OVE AKTUELL – Informationstechnik

„Cyber Security“

April 2020

Sehr geehrte Damen und Herren!

Nach einer gefühlten Ewigkeit im COVID-19-bedingten Homeoffice findet Sie unser **Newsletter OVE AKTUELL**, diesmal mit dem Schwerpunkt **„Cyber Security“**, hoffentlich in bester Gesundheit. Auch diesmal bieten wir Ihnen gerne wieder eine interessante Lektüre, die Abwechslung zu den täglich neuen Zahlen und Fakten rund um die COVID-Pandemie bringen kann.

An dieser Stelle finden Sie normalerweise einen **Hinweis zum Veranstaltungsangebot des OVE**, aber mit **COVID-19** ist alles anders: Die in bewährter Form abgehaltenen Weiterbildungsangebote und Veranstaltungen des OVE sind derzeit nach wie vor ausgesetzt, allerdings gibt es **einige der Seminare aktuell als Online-Version!** Die Mitarbeiter/innen der OVE Academy arbeiten bereits mit vollem Engagement an Ersatzterminen für entfallene Veranstaltungen. Im Herbst sind Seminare und Workshops dann hoffentlich auch wieder in gewohnter Form möglich. Details dazu finden Sie hier.

Herzlichen Dank für Ihr Verständnis und bleiben Sie gesund!

Weitere Neuigkeiten aus dem OVE finden Sie am Ende dieses Newsletters.

Cyber Security

Informationssicherheitsmanagement in der Industrie

Liebe Leserinnen, liebe Leser,

im Herbst vorigen Jahres, inzwischen fast schon wieder vor einem halben Jahr, trafen wir uns im Haus der Ingenieure, um den aktuellen Stand der Entwicklung der IEC 62443 zu diskutieren. Wer hätte damals gedacht, dass solche Veranstaltungen bald zumindest für eine gewisse Zeit nicht möglich sein würden? Die über 70 Teilnehmer/innen der Veranstaltung bekamen einen breiten Überblick über die aktuellen Herausforderungen und Lösungsansätze für die Steigerung der Sicherheit ihrer industriellen Anlagen gegenüber Cyber-Angriffen. Nachdem es seitdem noch keinen Newsletter der AG Cyber Security gab, möchte ich hier die Gelegenheit nutzen und die Vorträge für diejenigen, die nicht dabei sein konnten, Revue passieren lassen.

Zuerst durfte ich selbst als Vorsitzender der Arbeitsgruppe einen Überblick über den aktuellen Stand der Entwicklungen der IEC 62443-Serie geben. Danach berichteten Ernst Schober und Mario Vukovic von der OMV Refining & Marketing GmbH über ihre Erfahrungen bei der Umsetzung der Standards in der OMV zur Absicherung der betriebenen Industrieanlagen. Dabei wurde deutlich, wie durch das Zurückgreifen auf Standards wie die IEC 62443 die Anforderungen in solchen komplexen Umgebungen effizienter umgesetzt werden können. Danach berichtete Daniel Siegl von LieberLieber Software GmbH über die von seinem Unternehmen entwickelten Technologien, um mittels modellbasierter Technologien einfache Systeme nach den Anforderungen der IEC 62443 planen und umsetzen zu können. Markus Hirsch von Fortinet fokussierte seinen Vortrag auf die Aufteilung von OT-Netzwerken in unterschiedliche Zonen und darauf, welche Mechanismen moderne Firewalls in diesem Bereich bieten können, wie z. B. die detaillierte Analyse von Industrieprotokollen. Als Hersteller von Produkten für die industrielle Automatisierung hat Phoenix Contact einen breiten Kundenkreis, der die Anforderungen der IEC 62443 umsetzen möchte. Dementsprechend hat das Unternehmen vor kurzem die Zertifizierung seiner Produktentwicklungsprozesse nach IEC 62443-4-1 abgeschlossen und auch weitere Zertifizierungen für Dienstleistungen durchgeführt. Erich Kronfuss berichtete über die Erfahrungen des Unternehmens im Zertifizierungsprozess. Zum Abschluss stellte Willibald Krenn ein vom AIT entwickeltes Tool namens ThreatGet vor, das Unternehmen bei der Durchführung von den in der IEC 62443 geforderten Risk Assessments unterstützt.

