Sicherheitswelten wachsen zusammen

Herausforderung für Organisationen durch Industrie 4.0

Christian Jacobs, qSkills GmbH & Co. KG, Michael Krammel, KORAMIS GmbH

Es mag paradox scheinen: In Zeiten von Industrie 4.0 und Maschine-zu-Maschine-Kommunikation rückt mehr denn je der Mensch in den Mittelpunkt. Die Qualifikation der Mitarbeiter entwickelt sich zum bestimmenden „kritischen Pfad“ [1,2]. Die zunehmende Komplexität der Produktion erfordert vom gering Qualifizierten bis hin zum Manager einen umfassenden Einblick in betriebliche und überbetriebliche Strukturen.

Durch die Vernetzung von Anlagenherstellern, Integratoren und Betreibern unter massivem Einsatz von IT und Big Data entsteht ein neuer, prozess- und unternehmensübergreifender Know-how-Bedarf sowohl in der Planung, in der Produktion, im Personalwesen und in der Beschaffung. Eine besondere Rolle spielt hier das Thema „Industrial Continuity Management“, also die Sicherung des Regelbetriebs von Industrieunternehmen unter Berücksichtigung von Unternehmensprozessen, Business Continuity Management und Security.

Besonders sensibel ist dabei das Thema „Security“. Dazu zählen unter anderem Cyber-Security, ICS-Security, Embedded- und Industrial-Security. Immer mehr Unternehmen sehen sich bei der Einführung von Industrie 4.0 mit einem akuten Handlungsbedarf zur Abwehr von Cyber-Bedrohungen in der Fabrikautomation und Prozesssteuerung, zum Beispiel von Industrial Control Systems (ICS), konfrontiert. Entsprechende Qualifikationen und organisatorische Strukturen müssen in den Unternehmen häufig erst noch aufgebaut werden [3].

Sicherheitswelten wachsen zusammen

Das Zusammenwachsen von Produktion und IT und die daraus resultierende steigende Anzahl an Zugangsmöglichkeiten und Schnittstellen vergrößern die Angriffsfläche und somit auch das Gefährdungspotenzial. Die wohlbekannten Sicherheitslösungen in der Office-IT sind jedoch nicht eins zu eins auf die Produktions-IT übertragbar. Die produktionsnahe IT kann zwar von den Erfahrungen der Office-IT lernen und Fehlentwicklungen vermeiden, die umzusetzenden Lösungen müssen jedoch auf Verträglichkeit mit den Rahmenbedingungen der Produktion geprüft und entsprechend angepasst werden.

So entstehen an der Schnittstelle zwischen Produktion, IT und Security neue Anforderungen an das Know-how und es werden neue Rollen und Tätigkeitsprofile benötigt. Das betrifft sowohl Produktionsmitarbeiter, die über ein Grundverständnis für IT-Sicherheit verfügen sollten, aber auch Experten wie etwa Chief Information Security Officer, die ihr Know-how-Spektrum um Produktionsaspekte erweitern müssen. Das Management sollte zumindest in der Lage sein, den Stellenwert des Themas Security im Rahmen der Industrie 4.0 einschätzen zu können.

Gefragt ist dabei übergreifendes Know-how, besonders in den Bereichen Big Data, Industrial-IT und Security, Systems-Integration, Automation und Production-Technology, verbunden mit Denken in Systemen und interdisziplinären Zusammenhängen, um verantwortliche Entscheidungen treffen zu können.

Unterschiedliche Denkwelten treffen sich

Der Begriff „Sicherheit“ besitzt im Umfeld der Industrial-IT bekanntlich zwei Dimensionen: Safety und Security. Während Safety traditionell im Produktions- und Ingenieursbereich verwurzelt ist, kommt mit IT-Security eine Begrifflichkeit mit anderen Anforderungen aus einer scheinbar fernen Denkwelt hinzu. Aus Kosten- und Flexibilitätsgründen wird bei Industrie 4.0 eine Verschmelzung von Büro- und

Christian Jacobs

Christian Jacobs ist seit 2014 Mitglied der Geschäftsleitung der qSkills GmbH & Co. KG, verantwortet die strategische Ausrichtung des Produktportfolios und ist für die internationalen Partnerschaften zuständig. Vorher war er mehrere Jahre in den USA für einen IT-Service Provider für Banking und Retail tätig. qSkills ist ein unabhängiges Schulungs- und Trainingsunternehmen für die Themen IT-Management und IT-Security und hat 2015 eine eigene Industrie 4.0 IT-Akademie initiiert.

