerweile fungiert Manufacturing Software als eigener Geschäftsbereich.

Bei der Entwicklung von Anlagen hat man begonnen, parallel zu eigentlichen Steuerungssoftware ein eigenes Datenversorgungssystem zu etablieren, bei dem auch die Mittel der IT zur Verfügung hat (z.B. Passwortverwaltung), um die Security zu erhöhen. Automatisierungsanlagen haben aber häufig eine sehr hohe Lebensdauer. Um auch diese Anlagen zu modernisieren, wird versucht durch regelmäßige Updates, den aktuellen Security-Level zu erhöhen. Zu diesem Zweck wird eine Wartungsvertrag angeboten der es dem Kunden ermöglicht durch die Installation der neusten Version der abwärtskompatiblen Software auch die Shopfloor-Ebene Up-to-Date zu halten. Teilweise wird bei älteren noch laufenden Anlagen bei Kunden die komplette Steuerung ersetzt, was die Leistungsfähigkeit der Anlagen erhöht und zugleich die Security erhöht. Ein wichtiges Prinzip bei der Entwicklung von Software ist die Standardisierung und Modularisierung von Lösungen.

Jüngst wurde im Unternehmen intern ein Netzwerk etabliert, in dem sich regelmäßig Software-EntwicklerInnen, Security-ExpertInnen und die ExpertInnen, die für den Betrieb der Anlagen verantwortlich sind, austauschen. Damit wird ein weiterer Schritt in Richtung Verschränkung von IT und OT gelegt. Beschafft das Unternehmen selbst Anlagen für die eigene Produktion, sind ebenfalls MitarbeiterInnen aus der Produktions-IT involviert.

[13] Einige Unternehmen, die sich besonders als Good Practice Beispiel eignen würden, gaben nicht ihre Einwilligung zur anonymen Beschreibung in diesem Bericht.

Good Practice: **Qualifizierungsnetz „InduSec"**

Die Experteninterviews zu SIGI haben ergeben, dass das Thema Weiterbildung von essenzieller Bedeutung ist und es gerade an der Schnittstelle IT/OT mehr Trainingsangebote mit Security-Fokus braucht. Ein Good-Practice-Beispiel in diesem Bereich ist das Qualifizierungsnetz „InduSec" zur sicheren Entwicklung und Produktion im Umfeld industrieller Steuerungssysteme. Dieses Konsortialprojekt bringt Forschungs- und Unternehmenspartner im Zuge von Schulungen zusammen mit dem Ziel, ein gemeinsames Sicherheitsverständnis von IT- und OT-Experten zu schaffen.

Die Inhalte des Lehrgangs wurden im Konsortium gemeinsam erarbeitet. Theorie-Teile und Praxismodule wechseln einander ab; anfangs werden Grundlagen vermittelt, anschließend spezielle Themen vertieft. Am Ende laufen alle Fäden in einem Planspiel zusammen, in dem das Vorgehen bei einem konkreten Cyberangriff geprobt wird. Teilnehmer sind vor allem Techniker aus IT und OT sowie Entscheidungsträger bei KMU. Kursstart war im Oktober 2019, der Lehrgang läuft bis Ende 2020.

„Bisher waren die Rückmeldungen der Teilnehmer durchweg positiv", sagt Stephanie Jakoubi, Projektleiterin beim Konsortialführer SBA Research. Viele Unternehmen haben Interesse am Lehrgang gezeigt, das Konsortium ist mit zehn Unternehmens- und vier Forschungspartnern entsprechend groß.

Das Bundesministerium für Digitalisierung und Wirtschaftsstandort fördert den Lehrgang über das Programm „Forschungskompetenzen für die Wirtschaft – Qualifizierungsnetze". Die Schulungen werden von den Forschungspartnern durchgeführt und sind für die Unternehmenspartner kostenlos. „Die Förderung hat den Unternehmen geholfen, die Weiterbildungsmaßnahmen auf Management-Ebene durchzubringen", sagt Jakoubi.

Auf Firmenseite sei die Awareness für Safety-Themen vorhanden, für Security allerdings noch nicht, sagt Jakoubi. Grund sei eine falsche Risikoeinschätzung: Viele Unternehmen glauben nach wie vor, dass sie keinen Cyberangriff fürchten müssen oder nicht interessant für Angreifer sind. „Innovation und Industrie 4.0 sind wichtig und notwendig, aber es geht nicht ohne Security", betont Jakoubi.

Good Practice: Technologieanbieter Phoenix Contact

Phoenix Contact ist ein internationales Unternehmen, welches Komponenten und Lösungen im Bereich Elektrotechnik und Automation anbietet. Dazu gehören beispielsweise Schaltgeräte, Industrie-Firewalls oder Systeme für eine sichere Fernwartung. Zu den Kunden zählen Maschinenbauer und Anlagenbetreiber. Phoenix Contact ist vor allem Hersteller und Systemintegrator, bietet aber auch als Service Provider Risikobewertungen, Schulungen und Beratung im Bereich IT/OT und Digitalisierung an.

2018 hat sich Phoenix Contact seinen sicheren Entwicklungsprozess nach IEC 62443-4-1 (Secure Product Development Lifecycle) durch den TÜV SÜD zertifizieren lassen. Eine Zertifizierung auf Komponenten-Ebene nach IEC 62443-4-2 wird ebenfalls angestrebt. Außerdem ist das Unternehmen seit 2019 auch nach IEC 62443-2-4 (ICS Security Service Provider) zertifiziert und hat eine Blueprint-Zertifizierung nach 62443-3-3 für sein Fernwartungs-System. Dieses bietet verschiedene Möglichkeiten der Absicherung (z.B. Authentifizierung, Anomalieerkennung, etc.), aus welchen der Kunde auswählen kann. Dazu braucht es aber zunächst eine individuelle Risikobewertung. „Ein Risikoverständnis beim Kunden zu schaffen ist unser Hauptziel", sagt Erich Kronfuß, Industrial IoT-Security Specialist bei Phoenix Contact.

Kern der IEC 62443 ist das Konzept der Segmentierung, d.h. Trennung verschiedener Produktions- bzw. Netzwerk-Bereiche, die möglichst unabhängig voneinander funktionieren und bei Bedarf (z.B. bei einer Störung oder im Fall eines Cyber-Angriffs) abgeschottet werden können. Auch kleine und mittelgroße Unternehmen können sich an diesem Konzept und den Vorgaben der IEC 62443 orientieren und dadurch ihre Sicherheit erhöhen, ohne den großen Aufwand einer Zertifizierung auf sich zu nehmen.

In Österreich interessieren sich bisher nur Industrieunternehmen, die kritische Infrastrukturen betreiben, für die Zertifizierungen von Phoenix Contact. „Andere Industriebetriebe kann man damit bisher nicht beeindrucken", sagt Kronfuß – auch, weil die Security Awareness dort noch nicht besonders stark ausgeprägt ist. Die Nachfrage nach 62443-zertifizierten Produkten und Dienstleistungen wird laut Kronfuß allerdings in Zukunft steigen, vor allem bei Zuliefererbetrieben, deren Kunden sie verstärkt einfordern werden. Letztendlich geht es bei der 62443 nicht vorrangig um Datenschutz, sondern um Verfügbarkeit, betont Kronfuß: „Security ist kein Selbstzweck, sondern ein Vehikel, um die Effizienz und Verfügbarkeit der Anlagen hochzuhalten."

Good Practice: Konsumgerätehersteller

Vom Unternehmen werden zahlreiche Strategien verfolgt, um im Produktionsbereich (Industrie 4.0) Safety & Security (Informations-, Daten-, und Kommunikationssicherheit) zu erhöhen. So ist die IT auf höchster Ebene im Unternehmen verankert, nämlich beim Finanzvorstand, sodass die wesentlichen Treiber für das Thema Safety & Security, der Finanzvorstand und der IT-Leiter, auch entsprechende Ressourcen zur Verfügung haben. Das Unternehmen weist eine hohe Awareness in dem Thema auf, das Risiko, Opfer von Cyberangriffen zu werden wird sehr hoch eingeschätzt. *„Die Geschäftsprozesse sind externen Hackern bekannt, daher werden Phishing-Mails immer dreister und sehen täuschend echt aus. Externe Hacker, die in das System eindringen, verschlüsseln den Rechner und verlangen Geld.*"

Die Bedrohungen, die als besonders relevant angesehen werden, sind Phishing-Angriffe, externe Hacker-Angriffe sowie eigene MitarbeiterInnen. Es werden daher zwei über Firewall getrennte Netzwerke betrieben (Office und Produktion) und tägliche Backups durchgeführt. Dabei sind die Backup-Systeme physikalisch vom Netzwerk getrennt.

Außerdem wird zu Fernwartungszwecken die Maschinennetzanbindung zum Hersteller nur gemeinsam mit dem IT-Sicherheitsteam durchgeführt (über VPN). Hier besteht eine hardwaremäßige Trennung, sodass zunächst ein Schalter umgelegt werden muss, um die Verbindung zu ermöglichen.