Auch für heuer planen wir wieder eine ähnliche Veranstaltung im Herbst und hoffen, dass bis dorthin die Durchführung auch schon wieder möglich sein wird – Details dazu werden noch folgen. Die Arbeit an der IEC 62443 geht aber natürlich trotz der aktuellen Schwierigkeiten weiter – so wurde unter anderem der Teil 62443-2-1 der Norm in den letzten Monaten massiv überarbeitet und soll in Zukunft den Titel „Security program requirements for IACS asset owners“ tragen. Die neue Version soll dabei noch mehr als bisher ergänzend zu einem im Unternehmen etablierten ISMS (Informationsicherheits-Managementsystem) die wesentlichen Aspekte für OT-Umgebungen (z. B. Automatisierungsysteme) hervorstreichen. Damit sollen für Unternehmen zusätzliche Hilfestellungen für diesen Bereich geliefert und die notwendigen Ergänzungen zu „klassischen“ ISMS-Normen wie der ISO 27001 beschrieben werden. Für den ersten Draft wurden über 500 Kommentare eingereicht, diese werden aktuell diskutiert und eingearbeitet – deshalb wird es wohl auch noch ein bisschen dauern, bis diese neue Version veröffentlicht werden kann. Trotzdem ist natürlich das Thema ISMS auch für industrielle Umgebungen aktuell schon relevant, und die zwei Artikel in diesem Newsletter beschäftigen sich deshalb damit, welchen Beitrag ein ISMS in industriellen Umgebungen zur Steigerung der Resilienz gegenüber Cyber-Angriffen, aber auch Ausfällen im Allgemeinen, liefern kann. Für die Beiträge darf ich mich bei den Autoren wieder herzlich bedanken – und natürlich auch wieder alle Leser/innen dazu einladen, ihre Erfahrungen, Ideen und Meinungen in künftigen Beiträgen vorzustellen.

Dipl.-Ing. Thomas Bleier, MSc
OVE-GIT Arbeitsgruppenleiter „Cyber Security“
OVE-OEK Vorsitzender der AG MR 65 Industrial Automation & Control System Security
Geschäftsführer B-SEC better secure KG
t@b-sec.net

ISMS im industriellen Umfeld

„Eine gut laufende Sicherheitsabteilung wird acht Personen benötigen“, sagte ich zu dem von der Familienstiftung ausgewählten Nachfolger im CEO-Sessel im Jahr 2016. „Gut, wir fangen mal mit Ihnen an und Sie bekommen einen dazu“, war die Antwort. Schneller Vorlauf nach 2020: Das Unternehmen beschäftigt in der Sicherheitsabteilung bereits fünf Personen – Tendenz steigend – und ist sich voll im Klaren darüber, dass die Abteilung weiter wachsen wird müssen, schon allein auf Grund der Herausforderungen, die Aspekte wie Predictive Maintenance und die verstärkte Anbindung von OT- und SCADA-Systemen an eine TCP/IP-basierte Infrastruktur mit sich bringen.

Leider zeigt auch die aktuelle Corona-Krise, dass insbesondere kriminelle Gruppen keinerlei Pardon kennen, wenn es darum geht, aus den Schwächen einer IT-Infrastruktur oder strukturellen Prozessschwächen eines Unternehmens Kapital zu schlagen. Zugegebenermaßen betrifft das rein online-basierte Dienste wie Banken, Online Gaming, Lieferdienste aller Art etc. grundsätzlich stärker als Industriebetriebe. Je nach Abhängigkeitsgrad von der eigenen IT, von Dienstleistern sowie Stabilität des Geschäftsmodells und offenen Schnittstellen nach außen sind aber Industriebetriebe Risiken desselben Schweregrades ausgesetzt. Die Qualität des ISMS entscheidet dabei über Wohl und Wehe und darüber, ob alle Einfallstore in das Unternehmen so ausreichend und risiko-basiert gesichert sind, dass entweder ein Eindringen nicht möglich ist oder ausreichend schnell Gegenmaßnahmen gesetzt werden können. Selbst das nunmehr besonders in den Vordergrund gerückte Thema Business Continuity ist etwas, das mittels ISMS sehr umfassend und schlagkräftig betrachtet werden kann. Betriebe, die dieses Thema bereits vor Jahren ernst genommen haben, stehen jetzt auch deutlich besser da, als solche, die das nicht getan haben.