Kontakt
Christian.Jacobs@qskills.de
Tel.: +49 911 801030
www.qskills.de

Anlagen-IT vorangetrieben. Das provoziert Situationen, die sowohl unter Aspekten der Security als auch der Safety kritisch sein können: Security-Lücken können zu Gefährdungen im Sinne der Safety führen und umgekehrt. Ein gegenseitiges Verständnis dieser Denkwelten ist in der Praxis also von entscheidender Bedeutung und ein wesentliches Qualifikationsmerkmal.

Auch die kontinuierliche IT-Sicherheitsüberwachung von Anlagen und Systemen erfordert ein übergreifendes, über die jeweiligen Sicherheitsdefinitionen hinausgehendes Verständnis und Know-how der Mitarbeiter. Ein Beispiel: Wurden in der Produktion zuvor Patches und Updates (wenn überhaupt) ausschließlich während definierter Wartungsfenster manuell eingespielt, so kann dies künftig – wenn Produktions-IT und Office-IT eng verbunden sind – zu erheblichen Sicherheits-Problemen führen. Hier muss es einerseits entsprechende Lösungen und auch Handlungsanweisungen für Mitarbeiter geben, andererseits ist es auch nötig, organisatorisch die Weichen entsprechend zu stellen.

Spezialisten, die in der Lage sind, Industrie-4.0-Infrastruktur sicher zu entwickeln, aufzusetzen und zu managen, sind auf dem Arbeitsmarkt derzeit kaum zu finden. Die Anforderungen sind vielfältig: Sie haben über IT, IT-Sicherheits-, Ingenieurs- und Managementkenntnisse sowie Soft Skills zu verfügen, wie sie in dieser Form und Konstellation bislang noch nicht ausgebildet werden. Nicht zuletzt deshalb fordert der Bundesverband IT-Sicherheit – TeleTrusT – daher auch eine Anpassung und Neuordnung der Ingenieursausbildung in Deutschland [4].

Spezialisten, die in der Lage sind, Industrie-4.0-Infrastruktur sicher zu entwickeln, aufzusetzen und zu managen, sind auf dem Arbeitsmarkt derzeit kaum zu finden.

Umfassende und integrierte Ausbildungen zum Beispiel zum Big Data Scientist, die auch das Thema Security angemessen berücksichtigen, haben in Deutschland Seltenheitswert.

Im Spannungsfeld von Organisation und Produktion – Das Beispiel „CISO"

„Industrie 4.0" wird erhebliche Auswirkungen auf die organisatorische Ein- und Anbindung des CISO (Chief Information Security Officer) und damit auch auf die Qualifikationsanforderungen an diese Position haben [5]. Entscheidende Fragen sind: Wer verantwortet das Thema Security in der Produktion? Wird es neben dem CISO dafür eine gleichberechtigte Position geben?

Wie genau das im Detail gestaltbar und operativ umsetzbar sein wird, ist derzeit noch kaum einzuschätzen. In Gespräch beziehungsweise in der Erprobung sind verschiedene unterschiedliche Organisationsmodelle, die derzeit konträr diskutiert werden und über die letztendlich das Management oder der Vorstand aus unternehmenspolitischer Sicht heraus zu entscheiden hat.

Die künftige Qualifikation des CISO ist jedenfalls stark von der Wahl des Organisationsmodells abhängig: Soll der CISO auch die Security in der Produktion mitverantworten, so benötigt er zusätzliche Kenntnisse, um die Belange der Produktion angemessen zu berücksichtigen und zu bewerten.

Über die Fachkenntnisse hinaus sind zunehmend Soft Skills wie Kommunikations- und Vermittlungsfähigkeit sowie Konfliktmanagement gefragt – der CISO muss Akzeptanz in der Produktion erlangen, vermitteln und alle Beteiligten „ins Boot holen" können. Dazu zählt auch, mit den Ängsten von Mitarbeitern um ihren Arbeitsplatz angesichts der Beschäftigungsdynamik von Industrie 4.0 angemessen umgehen zu können und ihnen im Zukunftsbild Industrie 4.0 ihren Platz aufzuzeigen.

