© Syntegon

Pharmaproduktion

Neue Regularien, KI und Covid-19 nehmen Einfluss

Seite 27

©chombosany_Getty Images

Internet of Things

Den Aufwand für Cyberkriminelle erhöhen

Seite 28

©sdecoret - stock.adobe.com

Cybersicherheit

Das Prinzip Hoffnung hat ausgedient

Seite 29

Security Management in der Prozessindustrie

NAMUR beschreibt Wege zum systematischen Aufbau eines Schutzkonzepts

Auch wenn derzeit das Corona-Virus die Schlagzeilen beherrscht – ein großes unternehmerisches Risiko liegt heute und wohl auch in Zukunft in der Gefahr von Cyberangriffen. Da kommt das neue Arbeitsblatt NA 169 der NAMUR zum Thema „Automation Security Management in der Prozessindustrie" gerade recht: Es beschreibt die Schritte zum systematischen Aufbau eines Schutzkonzepts gegen Angriffe auf Automatisierungssysteme der Prozessindustrie. Zu diesem brisanten Thema äußern sich im CHEManager-Interview Felix Hanisch, Head of Process & Plant Safety bei Bayer in Leverkusen und Vorstandsvorsitzender der NAMUR, Erwin Kruschitz, Vorstandsvorsitzender von Anapur in Frankenthal und Leiter des NAMUR-Arbeitskreis „Automation Security", sowie Hartmut Manske, Head of Automation & Robotics bei Merck in Darmstadt, der maßgeblich an der Verfassung des NA 169 beteiligt war. Die Fragen stellte Volker Oestreich.

"Funktionale Sicherheit und IT-Security lassen sich auch dann nicht voneinander trennen, wenn unterschiedliche Organisationseinheiten sie realisieren."

Felix Hanisch, Head of Process & Plant Safety, Bayer und Vorstandsvorsitzender der NAMUR

„Die Interaktion zwischen IT und OT läuft nicht nur innerhalb der Unternehmen, sondern auch auf Verbandsebene."

Erwin Kruschitz, Vorstandsvorsitzender, Anapur, Frankenthal und Leiter NAMUR-Arbeitskreis „Automation Security"

„Ständig werden neue Schadcodes ins Netz gestellt, neue Angriffsvektoren entworfen, weiterentwickelte Angriffs-Tools zum Download angeboten."

Hartmut Manske, Head of Automation & Robotics, Merck

CHEManager: Zur Cyber Security in der Industrie gibt es eine Vielzahl von Publikationen, Normen und Vorschriften. Was hat die NAMUR zur Herausgabe des NA 169 „Automation Security Management in der Prozessindustrie" veranlasst und an wen richtet sich dieses Arbeitsblatt?

Hartmut Manske: Das Dokument ist für Personen geschrieben, die aktiv an der Bereitstellung, Bedienung, Steuerung und Überwachung sowie der Administration von IT-Systemen zur Produktionssteuerung und -überwachung mitwirken bzw. diese verantworten. Als Zielgruppe adressiert das Dokument vor allem Betriebe der Prozesschemie und Pharmaproduktion und fokussiert auf Aspekte der IT-Security für die produktionsnahen IT-Systeme. Wesentliche Rahmenbedingungen – technisch wie regulatorisch – weichen von dem Umfeld der Fertigungsindustrie ab – deshalb haben wir das NA 169 erstellt.

Felix Hanisch: In der Betrachtung der Automatisierungssysteme hat ein Paradigmenwechsel stattgefunden. Die Annahme, dass die Systeme durch eine physikalische Trennung, das sogenannte AirGap, oder durch technologische Abschottung auch bei Anbindung an das als sicher geltende Unternehmensnetz nicht gefährdet sind, musste revidiert werden. Außerdem sind IT-Security-Maßnahmen auf Unternehmensebene nur bedingt geeignet, um Automatisierungseinrichtungen zu schützen. Security-Maßnahmen der IT setzen in der Regel darauf, dass alle im IT-Netzwerk verfügbare Systeme nach homogenen IT-Security-Standards auf der Basis einheitlicher Technologie betrieben werden. Automatisierungssysteme dagegen werden gemäß diverser Vorgaben der Systemhersteller mit unterschiedlichen Technologien betrieben. Dadurch haben wir – zumindest heute noch – teils andere Rahmenbedingungen, wie zum Beispiel abweichende Patchintervalle oder unterschiedliche Härtung von Systemen.