Wichtig in einem ISMS für Industriebetriebe sind ein funktionsübergreifender Zugang zu dem Thema sowie ein strikt risiko-basierter Ansatz, denn nicht jedem Hype, den ein Sicherheitsunternehmen so „dahinplappert“, muss man tatsächlich nachlaufen. Eine gut durchdachte Risikoanalyse spart auf mittlere und lange Sicht mehr Kosten und schlaflose Nächte (vor allem für den CISO/CSO), als das jedes noch so gehypte Tool könnte. Weiters sind gute KPIs notwendig, um die Wirksamkeit des ISMS kurz- und mittelfristig messen zu können, sodass strukturelle Probleme rasch erkannt werden können und diesen gegengesteuert werden kann. Abgerundet wird ein industrielles ISMS durch Trainings- und Schulungsmaßnahmen, die den Mitarbeitern in positiver und Verbesserung fördernder Weise vermittelt werden, sodass das dritte Einfallstor in ein Unternehmen, der Mensch, genauso resistent werden kann wie die beiden anderen Sphären der physischen und der IT-Sicherheit.

Über den Autor

Michael Krausz unterstützt seit dem Jahr 2001 Betriebe bei der Einführung von ISMS und Compliance Managementsystemen. Er war bisher in 29 Ländern auf vier Kontinenten für heimische und internationale Kunden tätig. Krausz ist CISO/DPO-as-a-service für namhafte in- und ausländische Industrieunternehmen.

Michael Krausz
Founder and Group CEO & CCO
i.s.c. – information security consulting eU

inquiries@i-s-c.co.at, T: +43 (1) 253 1000, www.i-s-c.co.at

Informationssicherheitsmanagement als wesentlicher Beitrag der IACS/OT-Betriebssicherheit

Die aktuellen Ereignisse rund um die SARS-CoV-2-Krise zeigen uns allen, wie wichtig der aufrechte Betrieb von (kritischen) Infrastrukturen ist. Es ist für uns selbstverständlich, dass in Krisenzeiten die Versorgung mit Strom oder Lebensmitteln genauso aufrechterhalten wird wie der Betrieb von Krankenhäusern oder die Produktion von medizinischen Gütern. Aber auch für die produzierende Industrie ist es erforderlich, dass Produktionsprozesse möglichst keine Unterbrechungen erfahren. Was hat dies mit Informationssicherheitsmanagement zu tun?

Informationssicherheitsmanagement (ISM) liefert einen wesentlichen Beitrag für den sicheren (Safety & Security) Betrieb von IACS/OT-Anlagen. Im Wirkungsbereich des ISM werden u. a. die folgenden Schutzziele mit technischen und organisatorischen (Schutz-)Maßnahmen adressiert:

- Verfügbarkeit
  z. B. Vorsorge gegen Pandemie, Schutz vor Cyber-Angriffen (z. B. Cyber-Erpressung, Wirtschaftskrieg im Cyber-Raum, Ransomware) – respektive Schutz vor IT/OT-Ausfällen
- Integrität
  Verhinderung von Verfälschung von Daten, z. B. Kundendaten, IT/OT-Systemkonfigurationen
- Vertraulichkeit
  z. B. Schutz von Know-how, Datenschutz

Hatten Sie schon bei dem einen oder anderen Schutzziel Probleme in Ihrem Unternehmen? Der Gesetzgeber sieht jedenfalls die Herausforderungen für die Gesellschaft. Um die Versorgungssicherheit zu gewährleisten, wurden das NIS-G und ergänzende Verordnungen in Kraft gesetzt. Im Wesentlichen geht es darum, unsere (kritische) Infrastruktur vor den Auswirkungen von Cyber-Angriffen zu schützen – z. B. ein Blackout zu verhindern. Um diese Ziele zu erreichen, wird vom Gesetzgeber vorgeschrieben, dass die betroffenen Unternehmen Schutzmaßnahmen für den sicheren IT/IACS/OT-Betrieb etablieren und deren Wirksamkeit über regelmäßige Überprüfungen nachweisen müssen.