Entscheidende Voraussetzung ist jedoch die eindeutige Definition seiner Rolle – soll er auch die Verantwortung der Security in der Produktion mitverantworten, so muss der CISO womöglich Verantwortung gegenüber Management, Business-IT und Produktion tragen. Dafür ist es erforderlich, eine ganzheitliche Managerrolle aus der „Vogelperspektive" einzunehmen. Für die inhaltliche Ausgestaltung

einschlägiger Berufszertifikate wird das künftig voraussichtlich eine Aufnahme von zusätzlichem Produktions-Know-how, einschlägigen Normen und Standards im Produktionsbereich sowie Soft Skills und Management-Know-how bedeuten.

Grundlegende organisatorische Überlegungen und Ansätze

Insbesondere Großunternehmen haben inzwischen auf sehr unterschiedliche Art und Weise begonnen, das Thema Industrial-Security in ihre Organisationen einzubinden. Hierbei lassen sich stark zentralisierte oder dezentralisierte Strukturen unterscheiden.

Hinsichtlich eines strukturellen Organisationsaufbaus ist es eine Möglichkeit, das Thema Industrial-Security von der IT verantworten zu lassen, die somit auch an die Produktion angepasste Richtlinien verfasst (Richtlinien-Kompetenz). Zum anderen gibt es aber auch Varianten, in denen Unternehmen die Industrial-Security unabhängig von der Office-IT autark der Produktion zugeordnet haben und diese somit eigenverantwortlich bleibt – dazu wird dann ein eigener Informations-Sicherheits-Beauftragter/Officer „Produktion“ (ISO-Prod) eingesetzt.

Variante 1:
Ein zentraler CISO verantwortet hierbei sowohl die Office- als auch die Produktions-IT und gibt von der Zentrale aus Prozesse und Richtlinien für beide Bereiche vor. Für die Umsetzung schaffen die einzelnen Niederlassungen/Werke dann in der Regel unterschiedliche Rollen für beide Bereiche. Die lokalen Rollen lassen sich je nach Größe der Niederlassung beziehungsweise des Werks unterschiedlich gestalten – alle Berichtswege laufen jedoch bei dem einen zentralen CISO zusammen.

Variante 2:
Diese Variante basiert ebenfalls auf einem zentralen CISO. Im Unterschied zu Variante 1 wird die Produktions- und Office-IT möglichst lange zusammenhängend beziehungsweise „linear“ verantwortet. Hierbei greift dann ein lokaler ISO (Informations-Sicherheits-Officer) für dedizierte Security-Themen im Rahmen der Produktion auf lokale Industrial-Security-Experten zurück.

Hinsichtlich eines strukturellen Organisationsaufbaus ist es eine Möglichkeit, das Thema Industrial-Security von der IT verantworten zu lassen, die somit auch an die Produktion angepasste Richtlinien verfasst (Richtlinien-Kompetenz).

Variante 3:
Eine dritte Variante trennt die beiden IT-Linien für Office und Produktion strikt und lässt deren Berichtswege erst im zentralen Management zusammenlaufen. Unabhängig von der konkreten Umsetzungsform ist jedoch immer eine abgestimmte Zusammenarbeit zwischen Produktions- und Office-IT zu entwickeln, um von den Erfahrungen und Fehlentwicklungen der Vergangenheit lernen zu können.

Security Strategist

Darüber hinaus ist zurzeit insbesondere bei Großunternehmen und Konzernen die Rolle eines „Security Strategist“ in der Diskussion. Getragen ist dies von der Erfahrung, dass ein klassischer CISO nur eingeschränkte Möglichkeit zu einer gesamtheitlichen Betrachtung hat beziehungsweise in der Regel nur beschränkt über ausreichende Budgetverantwortung verfügt.

Aufgabe des Security Strategist ist die strategische Ausrichtung der Security und die ganzheitliche Betrachtung von Sicherheitsaspekten unter Einbeziehung sowohl der Wertschöpfungsketten als auch von Beschaffung und HR. Der Security Strategist ist direkt dem Vorstand unterstellt und hat Budgetverantwortung, um Security Strategien im Unternehmen auch wirkungsvoll umsetzen zu können.

Schulungen und Qualifizierung rund um das Thema Security

Es ist davon auszugehen, dass die Berufsausbildung angepasst wird und erforderliche Security-Aspekte sukzessive Eingang in die Ausbildung

Grundsätzlich eignen sich für Industrial-Security sowohl Mitarbeiter aus dem Bereich „IT“ als auch aus dem Bereich „Produktion“. Neben Produktions- und Security-Kenntnissen sind auch vertiefende IT-Kenntnisse für die Rolle des Industrial-Security-Experten notwendig.