Erwin Kruschitz: Aus der Sicht der Automatisierungssysteme müssen Netzwerke außerhalb des Automatisierungsumfelds hinsichtlich der Risikoeinschätzung als nicht sicher eingestuft werden. Deshalb müssen maßgeschneiderte Schutzkonzepte eingesetzt werden, wobei die spezialisierte Funktion und die geringere Variabilität eines Automatisierungssystems genutzt werden kann. Da eine effektive physikalische Trennung bei Nutzung nicht kabelgebundener Endgeräte, mobiler Datenträger oder durch Anschluss von Programmiergeräten aufgeweicht wird und dadurch eine Gefährdung von Automatisierungssystemen erfolgt, sind besondere Anstrengungen zu unternehmen, diese Faktoren zu minimieren.

Ebenso ist eine Rückwirkung der Automatisierungssysteme auf außenliegende Netzwerke und die damit verbundenen Systeme zu unterbinden. Die Komplexität erfordert ein strukturiertes technisches und organisatorisches Vorgehensmodell. Dabei wird empfohlen, sich an der Struktur und den Inhalten von Normen und Standards auszurichten.

Was sind die besonderen Herausforderungen und Ziele bei Security-Maßnahmen für die Prozessautomation?

H. Manske: Bei der Auswahl und Umsetzung von Security Maßnahmen im Bereich der Automation ist es von besonderer Bedeutung, dass es zu keiner oder nur zu einer tolerierbaren Beeinträchtigung des Produktionsprozesses kommt. Dies führt zu einer abweichenden Gewichtung der klassischen IT-Security-Ziele, nämlich – in dieser Reihenfolge – Vertraulichkeit, Integrität und Verfügbarkeit. Bei uns liegt der Schwerpunkt eindeutig auf der Verfügbarkeit. Gleichzeitig muss als primäres Ziel mit höchster Gewichtung der Schutz von Verfügbarkeit und Integrität der Safety-Funktionen beziehungsweise der Safety-Systeme berücksichtigt werden.

Automation Security und Functional Safety sind unterschiedliche Dinge – aber wie eng sind sie miteinander verknüpft?

F. Hanisch: Die deutsche Entsprechung des englischen Begriffes „Security" ist „Angriffssicherheit". Aufgabe der Security ist es, materielle wie immaterielle Dinge, die für den Eigentümer einen Wert darstellen, vor Bedrohungen zu schützen. Neben den von Herrn Manske genannten klassischen Schutzzielen der IT Security ist bei der Automation Security immer auch der Aspekt der Betriebssicherheit oder „Safety" mit zu betrachten. Automatisierungseinrichtungen übernehmen auch Funktionen des Personenschutzes, der Anlagensicherheit, des Umweltschutzes oder des Schutzes wertvoller Güter. Diese „Funktionale Sicherheit" betrachtet Gefährdungen für Menschen, die Umwelt und die Anlage selbst, die durch Zufall und Unfall entstehen. Die Gefahren lassen sich durch Wahrscheinlichkeiten ausdrücken, da sie nicht Auswirkungen eines gezielten Willens eines Angreifers sind. Themen der funktionalen Sicherheit sind nicht im primären Fokus des NA 169, werden aber von den Erörterungen berührt, denn aus Fehlfunktionen von Automatisierungssystemen können Gefährdungen auch für nicht-digitale Objekte resultieren. Dem wird mit sicherheitsgerichteten Steuerungen begegnet, die auch bei Cyberangriffen ihre Schutzfunktion erfüllen müssen. Es gibt mittlerweile Beispiele, bei denen diese gefährdet war.

Das heißt, Schwachstellen bei der Cyber Security können Probleme bei der Functional Safety als Konsequenz haben?

F. Hanisch: Funktionale Sicherheit und IT Security lassen sich nicht voneinander trennen, auch dann nicht, wenn unterschiedliche Organisationseinheiten sie realisieren. Konkret bewerten wir die grundlegenden Anforderungen an IT Security im Kontext der funktionalen Sicherheit durch eine IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen auf Basis des NAMUR Arbeitsblattes NA 163. Dies ist mittlerweile schon ein Download-Klassiker auf der NAMUR Homepage. Das wird das neue Arbeitsblatt NA 169 hoffentlich auch bald sein!

Welche Vorgehensweise für die Einrichtung eines „Cyber-Security-Management-Systems" empfehlen Sie und wie hilft das NA 169 dabei?