Für die strukturierte Behandlung dieser Aufgabenstellung bietet es sich an, ein Informationssicherheits-Managementsystem (ISMS) zu etablieren. Hierzu gibt es eine Vielzahl von Best Practices und Standards. Der in Europa mit dem größten Verbreitungsgrad etablierte Standard hierzu ist die ISO/IEC 27001. Für Sicherheit in IACS/OT-Umgebungen wurde die IEC 62443-Normenfamilie entwickelt. Behandelt die ISO/IEC 27001 im Wesentlichen die Herausforderungen der IT, zielt die IEC 62443 spezifisch auf die Anforderungen in IACS/OT-Umgebungen ab. Die Standards sind auf Managementsystemebene umfänglich kompatibel und bieten so die Möglichkeit der Bildung eines durchgängigen Sicherheitsmanagements.

Ein wesentlicher Bestandteil bzw. der Kernprozess eines ISMS ist das Informationssicherheits-Risikomanagement. Dies ermöglicht, strukturierte Verbesserungspotentiale im Betrieb der IACS/OT-Infrastruktur aufzuzeigen. Eine österreichische Lösung, die bei über 50 % der in Österreich ISO 27001-zertifizierten Unternehmen im Einsatz ist, ist das Risikomanagement-Tool CRISAM®. Dieses liefert auch einen wesentlichen Beitrag zur Erfüllung gesetzlicher Anforderungen, wie z. B. jener, eine risikobasierte Unternehmenssteuerung zu etablieren.

Zusammenfassend gesagt: Österreichs Unternehmen stehen vor großen Herausforderungen im sicheren IACS/OT-Betrieb, diese können jedoch mit Hilfe eines strukturierten Informationssicherheits-managements nachhaltig bewältigt werden.

Dipl.-Ing. Harald Montenegro, MSc
Senior Consultant & Business Development
CALPANA business consulting GmbH

harald.montenegro@calpana.com, T: +43 (664) 88 10 92 21, www.crisam.net

Aktuelles aus dem OVE

Covid-19: Der OVE bleibt auch weiterhin erreichbar

Der OVE unterstützt die Maßnahmen zur Eindämmung des Coronavirus und damit auch die behördlichen Vorgaben zur Reduktion der Sozialkontakte. Damit unsere Mitarbeiterinnen und Mitarbeiter wie gewohnt für Sie erreichbar bleiben, haben wir entsprechende Maßnahmen getroffen.

Digitaler Zugriff auf Fachwissen: OVE und ASI unterstützen

Die aktuelle Situation aufgrund von Covid-19 stellt den Lehr- und Ausbildungsbetrieb vor große Herausforderungen. Gemeinsam mit Austrian Standards unterstützt der OVE beim Home-Learning und Home-Teaching.

Medizinische Geräte: Kostenfreie Standards von ISO und IEC

Viele Unternehmen stellen im Kampf gegen Covid-19 derzeit ihre Produktion auf die Herstellung von medizinischen Geräten um. Der OVE gemeinsam mit den internationalen Standardisierungsorganisationen ISO und IEC unterstützt diese Bemühungen.

"Klima wenden": Einreichfrist für Videowettbewerb verlängert

Aufgrund der aktuellen Situation wird die Einreichfrist für den Videowettbewerb von ScienceClip.at verlängert. Noch bis 13. November 2020 können Schülerinnen und Schüler ihr Video einreichen.

Mit freundlichen Grüßen
Ihr OVE Österreichischer Verband für Elektrotechnik

Hinweis: *Nicht immer werden in diesem Newsletter weibliche Formen explizit angeführt. Es wird jedoch ausdrücklich darauf hingewiesen, dass sich alle personenbezogenen Formulierungen grundsätzlich gleichermaßen auf Frauen und Männer beziehen.*

Impressum:
OVE Österreichischer Verband für Elektrotechnik
Krenngasse 37
8010 Graz

Newsletter abbestellen