Externe Impulse über laufende Verbesserungen der Sicherheitsmaßnahmen kommen vor allem über Akteure im ERP-Bereich (Kooperation mit Beratern).

Zusätzlich zu diesen Maßnahmen werden sämtliche MitarbeiterInnen regelmäßig geschult, insbesondere auch drüber, was in Falle eines Cyberangriffes zu tun ist (Meldung).

Als zukünftige Maßnahmen im Bereich Security werden Standardisierung und Vereinheitlichung der Systeme als bedeutsam gesehen. Eine ISO-Zertifizierung von Maschinen für Security wird auch im Sinne einer verkaufsfördernden Maßnahme als Zukunftsthema betrachtet.

Good Practice: Cleanup-Projekt der A1 Telekom Austria AG

„Aus Security-Sicht sind viele unterschiedliche Assets eine Herausforderung", sagt Alexandra Fehringer, Leiterin Information Security und seit 2019 CISO bei A1 Telekom Austria. Unterschiedliche Hersteller, unterschiedliche Gerätetypen und unterschiedliche Service-Management-Tools erhöhen die Komplexität und den Aufwand, da Schutzbedarf, Baseline und Standards für jedes einzelne Asset definiert werden müssen. Manches läuft Gefahr, einfach vergessen zu werden, sobald man es nicht mehr benötigt – „der Lifecycle wird nicht beendet", formuliert es Fehringer. Sie hat daher 2019 gemeinsam mit ihrem Kollegen Lukas Driza als Projektleiter den „Cleanup" bei A1 initiiert: Sämtliche Assets wurden kritisch auf ihre Verwendung und ihren Nutzen geprüft, redundante oder nicht mehr benötigte Dienste und Systemkomponenten wurden migriert bzw. ganz abgeschaltet.

Die größte Herausforderung beim Cleanup war laut Fehringer die Kommunikation mit den Fachverantwortlichen: Es ist wichtig, bewusst zu machen, dass vielen Komponenten auch eine hohe Angriffsfläche darstellen und man sich von Altlasten trennen muss. Dass weniger einfach oft mehr ist. Dem Informationssicherheitsteam wurde eigens Personal zur Seite gestellt, um sie zu auch langfristig bei dieser Aufgabe zu unterstützen. „Der menschliche Kontakt ist meist besser als Automatismen", so Fehringer, und hat zusammen mit einer Security-Awareness-Kampagne dabei geholfen, alle Mitarbeiter ins Boot zu holen. „Warum wir das als Infosec machen? Weil es unser ureigenstes Interesse ist, dass wir die Assets schützen können."

Auch die Kommunikation zwischen Management und Technik stand im Fokus. Die richtigen Kennzahlen zu entwickeln, um den Projekterfolg messbar zu machen, hat wesentlich dazu beigetragen, der Geschäftsführung den konkreten Nutzen des Projektes zu verdeutlichen. Hier wurden auch kreative Vorschläge der Bediensteten aufgegriffen: Beispielsweise wurden (neben den Kostenersparnissen) die CO_2-Einsparungen durch das Abschalten ganzer Services ermittelt.

Durch den Cleanup müssen inzwischen weniger Assets verwaltet werden; es sind weniger Backups, Scans und Patches erforderlich. Die Datenqualität der Configuration Management Database (CMDB) und des SIEM-Tools sind deutlich gestiegen. Außerdem haben sich potenzielle Folgeprojekte ergeben: Nachdem das Pilotprojekt sich auf die drei Wiener Standorte der A1 beschränkt hat, werden als nächstes die regionalen Standorte aus Security-Sicht aufgerollt. Außerdem wird aktuell zwischen den sicheren Assets (GOOD), den Assets mit negativer Bewertung (BAD) und den noch nicht beurteilten Assets (UGLY) unterschieden. „Von den BAD Assets wollen wir uns klarerweise trennen", so Fehringer. Dazu wird definiert, welche Kriterien und Attribute eine „gute" Applikation ausmachen, damit künftig eine

einheitliche Metrik für den Cleanup-Prozess vorliegt. Dieser ist nämlich, wie die ganze Security-Thematik, keine einmalige Angelegenheit, sondern ständiger Re-Evaluation unterworfen.

Fehringers Rat an KMU, die eine ähnliche Aktion starten möchten, lautet daher: Die Assets müssen *regelmäßig* geprüft und zentral verwaltet werden, und zwar im Rahmen eines *einheitlichen Prozesses*. A1 führt neben der automatisierten Bewertung durch Tools inzwischen eine halbjährliche Inventur durch und erfasst auch Security-Aspekte in der CMBD, damit alle relevanten Informationen an einer Stelle vorliegen. Wenn alle Assets dezentral verwaltet werden, statt zentral, wird jede Auswertung zum Knochenjob und Fortschritte und Erfolge können nur schwer gemessen werden. Durch das Cleanup-Projekt konnten übrigens mittlerweile etwa 178.720 kWh pro Jahr eingespart werden. Es tut also auch der Energiebilanz gut und spart echtes Geld.

4 Security als Standortfaktor

4.1 Spezifika österreichischer Industrieunternehmen

Mit der zunehmenden Digitalisierung der österreichischen Industrie ergeben sich zahlreiche Herausforderungen in Bezug auf Gewährleistung der Daten-, Informations- und Kommunikationssicherheit. Nur durch entsprechende Security-Maßnahmen für den zunehmend vernetzten Produktionsbereich kann das Potenzial von Industrie 4.0 realisiert werden. Ungelöste Fragen der Security sind eine der zentralen Barrieren für die Einführung von Industrie 4.0.[14] Security wird damit zu einem wichtigen Faktor für den Produktionsstandort Österreich.

Im Allgemeinen zeigt sich, dass die österreichische Industrie durch viele kleine und mittlere Unternehmen dominiert wird. Des Weiteren hat Österreich einen großen Anteil von Medium-Low- und Medium-High-Tech-Industrien.[15] Wie in Abschnitt 2.1 gezeigt wurde, sind die Größe und die Technologieintensität der Branche eine wichtige Determinante für das Sicherheitsbewusstsein und das Ausmaß der bereits eingesetzten Security-Maßnahmen. Zukünftig werden aber auch die kleineren Unternehmen und Betriebe im Low-Tech-Bereich vermehrt digitale Produktionstechnologien einsetzen.

So planen gemäß einer Hochrechnung des EMS für Gesamtösterreich über 300 österreichische Kleinbetriebe mit unter 50 MitarbeiterInnen bis 2021 erstmalig ein echtzeitnahes Produktionsleitsystem einzuführen und knapp 300 Kleinbetriebe mobile/drahtlose Geräte für die Programmierung und Bedienung von Anlagen und Maschinen einzusetzen. Auch über 90% der erstmaligen Nutzer von Industrierobotern sind KMU. Auf Branchenebene sind Low-Tech- bzw. Medium- Low-Tech-Industrien wie Holz, Papier und Druck sowie Metallhersteller und -verarbeiter die Branchen mit der größten absoluten Zahl an Betrieben, die erstmalig echtzeitnahe Produktionsleitsysteme einzuführen planen. Aber auch eine große Anzahl an Betrieben der Nahrungs- und Getränkeindustrie plant den Einsatz der unterschiedlichen digitalen Techniken in der Produktion. Mit diesem erstmaligen Einsatz digitaler Techniken werden auch diese Unternehmen vor der Herausforderung stehen, Maßnahmen zur Erhöhung der IT-Security umzusetzen.

---

[14] Vgl. ITA und AIT (2015) sowie Lassnigg et al. (2017).

[15] Vgl. Leitner et al. (2015).

Einige weitere Besonderheiten der österreichischen Industriestruktur können auf Basis weiterer Studien und der Ergebnisse von im Rahmen des Projekts durchgeführten Interviews und Workshops genannt werden. Die ExpertInnen argumentieren, dass **Kleinunternehmen** besonders innovativ und flexibel bei der Implementierung von Sicherheitslösungen sind, ihnen aber gleichzeitig häufig die Kapazitäten fehlen, um Sicherheitsrisiken zu identifizieren bzw. umfassende Maßnahmen zu implementieren.

Neben der Betriebsgröße sind die **Zulieferstrukturen** ein Spezifikum der österreichischen Industrie. Beispielhaft kann hier etwa die deutsche Automobilindustrie angeführt werden. Diese Abnehmer haben hohe Standards bei der Sicherheit, die sie auch bei ihren Zulieferern einfordern.