H. Manske: Das Dokument beschreibt die Schritte zum systematischen Aufbau eines Schutzkonzepts gegen Angriffe auf Automatisierungssysteme der Prozessindustrie. Damit soll erreicht werden, dass eine Beeinträchtigung der funktionalen Sicherheit verhindert, die Zuverlässigkeit und Verfügbarkeit der Systeme und Anlagen sichergestellt und der Schutz von kritischen Daten gegen unberechtigten Zugriff und Manipulation gewährleistet wird.

Der Begriff „Angriff" erstreckt sich dabei auf alle Aktivitäten, welche die Schutzziele gefährden, also auch auf solche, die nicht mutwillig, sondern in Unkenntnis oder Fahrlässigkeit vom Bedien- oder Wartungspersonal geschehen. Insbesondere werden auch die Ausbreitung und die Auswirkung von Schadcode auf Systeme der Automatisierungstechnik als Angriff betrachtet. Dabei ist zu berücksichtigen, dass in einem qualifizierten System im Sinne der GMP das Vorhandensein einer Schadsoftware ohne direkt erkennbare Auswirkungen ein erhebliches Problem darstellen kann.

Wir beschreiben also mit dem NA 169 eine Vorgehensweise für die Einrichtung und den Betrieb eines „Cyber Security Management Systems", das die Maßnahmen, Rollen und die Aufbauorganisation für einen Anlagenbetreiber umfasst. Ziel ist es dabei, für eine große Zahl von Systemen kurzfristig einen Grundschutz zu implementieren und die Detailbetrachtung auf eine geringe Anzahl von Systemen zu reduzieren.

E. Kruschitz: Die Aktivitäten zur Einführung eines CSMS für die Automatisierung sollten als ein Projekt implementiert werden und anschließend im weiteren Betrieb als kontinuierlicher Prozess mit einem Abstimmungsprozess auf strategischer und operativer Ebene fortgeführt werden. Dem Projektteam sollten Mitarbeiter der Automatisierungstechnik, der Betreiber und der Unternehmens-IT angehören. Im Rahmen des Projektes müssen die Rollen und Zuständigkeiten sowie die Organisationsstruktur für den späteren Betrieb des CSMS festgelegt werden. Dabei kann man ein Rollenkonzept analog zu den Rollen in der IT Security in Betracht ziehen.

Sofern Anlagen betroffen sind, für die eine GMP-konforme Qualifizierung vorliegt, sollten die neu zu schaffenden Prozesse mit der Qualifizierung synchronisiert werden, da hieraus erhebliche Synergieeffekte entstehen können.

F. Hanisch: Es ist ganz wichtig, dass die Betriebsmitarbeiter, die die Maßnahmen des CSMS ausführen oder akzeptieren sollen, hinreichend über deren Sinnhaftigkeit aufgeklärt werden. Die Einführung muss daher von einer Awareness-Kampagne und der Einführung eines entsprechenden Schulungsprogrammes begleitet werden. Die Mitarbeiter müssen in die Lage versetzt werden, Anomalitäten auf Systemen und in deren Verhalten zu erkennen und sie müssen trainiert sein, entsprechende Maßnahmen wie Meldung, Protokollierung und Gegenwirkung durchzuführen. Daher ist die Stärke der Verteidigungsstrategie nicht nur von den eingesetzten technischen Mitteln und der Kompetenz der Spezialisten abhängig, sondern sie steht und fällt mit dem Bewusstsein aller Mitarbeiter, die mit den betreffenden Systemen arbeiten.

Wann muss man mit den Überlegungen für die geeignete Automation Security beginnen und wie sollte sie die Automatisierungspyramide mit ihren verschiedenen Ebenen von den Feldgeräten bis hin zum ERP berücksichtigen?

F. Hanisch: Die Automation Security Policy definiert im Idealfall alle organisatorischen Vorgaben und Prozesse von der Beschaffung eines Automatisierungssystems bis zu dessen Außerbetriebnahme und Entsorgung. Während bei Beschaffung und Entsorgung häufig auf Standards zurückgegriffen und Prozesse aus der IT genutzt werden können, muss der Bereich der Konzeption und Konfiguration sowie die Vorgaben zum Betrieb ausführlich betrachtet werden. „Security by Design" ist hier das Motto. Wie gelingt es mir, die Systeme so aufzubauen, dass in der Betriebsphase Schutzmaßnahmen kosteneffizient, also möglichst automatisiert, aufrechterhalten und an aktuelle Bedrohungslagen angepasst werden können? Dazu gehören Vorgaben für Patch-Intervalle, der Einsatz von Antiviruslösungen für die Systeme im Produktionsbetrieb, Verfahrensanweisungen für den Umgang mit Wechseldatenträgern aber auch Anweisungen für Dienstleister und Lieferanten.