Michael Krammel

Michael Krammel ist seit 2009 Geschäftsführer der KORAMIS GmbH und hat dort die Geschäftsfelder Industrial Automation und seit 2005 Industria-Security aufgebaut. Er ist Mitglied in der Industrie 4.0 Plattform (Sichere Systeme) sowie in weiteren relevanten Gremien und Fachausschüssen und verfügt über mehr als 25 Jahren Erfahrung in der Automatisierung, Netzleit-und Prozessleittechnik. Schwerpunkt ist Industrial-Security.

Kontakt
m.krammel@koramis.de
Tel.: +49 681 9681910
www.koramis.de

erhalten, ohne dass zwingend vollkommen neue Berufsbilder entstehen.

Während die Ausbildung mittel- und langfristig die Basis für eine adäquate Qualifikation sicherstellen sollte, kann schon jetzt eine geeignete Weiterbildung akuten Qualifizierungsbedarf kurzfristig abdecken, um Industrie 4.0 jetzt in die Praxis einführen zu können. Der Qualifizierungsbedarf ist beträchtlich. Und es sind in der Regel Großunternehmen und Konzerne, die derzeit die entsprechenden Maßstäbe und Impulse setzen. Generell lassen sich einige wesentliche Anforderungen an Qualifizierungsmaßnahmen formulieren:

- So ist es sinnvoll, kompakte und gegebenenfalls zertifizierbare Schulungsinhalte zu entwickeln. Dies führt zu einer Nachvollziehbarkeit der Qualifikation und macht eine Zusatzausbildung für die Mitarbeiter wertvoller. Schulungen sollten interdisziplinär angelegt sein und kreativ die Brücken zu unterschiedlichen Fachdisziplinen schlagen.

- Die relevanten Lerninhalte im Bereich IT- und Industrial-Security lassen sich heute nur eher allgemein beschreiben, ebenso wie die passende Organisation der Verantwortlichkeit von Industrial-Security im Unternehmen. Ins Detail gehende Studien liegen gegenwärtig noch nicht vor.

- Die Vielfalt der möglichen Technik- und Themengebiete sowie Herangehensweisen und Vorkenntnisse der einzelnen Teilnehmer sind bei der Entwicklung von standardisierten Weiterbildungspfaden zu berücksichtigen. Eine große Bedeutung kommt daher dem Dialog mit der produzierenden Industrie zu, um die Anforderungen an Weiterbildung und Organisation aufzunehmen und modulare Schulungskonzepte entwickeln zu können.

Relevante Zielgruppen

Als Zielgruppe für das Thema Industrial-Security kommt ein breiter Adressatenkreis sowohl in der Unternehmensleitung als auch auf den operativen Ebenen infrage.

Seitens der Betreiber der Wertschöpfungskette, Integrator und Hersteller – lassen sich drei Hauptgruppen definieren: das Management, Industrial-Security-Experten sowie involvierte Mitarbeiter neben Externen. In der letzten Gruppe sind vor allem Awareness-Schulungen gefragt. Innerhalb der Experten-Zielgruppe ist ein differenziertes Niveau an Vorkenntnissen und Erfahrungswerten zu erwarten. Mit dem Thema Industrial-Security betrauen Unternehmen, je nach Größe und Struktur, Mitarbeiter unterschiedlichster Abteilungen und Erfahrungswelten. Deren unspezifische Vorkenntnisse gilt es bei der zielgruppengerechten Ansprache der Mitarbeiter in Schulungen sorgsam zu berücksichtigen.

Grundsätzlich eignen sich für Industrial-Security sowohl Mitarbeiter aus dem Bereich „IT“ als auch aus dem Bereich „Produktion“. Neben Produktions- und Security-Kenntnissen sind auch vertiefende IT-Kenntnisse für die Rolle des Industrial-Security-Experten notwendig.

Während zum Beispiel für Anlagenbediener spezifische Sensibilisierungsmaßnahmen in der Regel ausreichen, müssen andere Zielgruppen ausführlicher geschult werden. Dies betrifft insbesondere die Mitarbeiter, die für Planung, Entwicklung, Integration beziehungsweise Errichtung, Betrieb und Wartung verantwortlich und darin maßgeblich involviert sind und somit Cyber-Sicherheit an dieser Stelle aktiv mitgestalten.