Des Weiteren kann angeführt werden, dass Betriebe dann eine hohe Awareness für Security haben, wenn ein sehr großes **Verantwortungsbewusstsein** in ihrer Tätigkeit liegt (z.B. Wahrung von Intellectual Property oder KundInnendaten). Die befragten ExpertInnen argumentieren ferner, dass der Energiesektor und die Betreiber kritischer Infrastrukturen als Vorreiter für die Erhöhung des Bewusstseins und die Einführung von Security-Lösungen betrachtet werden können. Hier können etwa das Austrian Energy CERT (AEC) für die österreichische Energie angeführt werden, das sich zum Ziel gesetzt hat, die IT-Sicherheitskompetenz im Energiesektor zu erhöhen.[16] Das laufende Security Incident Management, also die Bearbeitung von eingehenden Anfragen und Sicherheitsmeldungen, die Durchführung von Schulungstätigkeiten und die Mitarbeit bei der Erstellung technischer Sicherheitskonzepte stellen dabei wichtige Aufgabenbereiche dar.

Nach Einschätzung der involvierten ExpertInnen besteht eine besonders große Herausforderung in der Integration von älteren Automatisierungsanlagen und Steuerungssystemen. Security-Maßnahmen sind oft nicht inhärent in den Anlagen verankert, sondern werden nachträglich hinzugefügt, was kostenintensiv und komplex ist. Ein Grund hierfür ist, wie von mehreren Experten angeführt, dass Hersteller von Produktionsmaschinen derzeit wenig strategische Sicherheitslösungen parat haben und Security nicht Teil ihrer Verkaufsstrategie ist; auf der anderen Seite formulieren Kunden ihre Security-Anforderungen eher als Option, statt darauf zu bestehen. Als weitere Barriere wurden fehlende Best Practices genannt: In der Elektro- und Automatisierungstechnik gibt es lang erprobte Methoden und Lösungen, auf die man zurückgreifen kann; im (industriellen) Security-Bereich sind eher individuelle, domänenspezifische Lösungen erforderlich. Ein möglicher Trend sind daher spezialisierte Angebote und Individuallösungen.

[16] Vgl. https://www.energy-cert.at/de/

Die kleinstrukturierte Anbieter- als auch Nachfragelandschaft führt in Kombination mit der überschaubaren Größe Österreichs dazu, dass sich die Akteure kennen, was zugleich den Austausch über sicherheitsrelevante Themen begünstigt („man kennt sich und redet auch über sensiblere Themen"). Dies ist notwendig, da Sicherheitsbewusstsein und Kapazitäten zur Umsetzung von Sicherheitsmaßnahmen in KMU intern oft nicht vorhanden sind. Dabei sind fehlende Ressourcen bei produzierenden KMU nicht nur oder in erster Linie monetär zu verstehen, sondern auch zeitlich. Der Know-how-Aufbau und die Förderung des Sicherheitsbewusstseins erfordern entsprechende zeitliche Ressourcen und den Willen, MitarbeiterInnen für Schulungen freizustellen. Einige ExpertInnen argumentieren ferner, dass die Fehlerkultur in Bezug auf Security und das Bewusstsein dafür im Allgemeinen schwach ist, auch, da Vorfälle nicht öffentlich werden. Mehr hierzu findet sich in Abschnitt 4.3.

4.2 Vorhandene Kompetenzen, Lösungen und Produkte

Während im vorangegangenen Kapitel die Spezifika der österreichischen Industriestruktur dargestellt wurden, soll im Folgenden der Frage nachgegangen werden, welche besonderen Kompetenzen, Lösungen und Produkte in Österreich für den Bereich Security im Produktionssektor vorhanden sind und wo Lücken und Schwächen gesehen werden.

Der Anbietermarkt für Safety und Security ist in Österreich nach Angaben der ExpertInnen (wie auch die Industriestruktur) klein strukturiert. Dies bietet Herausforderungen, aber auch Chancen. Was die Beurteilung der Frage betrifft, ob ein Mangel an Lösungen vorliegt, variiert die Einschätzung der in dieser Studie involvierten ExpertInnen. Dabei stellt sich zunächst die Frage, ob die Lösungen zwingend von österreichischen Akteuren entwickelt bzw. angeboten werden müssen. Weiters stellt sich die Frage, ob Lösungen aus dem Ausland vertraut werden kann. Einige Akteure argumentieren, dass Lösungen durch die österreichischen aber auch internationalen Anbieter prinzipiell vorhanden sind, jedoch die Lösungen nicht effektiv eingesetzt werden. In der Verwendung von Basistechnologien, Open Source- und Freeware-Lösungen wird eine Antwort gesehen. In Österreich existieren viele innovative KMU, die innovative Sicherheitslösungen entwickeln und anbieten und auf Basis ihrer Flexibilität die Integration von immer komplexeren Systemen als Chance nützen können.

Wenngleich keine systematischen empirischen Befunde vorliegen, argumentieren einige ExpertInnen hingegen auch, dass in Österreich ein Mangel an geeigneten Lösungen vorliegt: So gibt es nach deren Angaben keine spezifischen Application-Whitelisting-Lösungen, zu wenig IDS/IPS-Traffic-Analyse- oder Netzwerk-Inventory-Tools. Weiters wird angeführt, dass es an Schnittstellen fehlt, die es ermöglichen, alles aus einer Hand anzubieten. Fehlende Überwachungssysteme und transparente Lösungen (Support, Schulungen, Wartung,

Ansprechperson auf Augenhöhe) werden ebenso genannt wie zu wenig interdisziplinäre Kompetenzen. Des Weiteren wird auf die bislang fehlenden spezifischen Standards für Industrie-4.0-Anwendungen hingewiesen. Auch Fragen der Interoperabilität stellen sich in diesem Zusammenhang, wobei der „Connect Actors"-Ansatz im Medizintechnikbereich als Vorbild gesehen wird. Im Allgemeinen wird im Vergleich zu anderen Branchen wie dem Banken- oder Energiesektor im produzierenden Bereich eine größere Notwendigkeit gesehen, stärker domänenspezifische Lösungen einzusetzen.

Im Zusammenhang mit der geforderten Entwicklung von Security-Lösungen wird eine Schwäche darin gesehen, dass es in Österreich kaum eine Hardware-Entwicklung und -Produktion gibt. Im Weiteren wird argumentiert, dass es schwierig ist, die öffentliche Beschaffung als Innovationstreiberin zu nutzen. Das mangelnde Bewusstsein geht einher mit einer nur bedingten Investitionsbereitschaft der österreichischen Industrie in Security-Lösungen.

Einige ExpertInnen argumentieren hingegen wiederum, dass die entsprechenden Lösungen hierzulande zwar vorhanden sind, aber das Bewusstsein bei den Unternehmen fehlt. Hier kann etwa angeführt werden, dass die involvierten ExpertInnen schätzen, dass rund 40% der Unternehmen Cyber-Angriffe nicht erkennen. Überhaupt ist nach Einschätzung der involvierten ExpertInnen das Bewusstsein für Security in Europa nicht besonders ausgeprägt. Themen wie Cyber War, „Asymmetric Hybrid Warfare" und Industriespionage können hier in die Diskussion eingebracht werden.

Insgesamt sind sich die im Zuge des Projekts involvierten ExpertInnen einig, dass der Markt für Security-Lösungen relativ intransparent und „überfüllt" ist: Es gibt viele unterschiedliche Anbieter mit unklaren Priorisierungen bzw. Abgrenzungen. Besonders Unternehmen, die erst jüngst begonnen haben, die Produktion zu digitalisieren und noch kein klares Bild über die Anforderungen haben, stehen vor der Herausforderung, Lösungen der unterschiedlichen Anbieter zu vergleichen. Aus Sicht eines großen Anbieters von Sicherheitslösungen ist es daher wichtig, mit den Kunden vorab über deren Anforderungen und Wünsche zu sprechen und Transparenz zu schaffen. Ein anderer Anbieter erwähnt in diesem Zusammenhang, dass viele Kunden nach der ersten Analyse abgeschreckt wären, wenn sich erweist, dass eine einfache bzw. oberflächliche Lösung nicht zielführend sei; häufig beschäftigen sie sich erst dann wieder mit dem Thema Security, wenn Verdacht auf einen Angriff oder ein Sicherheitsproblem besteht.

Eine spezifische Chance für Österreich wird in der Entwicklung von Speziallösungen gesehen, z.B. in der Tiefenanalyse von Chips in Produktionsanlagen, HW-Verifikation, FPGAs; HW-Trojaner, Machine Learning für Aktive/Reaktive Sicherheit und Erkennung.

Eine Chance zur Reduktion der Schwächen wird darin gesehen, vorhandene etablierte Cluster (thematisch/technologisch) für Security zu nutzen, insbesondere um Bewusstsein zu erhöhen und Know-how gemeinsam aufzubauen. Des Weiteren könnten Gewerbezonen und Industrieparks genützt werden, um Security als Infrastruktur zur Verfügung zu stellen.