Bei der Einführung von Schutzmaßnahmen, zum Beispiel einer Segmentierung, ist zu berücksichtigen, dass die Absicherung nicht nur innerhalb eines Systems zwischen den Ebenen erfolgen muss, sondern auch zwischen Komponenten innerhalb einer Ebene. Beispielsweise sollten parallel angeordnete Automatisierungssysteme gegeneinander geschützt werden.

H. Manske: Die fundamentale Grundlage einer Security-Strategie ist die Kenntnis aller Systeme – sowohl Software als auch Hardware – und deren aktueller Konfiguration. Eine mangelhafte Informationsbasis kann zu einem Betrieb mit unzureichend gepatchten Systemen führen oder sie kann auch das Business Continuity Management (BCM) in einer kompromittierten Situation negativ beeinflussen. Es ist also eine geeignete Asset-Inventory-Lösung zu identifizieren, zu implementieren und der Pflegezustand umfassender und adäquater Informationen sicherzustellen, wozu auch ein Lizenzmanagement und eine Patch-Strategie beitragen. Neben der eingesetzten HW/SW spielen auch die Struktur und die Verbindungen wichtige Rollen, daher ist es unabdingbar, dass diese ebenfalls erfasst und dokumentiert werden.

Fortsetzung auf **Seite 26** ▶

Automation Security Management in der Prozessindustrie

◄ Fortsetzung von **Seite 25**

Bei den Diskussionen zur Automation Security wird immer die notwendige Zusammenarbeit von OT und IT beschworen. Was genau gehört zur OT und wo liegen die Schnittstellen bzw. die Verbindungsstellen zur IT?

E. Kruschitz: „Operational Technology" oder kurz OT ist definitionsgemäß die „Hard- und Software, die eine Änderung von Prozessen und Ereignisse im Unternehmen durch die direkte Überwachung und/oder Steuerung der physischen Geräte erkennt oder bewirkt". Damit ist die Automatisierungstechnik oder Automation Technology AT Teil der OT. Dazu gehören also zum Beispiel Prozessleitsysteme und zugehörige Engineering-Systeme, sicherheitsgerichtete Steuerungen, SCADA und Asset Management-Systeme und natürlich die Feldgeräte mit den zugehörigen Konfigurationswerkzeugen und der Kommunikationsinfrastruktur.

Abhängig von der Aufteilung der Verantwortungsbereiche können auch MES Systeme, PIMS und LIMS, Logistiksysteme oder die Gebäudeautomatisierung in den Bereich der Automation Security fallen.

F. Hanisch: Damit eine klare Abgrenzung der Rollen und Verantwortlichkeiten möglich wird, muss ein grundlegendes gegenseitiges Verständnis zwischen den Verantwortlichen bzw. Betreibern der Operational Technology und der Unternehmens-IT herbeigeführt und sichergestellt werden, dass jedes einzelne System in eine definierte Zuständigkeit fällt.

Das Ergebnis eines solchen Abstimmungsprozesses sollte eine übergeordnete, unternehmensweite Corporate Security-Strategie für alle Systeme sein. Die IT Security und die Bereiche der OT Security bilden dabei die Säulen dieser unternehmensweiten Strategie, die die Grundlage aller Maßnahmen in einem Unternehmen zur Absicherung gegen computergestützte Angriffe darstellt. Dabei sollte beachtet werden, dass soweit als möglich mit gleichen Prozessen und Standards in allen Bereichen gearbeitet wird und unterschiedliche Vorgehensweisen auf die speziellen Anforderungen der Automatisierungssysteme beschränkt bleiben.

Wie sieht es in der Realität mit diesen Abgrenzungen aus und wie funktioniert die Zusammenarbeit zwischen IT und OT?

E. Kruschitz: Inzwischen kann man mehr und mehr von Zusammenarbeit sprechen. Dort, wo wir vor ein paar Jahren mehr übereinander gesprochen haben, sprechen wir jetzt miteinander. Durch die Digitalisierungsinitiativen ist das Bewusstsein gereift, dass es in der OT viele spannende Betätigungsfelder gibt. Und die können mit modernen Mitteln der IT und der langjährigen Digitalisierungserfahrung der OT bearbeitet werden.