Auch Management- oder Produktionsverantwortliche sollten in einem angemessenen Umfang qualifiziert werden, der über typische Sensibilisierung hinausgeht [6,7].

Das BSI Bundesamt für Sicherheit in der Informationstechnik) unterscheidet im Wesentlichen zwei Hauptzielgruppen für Schulungen:

1. Management und Produktionsverantwortliche
2. Mitarbeiter mit Verantwortung und/oder Einflussmöglichkeiten auf Cyber-Sicherheit eines ICS.

Management

Zum Management werden Produktionsverantwortliche, Management (C-Level) und gegebenenfalls Mitarbeiter mit operativem Bezug zu Security gezählt. Für diese Gruppe ist eine Einstiegsveranstaltung geeignet.

Hauptziele einer etwa eintägigen Schulung sind das Aufzeigen der Bedrohungslage, Verdeutlichung des Handlungsbedarfs, Vermittlung eines grundlegenden Verständnisses von elementaren Begrifflichkeiten und systematischen Ansätzen. Es sollen Kenntnisse der wichtigsten organisatorischen und technischen Maßnahmen auf abstraktem Niveau sowie die Schaffung der Voraussetzungen vermittelt werden, um Projekte und Maßnahmen anzustoßen und diese auf Management-Ebene nachvollziehen zu können.

Produktionsverantwortliche

Zu der Zielgruppe zählen unter anderen Produktions-CISO, Ingenieure, Infrastruktur-Betriebspersonal, Wartungstechniker, Instandhalter – also die Mitarbeiter, die einen technischen Hintergrund in ICS haben und mit der Planung, der Entwicklung, Integration/Errichtung, Betrieb oder der Instandhaltung betraut sind. Der Umfang wird mit drei bis fünf Tagen veranschlagt.

Ziele sind unter anderem die Vermittlung eines grundlegenden Verständnisses der relevanten Begrifflichkeiten, Technologien und Elemente der IT beziehungsweise IT-Sicherheit. Weiterhin geht es darum, ein fundiertes Verständnis der Bedrohungslage zur Bewertung der eigenen Gefährdungslage und die Grundsätze eines ISMS (Information Security Management System) und vertiefende Kenntnisse von organisatorischen und technischen Maßnahmen zu vermitteln. Konkrete Ansatzpunkte für die Umsetzung im operativen Betrieb beziehungsweise bei der Planung neuer Anlagen oder bei der Leitung von Sicherheitsprojekten (gegebenenfalls mit externer Beauftragung) sind weitere Lernziele für Produktionsverantwortliche.

Anspruch an diese Qualifikationsmaßnahme ist es, den Teilnehmern wesentliche Einblicke in die Möglichkeiten von Industrie 4.0 zu gewähren und ihnen die Fähigkeit zu verleihen, Gesamtkonzepte bewerten zu können.

© istockphoto | 50600840 | venimo

Letztendlich wird der Schulungsbedarf in Folge von Industrie 4.0 erheblich steigen. Neben zusätzlichem Fachwissen sind vor allem „weiche“ Qualifikationen wie etwa Kooperations- und Kommunikationsfähigkeit gefragt. Interdisziplinarität, die Fähigkeit zur Zusammenarbeit sowie ein gemeinsames Begriffsverständnis sind wesentliche Anforderungen. ■

Kurz und bündig

Die Qualifikation der Mitarbeiter entwickelt sich bei Industrie 4.0 zu einem wichtigen Faktor. Die zunehmende Komplexität der industriellen Produktion erfordert vom gering Qualifizierten bis hin zum Manager einen umfassenden Einblick in die betrieblichen und überbetrieblichen Strukturen. Besonders sensibel ist dabei das Thema „Security“. Dabei geht es nicht zuletzt um die Abwehr von Cyber-Bedrohungen in der Fabrikautomation und Prozesssteuerung. Entsprechende Qualifikationen und organisatorische Strukturen müssen in den Unternehmen häufig erst noch aufgebaut werden. Es ist davon auszugehen, dass die Berufsausbildung angepasst werden muss und erforderliche Security-Aspekte sukzessive Eingang in die Ausbildung erhalten. Schon jetzt könnte eine geeignete Weiterbildung akuten Qualifizierungsbedarf kurzfristig abdecken, um Industrie 4.0 in die Praxis einführen zu können.

Die Literaturangaben finden Sie unter folgendem Link:
http://bit.ly/23IM2Xb