4.3 Kommunikation und Zusammenarbeit bei Sicherheitsvorfällen

Im Folgenden soll der Fragestellung nachgegangen werden, wie es um die Kommunikation und Zusammenarbeit bei Sicherheitsvorfällen in der österreichischen Industrie steht.

Der gegenseitige Austausch von Informationen zu Sicherheitsvorfällen und Erfahrungen im Cybersecurity-Bereich (innerhalb der Branchen, aber auch auf nationaler und internationaler Ebene) wird von den ExpertInnen als wichtig bezeichnet. Entsprechende Trust Circles funktionieren bei großen Unternehmen und in bestimmten Branchen gut, beispielsweise das EnergyCERT im Energiesektor, wo die einzelnen Anbieter nicht in Konkurrenz stehen und daher wenig Berührungsängste haben. Auch in der Finanz- und Versicherungsbranche gibt es bereits entsprechende Gremien und Foren zum gegenseitigen Austausch, obwohl hier die Konkurrenzsituation viel stärker gegeben ist. Weniger gut funktioniert der Austausch bei kleineren Unternehmen, bei denen das stetige Sichten und Analysieren entsprechender Informationen auch eine Ressourcenfrage ist und die Unternehmen in der Regel schnell überfordert.

In der Produktion ist die Kommunikation über Sicherheitsvorfälle bisher sehr zurückhaltend, was mit dem eher schwach ausgeprägten Security-Bewusstsein zusammenhängt; man hat hier noch „sehr viel Respekt" vor einem gegenseitigen Austausch, obwohl gerade die ProduktionsleiterInnen hiervon profitieren könnten. Sensible Informationen werden eher über private Kontakte ausgetauscht, denn Vertrauen ist eine Grundvoraussetzung für eine solche Verständigung. Vertrauensbildende Maßnahmen könnten daher die Bereitschaft zum Austausch steigern. Ein ganz anderer, womöglich effektiverer Ansatz wäre eine gesetzlich festgeschriebene Meldepflicht, wie es sie zum Teil bereits in anderen (kritischen) Branchen gibt (z.B. Energie). Auch die Zulieferer sollten hier in die Pflicht genommen werden, beispielsweise mittels standardisierter Lastenhefte.

Wichtige Fragen im Zusammenhang mit der Kommunikation von Sicherheitsvorfällen sind: **Was** wird **wie** und **wann** an **wen** gemeldet? Was passiert **nach** der Meldung?

- **Was**: Wird eine festgestellte Anomalie im System gemeldet? Oder erst ein erfolgreicher Angriff? Oder bereits der Verdacht auf einen Angriff?

- **Wie**: In welcher Form und Granularität erfolgt die Meldung? Bei der Offenlegung sind verschiedene Stufen denkbar (vgl. CERT), je nachdem, wie viele Organisationen potenziell betroffen sind, wie einfach sich die Sicherheitslücke ggf. ausnutzen lässt bzw. ob es bereits eine Lösung für das Problem gibt.
- **Wann**: Zu welchem Zeitpunkt erfolgt die Meldung, bereits bei einem Verdacht oder erst nach erfolgter Analyse?
- **An wen**: Wer wird informiert? Weitere, potenziell betroffene Unternehmen in der gleichen oder auch in anderen Branchen; Behörden? Denkbar wäre eine zentrale Stelle, eine Art „Industrie-CERT", wo die gemeldeten Vorfälle gesammelt und ggf. weiterverbreitet werden.
- **Follow-Up** nach der Meldung: Werden auch weitere Entwicklungen bzw. Gegenmaßnahmen kommuniziert? Welchen Mehrwert hat der/die MelderIn durch die Meldung („was habe ich davon")?

Gerade die letzte Frage ist zentral für die Akzeptanz einer Plattform zum gegenseitigen Austausch – der Informationsaustausch sollte grundsätzlich in beide Richtungen erfolgen: Vorfälle sollten an eine zentrale Instanz, eine Art „Industrie-CERT" gemeldet werden; umgekehrt sollte diese Zentrale aber auch konkrete Unterstützung anbieten und eine erste Anlaufstelle bei Fragen und Sicherheitsproblemen sein. Folglich müssen dort auch „echte ExpertInnen" sitzen.

Als weiterer Faktor wurde hier auch die Fehlerkultur in Österreich genannt: Im Gegensatz zu beispielsweise den USA oder Skandinavien, wo man Fehler eher als etwas Positives sieht, aus dem man gemeinsam lernen kann („learning by failure"), werden Fehler hierzulande negativ wahrgenommen als etwas, worüber man besser nicht spricht. Dabei kann ein proaktiver Umgang mit Sicherheitsvorfällen von außen durchaus positiv registriert werden und ggf. einem Imageschaden vorbeugen (Beispiel: Umgang mit Trojaner Emotet bei der Firma Heise im Mai 2019). Ein Austausch kann dazu beitragen, Security als Wettbewerbsvorteil darzustellen, und Vorbilder können andere motivieren, aktiv zu werden.

Um ein positiveres Image für das Thema Security und den gegenseitigen Austausch zu schaffen, könnten die ausgetauschten Inhalte auch erweitert werden, indem man nicht nur über Sicherheitsvorfälle berichtet, sondern auch über Best Practices, Erfahrungen und erfolgreiche Maßnahmen. Zusätzlich sollte man einen informellen Austausch in Konferenzen und Symposien fördern.

Für den Umgang mit konkreten Sicherheitsvorfällen wurde der Wunsch nach einer „Task Force" genannt (beispielsweise als Teil des Bundesministeriums für Landesverteidigung). Eine solche Gruppe technischer Top-ExpertInnen, die auf nationale und

herstellerunabhängige Ressourcen zurückgreift, vermag im Angriffsfall rasch und kompetent zu helfen und agiert dabei nicht im Verborgenen, sondern offen und transparent.

4.4 Handlungsempfehlungen für Industrieunternehmen

Eine Reihe von strukturellen Faktoren haben einen Einfluss auf das Sicherheitsbewusstsein in Unternehmen und das Ausmaß der eingesetzten Maßnahmen. Die Unternehmensgröße, die technologische Intensität der Branche, die Intensität von Industrie-4.0-Technologien, Zulieferbeziehungen, die Internationalisierung, und die Bedeutung von Intellectual Property für das Geschäftsmodell sind wichtige Determinanten. Was die internen Prozesse und Faktoren betrifft, wird Security bei Unternehmen, die einen hohen Security-Reifegrad aufweisen, als strategisches Thema positioniert und als kontinuierlicher Verbesserungsprozess aufgesetzt. Darüber hinaus haben die führenden Unternehmen entsprechende Teams mit enger Verbindung zur Geschäftsführung etabliert, ein gut dotiertes Budget geplant und sind durch hohe Kompetenzen der IT-LeiterIn charakterisiert.

Auf Basis der durchgeführten Analysen können folgende Empfehlungen für Unternehmen abgeleitet werden:

- **Security als strategisches Thema positionieren**: Eine ganzheitliche und strategische Sicht auf Security ist zentral. Security muss dabei als kontinuierlicher Improvement-Prozess gesehen bzw. gelebt werden und wird damit Teil der Unternehmenskultur.[17] Dies kann nur gelingen, wenn Security unter dem Vorstand bzw. der Geschäftsführung positioniert ist, auch um nötige Aufmerksamkeit und die Ressourcen zu sichern. Dadurch wird auch vermieden, dass sich Unternehmen Security-Produkte anschaffen und sich in (falscher) Sicherheit wiegen. Eingebettet in den strategischen Rahmen müssen die Unternehmen den Kommunikations- und Schutzbedarf festlegen und Risikoanalysen durchführen. Gleichzeitig müssen Unternehmen als Beschaffer von Industrie-4.0-Lösungen bei den Herstellern aktiv Sicherheitseigenschaften einfordern, beispielsweise in Form von Lastenheften.

- **Bewusstsein für Bedrohungen im Unternehmen erhöhen**: Wenngleich die Awareness in den letzten Jahren gestiegen ist, gibt es noch einen hohen Handlungs- und Aufklärungsbedarf in der Industrie. Vor allem kleinere Betriebe haben die Einstellung: „Mir wird schon nichts passieren!" Mangelndes Bewusstsein impliziert eine geringe

[17] Ein befragter Experte bringt dies auf den Punkt, wenn er argumentiert: *„Es wird nie wieder so wenig los sein wie heute. Die Hacker sind immer einen Schritt voraus. Es wird nie aufhören. Es wird immer mehr."*

Bereitschaft zu strategischem und proaktivem Handeln und externer Kommunikation, etwa bei tatsächlichen Sicherheitsvorfällen. Als primäres Risiko gelten die MitarbeiterInnen, entsprechend haben Awareness-Kampagnen zunächst hier anzusetzen.

- **„Hausaufgaben" machen**: Industrieunternehmen und Anlagenbetreiber sollten auf Basis einer Risikoanalyse individuelle Maßnahmen setzen und langfristige Konzepte entwickeln. Ein erster Schritt ist, innerhalb des Unternehmens die Assets samt ihrem Schutzbedarf zu identifizieren und entsprechende technische und organisatorische Sicherheitsmaßnahmen (z.B. im Bereich Netzwerksegmentierung und Authentifizierung) zu setzen. Erstes Ziel sollte sein, eine vernünftige Basis zu schaffen, um sich vor einfachen Angriffen zu schützen. Freilich ist dies keine einmalige Aktion, sondern ein Prozess, der regelmäßig durchlaufen werden muss.

- **Interne und externe Kommunikation fördern**: Zur Reduktion von Sicherheitsrisiken ist die Kommunikation zwischen Führungskräften und MitarbeiterInnen im Allgemeinen sowie zwischen IT und OT (IT- und ProduktionsleiterIn) im Speziellen durch das Management zu fördern. Durch gezielte Maßnahmen soll der Austausch zwischen den MitarbeiterInnen der entsprechenden Abteilungen gefördert werden.
  Des Weiteren sind Maßnahmen zu setzen, die das Lernen innerhalb der Branche ermöglichen und auch dazu führen, dass sich Unternehmen gegenseitig bei Vorfällen warnen (z.B. Austausch über Vorfälle durch Trust Circles). Durch die Vernetzung mit anderen Betrieben kann überdies die Standardisierung von Lösungen vorangetrieben werden. Der Austausch mit anderen Unternehmen schafft auch Orientierung bei der Implementierung von Security-Lösungen in einem Markt, der tendenziell als intransparent betrachtet wird. Organisationen wie der Verein Industrie 4.0 können ebenfalls als Plattform für den Austausch sicherheitsrelevanter Informationen dienen.

- **Qualifizierung und Schulung vorantreiben**: Die Rekrutierung und die Bindung von hoch qualifizierten MitarbeiterInnen (an der Schnittstelle zwischen IT und OT) ist eine zentrale Herausforderung für Industrieunternehmen. Internationales Recruiting und entsprechende Budgets sind eine Voraussetzung, wenngleich kleinere Unternehmen in peripheren Regionen hier vor teilweise schwierigen bzw. unlösbaren Aufgaben stehen. Jedenfalls ist die Qualifizierung der MitarbeiterInnen, etwa auch im Rahmen eigener Akademien und in Kooperation mit spezifischen Anbietern, eine wichtige Strategie zur Erhöhung der Security. Weiterbildungsmaßnahmen sollten möglichst in den Arbeitsalltag integriert werden, statt nur in Form von Kursen angeboten zu werden, deren Inhalte man schnell wieder vergisst.

- **F&E-Projekte durchführen**. Die Notwendigkeit, selbst F&E-Projekte durchzuführen, hängt von der Komplexität der Produktion und den damit verbundenen Anforderungen ab. Unternehmen, die selbst F&E-Projekte durchführen, sollten sich als Partner in F&E-Netzwerke auf nationaler und europäischer Ebene einbringen.

4.5 Handlungsempfehlungen für die Politik

4.5.1 Forschung und Entwicklung

Die Förderung der Entwicklung von spezifischen Lösungen ist ein wichtiges Element im Zuge des digitalen Wandels des Produktionssektors, weshalb es wichtig ist, spezifische Maßnahmen zur Förderung von F&E zu setzen. Für die F&E-Politik ergeben sich folgende Schlussfolgerungen:

- Bei der Entwicklung von Security-Lösungen müssen die Entwickler mit produzierenden Unternehmen zusammenarbeiten. Bei aktuellen Forschungsprogrammen der FFG (Produktion der Zukunft, IKT der Zukunft, KIRAS) sollten vornehmlich kooperative Projekte gefördert werden. Dadurch kann auch gewährleistet werden, dass die spezifischen Bedürfnisse des österreichischen Marktes adressiert werden. Durch die Einbindung der Industriekunden wird auch dem Prinzip von Open Innovation nachgekommen und es können echte Marktbedürfnisse adressiert werden.

- Ein großer Bedarf für F&E-Projekte wird bei den Maschinen- und Anlagenproduzenten, etwa Automatisierungstechnikunternehmen, gesehen. Vor allem bei der Entwicklung von Steuerungssoftware müssen sich Unternehmen stärker mit Security-Aspekten befassen. Auch die Entwicklung von Cloud-Lösungen ist ein zunehmend wichtiges Thema, das viele Akteure betrifft und Kooperation erfordert. Im Rahmen von geförderten Projekten müssen Security-SpezialistInnen eingebunden werden, die gemeinsam mit AutomatisierungstechnikerInnen umsetzbare Vorschläge entwickeln.[18]

- Bislang werden etablierte F&E-Netzwerke auf europäischer Ebene vor allem von größeren Unternehmen dominiert. Es sind Maßnahmen zu setzen, damit KMU an diese

[18] Ein befragter Experte spricht hier vom „Dornröschenschlaf Automatisierungstechnik" und davon, dass es einen massiven Nachholbedarf gibt. Dabei sind ausgeklügelte Konzepte notwendig, um Steuerungssoftware und Automatisierungstechnik nachzurüsten, die teilweise noch auf Systemen aus den 1980er- oder 1990er-Jahren basieren. Hier müssen andere Ansätze gewählt werden, um Anomalien zu erkennen und zu verhindern, siehe auch Abschnitt 3.1.6.

Netzwerke herangeführt werden und gleichzeitig verhindert wird, dass nach Abschluss der Projekte hoch qualifizierte MitarbeiterInnen das Unternehmen verlassen.

- Die F&E-Förderung ist auch dahingehend zu gestalten, dass die Kontinuität gesichert wird aber gleichzeitig bei der Abwicklung auch die Flexibilität erhöht wird, etwa dann, wenn sich Entwicklungspfade als unrealistisch herausstellen und kurzfristig Adaptionen des Programms wichtig wären („Projekt umplanen anstelle von Deliverables nach Plan abarbeiten").

- Für die Definition von möglichen inhaltlichen Schwerpunkten ist eine entsprechende Risiko- und Zielgruppenanalyse notwendig. Mögliche thematische Schwerpunkte der F&E-Förderung ergeben sich jedenfalls an der Schnittstelle zwischen Automatisierungs- bzw. Steuerungstechnik und Security.

- Die F&E-Aktivitäten sind in enger Abstimmung mit den Aktivitäten im Kontext der Standardisierung und Kommunikation (siehe Abschnitt 4.5.3 und 4.5.4) durchzuführen.

- Kein direktes Thema der klassischen F&E-Förderung ist die Schaffung von Rahmenbedingungen für Risikokapital. Dennoch wurden von den im Projekt konsultierten ExpertInnen darauf hingewiesen, dass in Österreich Risikokapital nach wie vor ein Engpass ist, wenn es um die Finanzierung bzw. das Upscaling von innovativen Projekten und Unternehmen geht.

4.5.2 Aus- und Weiterbildung

Der Bereich der Aus- und Weiterbildung ist von zentraler Bedeutung für die Erhöhung der Security Awareness in den Unternehmen wie auch in der gesamten Gesellschaft. Konkrete Empfehlungen, die Aus- und Weiterbildung betreffen, lauten:

- Förderung der Zusammenarbeit aller betroffenen Stakeholder (Sozialpartner, Interessensverbände, Bildungsträger, etc.) für die Bedarfsbestimmung neuer Berufsbilder und damit auch geänderter Aus- und Weiterbildungsangebote für Produktions- und IT-Sektor.

- Darüber hinaus ist die verstärkte Abdeckung von IT-Grundkenntnissen in der Primar- und Sekundarstufe notwendig. Diese „digitale Grundkompetenz" wird in Zukunft in allen Arbeitsmarktsektoren benötigt werden und ist eine Voraussetzung für die Entwicklung neuer bzw. die Weiterentwicklung bestehender Berufsbilder im Produktionssektor. Sämtliche Aktivitäten, die in der Vergangenheit zur Förderung von MINT und zum IT-Unterricht in der Sekundarstufe gemacht wurden, sind im Kontext dieser Studie daher zu

begrüßen. Das Thema Security muss dabei explizit auch bei der LehrerInnen-Ausbildung integriert werden.

- Gemeinsame Definition von Rahmenbedingungen, die erforderlich sind, damit bei jungen, innovativen Menschen das Interesse für den Produktions- und IT-Sektor als Ausbildungs- bzw. Studienbereich geweckt werden kann: Dies umfasst nicht nur die Attraktivierung und Bewerbung bestehender Ausbildungen und Studien, sondern auch die Förderung von entsprechenden Berufsbildern am Arbeitsmarkt, die das Interesse von jungen Menschen wecken.
- Moderne und digitale Lehrmethoden sollen bei der Security-Aus- und Weiterbildung zum Einsatz kommen. Ein Preis für innovative Ausbildungsprogramme im Bereich Security könnte geschaffen werden.
- Cybersecurity-Kompetenzen sind sowohl im Rahmen der klassischen IT-Lehrgänge zu verankern, als auch bei den Maschinenbau- und Automatisierungstechnik-Curricula an den Hochschulen, HTLs und Colleges. Damit wird zugleich das Bewusstsein für das Thema weiter vorangetrieben. Die Lehrgänge sollten dabei möglichst herstellerunabhängig und praxisbezogen sein.
- Wenngleich die Organisation von „Hacker-Events" jüngst in Österreich an Popularität gewonnen hat, sind derartige Veranstaltungen und Formate weiter zu forcieren. Aus- und Weiterbildungseinrichtungen sollten derartige Events organisieren.
- Um die Kompetenzen von Unternehmen im Security-Bereich gezielt zu stärken, sollten Schulungsmaßnahmen wie Aus- und Weiterbildungsnetzwerke gefördert werden. Ein bereits existierendes Beispiel sind die von der FFG geförderten Innovationslehrgänge.
- Die Etablierung von Digital Innovation Hubs (DIH) in Österreich sollte vorangetrieben werden und wird derzeit vom Bundesministerium für Digitalisierung und Wirtschaftsstandort unterstützt. Sie sollen als zentrale Anlaufstelle für Unternehmen insbesondere KMU, Start-ups und Mid-Caps den Zugang zu Technologietests, Finanzierungsberatung, Marktinformationen und Networking-Gelegenheiten ermöglichen.[19].

[19] Vgl. https://ec.europa.eu/digital-single-market/en/digital-innovation-hubs
Vgl. https://www.ffg.at/dih

4.5.3 Standardisierung und Zertifizierung

Das Thema der Standardisierung spielt eine besonders wichtige Rolle im Zusammenhang mit der Erhöhung der Sicherheit in der zunehmend digitalisierten Produktion. In diesem Kontext wird die Umsetzung folgender Maßnahmen empfohlen:

- Im Hinblick auf das Thema Standardisierung und Zertifizierung gilt im Allgemeinen, dass relevante Normen teilweise schon vorhanden sind (beispielsweise ISO 27000 oder IEC 62443), allerdings noch Best Practices fehlen. Des Weiteren sind die konkreten Anwendungen nicht immer klar und vor allem kleinere Unternehmen damit schnell überfordert. Hier können Leitfäden helfen, die AnwenderInnen darin unterstützen, den richtigen Standard (-Teil) für ihre Zwecke zu identifizieren. Teilweise existieren solche Leitfäden bereits, z.B. der „Orientierungsleitfaden für Hersteller zur IEC 62443" des Zentralverbands Elektrotechnik- und Elektronikindustrie e. V. (ZVEI).
- Die branchenunabhängige Norm IEC 62443 ist im Bereich der industriellen Automatisierung weit verbreitet und allgemein anerkannt, auch wenn es in Österreich bisher wenige Zertifizierungen nach dieser Norm gibt. Aufgrund ihrer zentralen Bedeutung für Sicherheit in der Industrie 4.0 wurde die IEC 62443 in Abschnitt 3.1.3 kurz erläutert. Die IEC 61508-1 für den Bereich der funktionalen Sicherheit verweist bezüglich der Cybersecurity auf die IEC 62443, da Safety immer auch ein gewisses Maß an Security erfordert (vgl. ZVEI S.5). Auch seitens der ExpertInnen wurde betont, dass man Safety mit Cybersecurity verknüpfen müsse und es beispielsweise keine Safety-Zertifikate von Cyber-Physical Systems ohne Cybersecurity-Audits geben dürfe.
- Es ist weiters Orientierung zu geben, was tatsächlich zertifiziert werden soll, d.h. wo eine Zertifizierung einen echten Mehrwert schafft (beispielsweise im Hinblick auf Interoperabilität oder Sicherheit) und wo nicht unbedingt. Letztendlich bestimmt der Markt, wo eine Zertifizierung erforderlich ist. Zugleich muss die öffentliche Hand zertifizierte Produkte bzw. Systeme dort einfordern, wo es sinnvoll erscheint und die Sicherheit dadurch gesteigert wird.
- Im Allgemeinen stellt sich bei sämtlichen Maßnahmen im Kontext der Zertifizierung und Standardisierung die Frage, ob diese auf nationaler oder internationaler Ebene durchgeführt werden soll. In diesem Zusammenhang sollten die Interessen Österreichs bei den entsprechenden europäischen Institutionen mit Nachdruck eingebracht werden.
- Schließlich wird von einigen der im Projekt involvierten ExpertInnen die Förderung eines „European Trusted Hardware und Software"-Siegels empfohlen, um in Europa auf eigene, sicherheitsgeprüfte Produkte zurückgreifen zu können und unabhängig von ausländischen Märkten und ggf. unsicheren Komponenten zu sein.

4.5.4 Bewusstseinsbildung und Kommunikation

Bewusstseinsbildung, Reduktion von Unsicherheiten durch Schaffung eines Orientierungsrahmens und Eliminierung von Kommunikationsbarrieren sind neben traditionellen Instrumenten ebenfalls Aufgaben moderner IKT- und Innovationspolitik. Die rasante Entwicklung der Digitalisierung kann dabei aufgrund der fehlenden Awareness für IT-Security als gesellschaftliches Problem gesehen werden. In diesem Bereich können folgende Empfehlungen formuliert werden:

- **Aufbau von Wissens-Datenbanken**: Der Aufbau einer Wissens-Datenbank auf Basis von Meldungen über Sicherheitsvorfälle kann dazu beitragen, das Bewusstsein zu erhöhen und Lernen zu ermöglichen. Kontrovers diskutiert wird, ob in diesem Zusammenhang eine gesetzliche Meldepflicht eingeführt werden soll, oder ob geeignete Incentives für Meldungen etabliert werden sollten. Auch müsste ein entsprechendes Design der Strukturen und Prozesse geschaffen werden (z.B. Anonymisierung), sodass die Bereitschaft zum Austausch gefördert wird. Als Vorbild fungieren hier sogenannte als Information Sharing and Analysis Centers (ISACs), die in einigen europäischen Ländern von Non-Profit-Organisationen betrieben werden.[20]
- Die **Etablierung eines „österreichischen BSI"** in Anlehnung an das deutsche Bundesamt für Sicherheit in der Informationstechnik wird von einigen österreichischen ExpertInnen ebenfalls vorgeschlagen.[21] Hierbei sollte auch die Frage nach einem sinnvollen Portfolio einer solchen nationalen Einrichtung geklärt werden. Eine derartige zentrale Stelle könnte beispielsweise Kompetenzen bündeln, Risikoanalysen und Zielgruppenanalysen durchführen und Anreize für die Entwicklung von Märkten schaffen.
- **Bewusstsein bei KMU fördern**: Bei kleineren Unternehmen ist die IT mitunter ausgelagert, weshalb sich hier spezifische Herausforderungen stellen. Eine zentrale Anlaufstelle für Security-Anfragen, etwa durch die WKÖ, ist eine Maßnahmen. Weiters sind allgemeinverständliche Leitfäden und Richtlinien (z.B. Top-10-Bedrohungen der ExpertInnengruppe Security & Safety der Industrie-4.0-Plattform) von hoher Relevanz. Nicht nur für KMU, sondern für alle Unternehmen gilt es dabei das Bewusstsein zu fördern, dass Prävention wichtig ist und nicht erst gehandelt werden soll, wenn etwas passiert ist. Der Staat bzw. die Förderorgane sollten hier aktiv auf KMU zugehen und gemeinsam Lösungen entwickeln.
- Führende Unternehmen agieren zu dem Thema bereits heute im Netzwerk ihrer gesamten Wertschöpfungskette. Durch Vorgaben solcher Leitbetriebe an beispielsweise ihre Zulieferer und eine verstärkte Zusammenarbeit auf diesem Gebiet können

[20] Vgl. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing
[21] Vgl. https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html

Lerneffekte erzielt werden und auch mittlere und kleinere Unternehmen ihre Awareness und Professionalität erhöhen. Förderprogramme wie z.B. das Kompetenznetzwerkförderprogramm der FFG, können hier als wirksame Maßnahme angeführt werden.

5 Zusammenfassung

Die Erfüllung der Informations-, Daten-, und Kommunikationssicherheit ist einer der zentralen Herausforderungen für die Implementierung von Industrie 4.0. Sämtliche Kommunikations-, Produktions- und Entscheidungsprozesse funktionieren nur, wenn die IKT-Infrastrukturen zuverlässig zur Verfügung stehen und gegenüber Ausfällen und Bedrohungen widerstandsfähig konzipiert sind. IT-Sicherheitsvorfälle bedrohen dabei nicht mehr nur einzelne Unternehmen, sondern können weitreichende Auswirkungen auf die wirtschaftliche Entwicklung insgesamt haben.

Vor diesem Hintergrund hatte die vorliegende Studie das Ziel, empirische Befunde zum vorhandenen Security-Bewusstsein und den gesetzten Maßnahmen von Seiten der österreichischen Industrie aufzubereiten. Des Weiteren wurden aus Sicht der Anbieter von Security-Lösungen der Status-quo und die Entwicklungsperspektiven beleuchtet. Neue technische und organisatorische Sicherheitsanforderungen wurden im Kontext internationaler Standardisierungsbestrebungen herausgearbeitet. Um Security als wesentlichen Standortfaktor für Österreich zu etablieren, war ein weiteres Ziel, Handlungsempfehlungen für Industrieunternehmen und die Politik aufzuzeigen.

Insgesamt kann konstatiert werden, dass das Sicherheitsbewusstsein in der Produktion in den letzten Jahren zugenommen hat, aus Security-Sicht jedoch Branchen wie die Finanz- oder Energiewirtschaft deutlich weiter sind. Am weitesten sind jene, vielfach großen Produktionsbetriebe, die ein sehr großes Verantwortungsbewusstsein in ihrer Tätigkeit haben, etwa in Bezug zur Wahrung von Intellectual Property oder KundInnendaten. Die empirischen Befunde auf Basis des EMS zeigen, dass es einen klaren positiven Zusammenhang zwischen dem Ausmaß der Nutzung von Industrie-4.0 Technologien (Industrie-4.0-Reifegrad) und dem Security-Bewusstsein einschließlich der eingesetzten Security-Maßnahmen (Security-Reifegrad) gibt. Des Weiteren zeigt sich im Allgemeinen, dass größere Betriebe, Unternehmen, die eine höhere Exportquote aufweisen und jene, die als Zulieferer tätig sind, vielfältigere Maßnahmen zur Erhöhung der Security einsetzen. Zugleich bedeutet dies, dass eine große Gruppe von Produktionsbetrieben dem Thema Security noch deutlich zu wenig Aufmerksamkeit schenkt.

Als Gründe für Sicherheitsrisiken gelten mangelndes Sicherheitsbewusstsein, ungenügende Sicherheitsvorsorge (z.B. Sicherheitslücken in Systemarchitekturen), erschwerter Schutz durch fehlende Standardisierung, unklare Kosten-Nutzen-Relationen bei Investitionen in die Sicherheit und die fehlende Akzeptanz von Cybersecurity-Lösungen seitens der Anwender

(z.B. aufgrund sinkender Benutzerfreundlichkeit). Aufgrund der wachsenden Komplexität der Angriffe und der Vernetzung ehemals getrennter Systeme können Sicherheitsanforderungen häufig nicht mehr durch einfache technische Ansätze erfüllt werden. Einzelne technische Werkzeuge, Prozesse, Organisationsstrukturen und Verhaltensmaßnahmen müssen daher übergreifend im gesamten System betrachtet werden. Technische Lösungen allein greifen zu kurz, umfassende Sicherheit ist nur erreichbar, wenn Technik und organisatorische Prozesse gemeinsam betrachtet werden. Wirksame Sicherheit ist daher auch nur mit Unterstützung des Managements möglich.

Als besonders groß wird der Bedarf für die Verbesserung der Security bei der Automatisierungstechnik gesehen, vor allem bei noch älteren Anlagen mit Steuerungs-systemen aus den 1980er- oder 1990er-Jahren, die nun im Zuge der Umsetzung von Industrie-4.0-Lösungen miteinander vernetzt werden. Security-Maßnahmen sind oft nicht inhärent in den Anlagen verankert, sondern werden nachträglich hinzugefügt, was kostenintensiv und komplex ist. Fehlende Best Practices sind eine weitere Barriere; im (industriellen) Security-Bereich sind eher individuelle, domänenspezifische Lösungen erforderlich. Ein möglicher Trend sind daher spezialisierte Angebote und Individuallösungen.

Insgesamt wird die Markttransparenz in Österreich als gering eingestuft und Unternehmen, die bzgl. Security noch am Anfang stehen, bekunden, dass die fehlende Klarheit über Sicherheitsmaßnahmen eine Barriere für die weitere Investition in Industrie 4.0 und vor allem die Vernetzung von Systemen ist. Derartige Unternehmen sind mitunter gar nicht in der Lage, die Anforderungen überhaupt zu definieren, um dann einen geeigneten Anbieter zu suchen.

Auf Basis der durchgeführten Analysen können folgende wichtige Empfehlungen für Industrieunternehmen abgeleitet werden:

- **Security als strategisches Thema positionieren**: Security muss auf Ebene der Geschäftsführung als strategisches Thema entwickelt und umgesetzt werden. Eingebettet in den strategischen Rahmen müssen Unternehmen den Kommunikations- und Schutzbedarf festlegen, Risikoanalysen durchführen und aktiv Lösungen bei den Anbietern von Industrie-4.0-Lösungen einfordern.

- **„Hausaufgaben" machen**: Industrieunternehmen und Anlagenbetreiber sollten auf Basis einer Risikoanalyse iindividueller Maßnahmen setzen und langfristige Konzepte entwickeln. Ein erster Schritt ist, innerhalb des Unternehmens die Assets samt ihrem Schutzbedarf zu identifizieren und entsprechende technische und organisatorische Sicherheitsmaßnahmen zu setzen. Erstes Ziel sollte sein, eine vernünftige Basis zu

schaffen, um sich vor einfachen Angriffen zu schützen. Freilich ist dies keine einmalige Aktion, sondern ein Prozess, der regelmäßig durchlaufen werden muss.

- **Interne und externe Kommunikation fördern**: Zur Reduktion von Sicherheitsrisiken ist die Kommunikation zwischen Führungskräften und MitarbeiterInnen im Allgemeinen sowie zwischen IT und OT (IT- und ProduktionsleiterIn) im Speziellen zu fördern. Was die Kommunikation bei Sicherheitsvorfällen betrifft, ist die Bereitschaft für proaktives Handeln und externe Kommunikation (z.B. bei Sicherheitsvorfällen) noch sehr gering. Unternehmen sollten verstärkt proaktiv im Rahmen der Vernetzung mit anderen Unternehmen über Vorfälle austauschen und voneinander lernen. Organisationen wie der Verein Industrie 4.0 können ebenfalls als Plattform für den Austausch sicherheitsrelevanter Informationen dienen.

- **Qualifizierung und Schulung vorantreiben**: Die Qualifizierung der MitarbeiterInnen, etwa in Kooperation mit spezifischen Anbietern, ist eine wichtige Strategie zur Erhöhung der Security. Nach wie vor gelten die MitarbeiterInnen als wichtigster Risikofaktor, zugleich steigt damit das Bewusstsein für Security.

Die Studie zeigt Handlungsbedarf für die Politik in vier Bereichen auf:

1. **Forschung und Entwicklung**
   Programme zur Förderung der Entwicklung von Security-Technologien und -Lösungen sollten ausgebaut bzw. in den unterschiedlichen Programmen der FFG (Produktion der Zukunft, IKT der Zukunft) verankert werden. Dabei besteht ein großer Bedarf bei der Förderung von kooperativen Projekten zwischen Akteuren aus den Bereichen Produktion und IT, etwa bei der Entwicklung von Automatisierungsanlagen.

2. **Aus- und Weiterbildung**
   Cybersecurity-Kompetenzen sind sowohl im Rahmen der klassischen IT-Lehrgänge zu verankern, als auch bei den Maschinenbau- und Automatisierungstechnik-Curricula an den Hochschulen, HTLs und Colleges. Die verstärkte Abdeckung von IT-Grundkenntnissen in der Primar- und Sekundarstufe kann als längerfristige Maßnahme verstanden werden. Ferner sollten weiterhin „Hacker-Events" in Österreich gefördert werden und spezifische Schulungsmaßnahmen wie Aus- und Weiterbildungsnetzwerke gefördert werden. Die Etablierung eines Digital Innovation Hubs (DIH) in Österreich wäre ebenso wichtig.

3. **Standardisierung und Zertifizierung**
   Maßnahmen zur Standardisierung und Zertifizierung schaffen einen klaren Rahmen und reduzieren die Unsicherheit bei der Entwicklung und dem Einsatz von Lösungen.

Wenngleich teilweise schon sehr umfangreiche und ausdifferenzierte Normen und Standards existieren, fehlen Best Practices und Leitfäden zur konkreten Nutzung bzw. Anwendung dieser Regelungen. Des Weiteren wird die Etablierung eines „European Trusted Hardware und Software"-Siegels empfohlen, damit europäische Akteure auf eigene, sicherheitsgeprüfte Produkte zurückgreifen können.

4. **Kommunikation und Bewusstseinsbildung**
   Die Bewusstseinsbildung ist ebenfalls ein wichtiges Thema. Der Aufbau von Wissensdatenbanken, in denen Sicherheitsvorfälle dokumentiert werden, die Etablierung eines österreichischen BSI, die Schaffung einer zentralen Anlaufstelle für KMU sowie die Herausgabe eines Leitfadens können hier genannt werden.

Abbildungsverzeichnis

Abbildung 1: Speicherung von Betriebsdaten nach Betriebsgrößen 7
Abbildung 2: Speicherung von Betriebsdaten und Industrie 4.0 Reifegrad 8
Abbildung 3: Bedrohungspotential von Cyberangriffen nach Betriebsgrößen 9
Abbildung 4: Bedrohungspotenzial von Cyberangriffen und Industrie-4.0-Reifegrad 10
Abbildung 5: Bedrohungspotenzial von Cyberangriffen und Exportanteil 11
Abbildung 6: Überprüfung von Sicherheitsmaßnahmen nach Betriebsgrößen 12
Abbildung 7: Reifegradmodell 13
Abbildung 8: Security-Reifegrad (0-12) nach Betriebsgröße, Einsatz von Industrie 4.0 Techniken (Industrie 4.0-Reifegrad), Exportanteil und Stellung in der Zulieferkette 14
Abbildung 9: Investitionen in Security 15
Abbildung 10: Einsatz von Security-Maßnahmen 16
Abbildung 11: Referenzarchitekturmodell RAMI 4.0 und Automatisierungspyramide 23

Literaturverzeichnis

Caralli, R. A., Allen, J. H., White, D. W. (2011): CERT resilience management model: A maturity model for managing operational resilience (CERT-RMM Version 1.1). Boston, MA: Addison-Wesley.

DOE and DHS (Department of Defence and Department of Homeland Security) (2014): Cybersecurity Capability Maturity Model Version 1.1,

Jung, O., Fenz, S., Kammerstetter, M., Hudic, A. (2016): Eine Architektur für sichere Smart Grids in Österreich, DACH Security 2016. syssec.

Institut für Technikfolgen-Abschätzung (ITA) der Österreichischen Akademie der Wissenschaften, AIT Austrian Institute of Technology (2015): Industrie 4.0 - Foresight & Technikfolgenabschätzung zur gesellschaftlichen Dimension der nächsten Revolution. Pilotstudie im Auftrag der Parlamentsdirektion. Wien, November 2015.

ISA (International Society of Automation) (2009): Industrial automation and control systems security: Establishing an industrial automation and control systems security program (ANSI/ISA-99.02.01-2009).

ISO (International Organization for Standardization) (2008). Systems Security Engineering – Capability Maturity Model (SSE-CMM) (ISO/IEC 21827:2008).

Langer, L., Skopik, F., Smith, P., Kammerstetter, M. (2016): From Old to New: Assessing Cybersecurity Risks for an Evolving Smart Grid, Computers & Security, 62 (2016), S. 165 - 175.

Lassnig, M., et al. (2017): Handlungsempfehlungen zur digitalen Transformation durch Industrie 4.0 und neue Geschäftsmodelle, Salzburg Research, Salzburg/Wien, Studie im Auftrag der FFG/BMVIT, 2017.

Leitner, K-H., Dachs, B., Degelsegger, A. et al. (2015): Stärkefelder im Innovationssystem: Wissenschaftliche Profilbildung und wirtschaftliche Synergien, Auftragsprojekt für das Bundesministerium für Wissenschaft, Forschung und Wirtschaft, Wien.

Leopold, H., Schwabach, C. Flachberger, C., Almer A, Klerx, J., Kasztler, A., Leitner, K-H. et al. (2014): Inno4Sec. Bedarfsträgerorientiertes Innovationskonzept für die Sicherheitsforschung, Projekt-Endbericht, Finanziert durch die FFG, Wien.

Paulk, M., Weber, C., Garcia, S., Chrissis, M.B., Bush, M. (1993): Key practices of the capability maturity model (Version 1.1, Technical Report CMU/SEI-93-TR-25). Software Engineering Institute, Carnegie Mellon University. http://www.sei.cmu.edu/reports/93tr025.pdf

Reischauer, G., Leitner, K-H. (2016): Innovation 4.0. Wie das Innovationspotenzial von Industrie 4.0 analysiert werden kann, Austrian Management Review, Vol. 6, S. 76-83.

Sommer, P., Brown, I. (2011). Reducing systemic cybersecurity risk. Organisation for Economic Co-operation and Development. http://www.oecd.org/dataoecd/57/44/46889922.pdf

Stouffer, K., Falco, J., Scarfone, K. (2011): Guide to industrial control systems (ICS) security (NIST Special Publication 800-82). National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

Verein Industrie 4.0 Österreich – die Plattform für intelligente Produktion (2018): Cyber-Security Leitfaden für Produktionsbetriebe. Schutz vor Cyberattacken – mehr Wertschöpfung mit Security, Juli, Wien.

Zahradnik, G., Rhomberg, W., Leitner, K-H. (2016): EMS 2015. Innovationen in der Produktion: Basisauswertung und Sonderauswertung zum Thema Industrie 4.0, AIT-IS-Report, Vol. 125, April, Wien.

ZVEI: Industrie 4.0: Das Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0), ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V., Frankfurt am Main.

Abkürzungen

AIT	AIT Austrian Institute of Technology GmbH
APT	Advanced Persistent Threats
BSI	Bundesamt für Sicherheit in der Informationstechnik
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CMDB	Configuration Management Database
COTS	Commercial off-the-shelf
CPS	Cyber Physical Systems
DDoS	Distributed-Denial-of-Service
DIH	Digital Innovation Hub
DoS	Denial of Service
DSVGO	Datenschutz-Grundverordnung
EMS	European Manufacturing Survey
ERP	Enterprise Resource Planning
F&E	Forschung und Entwicklung
FH	Fachhochschule
FPGA	Field Programmable Gate Array
FTI	Forschung, Technologie und Innovation
ggf.	gegebenenfalls

FFG	Forschungsförderungsgesellschaft
HTL	Höhere Technische Lehranstalt
HW	Hardware
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IKT	Informations- und Kommunikationstechnologien
IoT	Internet of Things
IPS	Intrusion Prevention System
IT	Information Technology
ISMS	Informationssicherheitsmanagementsystems
IPS	Intrusion Prevention System
ISO	International Standards Organization
KIRAS	Österreichisches Sicherheitsforschungsprogramm
KMU	Kleine und mittlere Unternehmen
MA	MitarbeiterInnen
MES	Manufacturing Execution System
MINT	Mathematik, Informatik, Naturwissenschaften, Technik
OT	Operational Technology
PLC	Programmable Logic Controllers

RAMI 4.0	Referenzarchitekturmodell Industrie 4.0
SCADA	Supervisory Control and Data Acquisition
SIGI	Sicherheit für die digitale Transformation der Produktion
SL-A	Security Level Achieved
SL-T	Security Level Target
TÜV	Technischer Überwachungsverein
USA	United States of America
vgl.	vergleiche
VPN	Virtual Private Network
WKÖ	Wirtschaftskammer Österreich
WLAN	Wireless Local Area Network
z.B.	zum Beispiel
z.T.	zum Teil
ZVEI	Zentralverbands Elektrotechnik- und Elektronikindustrie e. V.

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie, Radetzkystraße 2, 1030 Wien
Autorinnen und Autoren: Leitner Karl-Heinz, Langer Lucie, Jung Oliver, Kasztler Andrea, Zahradnik Georg
Wien, 2020 Stand: 24. März 2020

Die vorliegende Studie wurde im Projekt „SIGI – Sicherheit für die digitale Transformation der Produktion" vom Austrian Institute of Technology (AIT) erstellt. **Diese F&E-Dienstleistung ist im Auftrag des Bundesministeriums für Verkehr, Innovation und Technologie, BMK entstanden und mit Mitteln des Programms Produktion der Zukunft finanziert.** Die Programmabwicklung erfolgt durch die FFG. Nähere Informationen zum Programm finden Sie unter https://www.ffg.at/produktion-der-zukunft-das-foerderprogramm

Copyright und Haftung:
Auszugsweiser Abdruck ist nur mit Quellenangabe gestattet, alle sonstigen Rechte sind ohne schriftliche Zustimmung des Medieninhabers unzulässig.
Es wird darauf verwiesen, dass alle Angaben in dieser Publikation trotz sorgfältiger Bearbeitung ohne Gewähr erfolgen und eine Haftung des Bundesministeriums für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie und der Autorinnen und Autoren ausgeschlossen ist. Rechtausführungen stellen die unverbindliche Meinung der Autorinnen und Autoren dar und können der Rechtssprechung der unabhängigen Gerichte keinesfalls vorgreifen.

Rückmeldungen: Ihre Überlegungen zu vorliegender Publikation übermitteln Sie bitte an i5@bmk.gv.at.

Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
Radetzkystraße 2, 1030 Wien
+43-1-71162-653500
i5@bmk.gv.at
bmk.gv.at