Felix Hanisch, Vorstandsvorsitzender der NAMUR, zeichnet auf der NAMUR-Hauptsitzung 2019 Erwin Kruschitz, CEO der Anapur und Leiter des Arbeitskreises 4.18 „Automation Security", mit der Goldenen Ehrennadel aus. © NAMUR

Aber es kommt diesen Gesprächen immer noch zu Missverständnissen. Ein Prozessautomatisierer versteht unter „Risiko", dass eine verfahrenstechnische Anlage nicht mehr funktioniert. Ein ITler versteht unter Risiko, dass Schadcode auf einen Computer gelangt. Das klingt banal, führt aber in der Frage, wie man einem Risiko begegnet und wer über den Umgang mit dem Risiko entscheidet, zu Diskussionen. Besonders spannend wird es, wenn es um Verantwortlichkeiten geht, zum Beispiel wenn eine Anlage durch ein cyber-kompromittiertes Safety System einen Gesundheits- oder Umweltschaden verursacht hat. Doch es gibt ermutigende Fortschritte. Die Interaktion läuft nicht nur innerhalb der Unternehmen, sondern auch auf Verbandsebene wie VCI, Bitkom, Dechema, DKE und ZVEI.

Die NAMUR arbeitet sehr eng mit dem BSI zusammen bei der Erstellung eines IT-Grundschutzprofils für die chemische Industrie.

Felix Hanisch

F. Hanisch: Ich halte es für ganz wichtig, dass wir hier seitens der NAMUR auch weiterhin sehr eng mit dem Bundesamt für Sicherheit in der Informationstechnik, kurz BSI, zusammenarbeiten, beispielsweise bei der Erstellung eines IT-Grundschutzprofils für die chemische Industrie. Wir profitieren hier beide von der gegenseitigen Expertise: Was sind die Herausforderungen in der realen Praxis? Was sind die Bedrohungsszenarien von morgen, für die wir uns heute vorbereiten müssen? Das geht nur zusammen!

H. Manske: Wir haben in der OT Security in den letzten Jahren deutliche Fortschritte gemacht und neben den normativen und technischen Voraussetzungen in vielen Unternehmen auch die notwendigen organisatorische Strukturen geschaffen. Dennoch gibt es immer noch trennende Elemente zwischen IT- und OT Security. Unser Ziel muss es daher sein, das Zusammenwachsen von IT und OT weiter voranzutreiben und ein Security Konzept „aus einem Guss" zu erreichen. Wir dürfen den immer raffinierter vorgehenden Angreifern keine noch so kleine Schwachstelle bieten, an der sie ansetzen können.

Cyber Security ist wie Hände waschen bei Corona: Je mehr es tun, desto besser wirkt es.

Erwin Kruschitz

E. Kruschitz: Organisatorisch haben Unternehmen unterschiedliche Ansätze gefunden, mit den Fragen umzugehen. Manche integrieren traditionelle OT Aktivitäten in IT-Organisationen. Andere ziehen eine Zuständigkeitsgrenze zwischen Prozess- und Betriebsleitebene oder trennen die „IT" in Produktions-IT und Finanz-IT. Für eine Bewertung der Modelle ist es allgemein noch zu früh.

Derzeit hält uns die Corona-Krise in Atem – ein realer Virus fordert intensive Schutz- und Bekämpfungsmaßnahmen. Aber diesen Virus werden wir in einer endlichen Zeit in den Griff kriegen. Kann man auf Ähnliches auch bei Cyber-Viren und anderen Cyberattacken hoffen?

H. Manske: Nein. Die Bedrohungslage ist einer hohen Dynamik unterworfen. Ständig werden neue Schadcodes ins Netz gestellt, neue Angriffsvektoren entworfen, weiterentwickelte Angriffs-Tools zum Download angeboten. Deshalb muss das erlangte Sicherheitsniveau permanent neu bewertet werden – zum Beispiel in regelmäßigen Intervallen und bei Bekanntwerden neuer Angriffsmethoden. Aber das gilt generell für das Thema Sicherheit. Genauso wie wir aus Schadensereignissen im allgemeinen lernen, unsere technischen Sicherheitsfunktionen anzupassen – deshalb haben heute alle Kraftfahrzeuge Sicherheitsgurte, ABS und vieles mehr – müssen wir in der Security immer wieder nachjustieren. Das Schwierige ist die angesprochene hohe Dynamik in diesem Bereich.

E. Kruschitz: Um Ihre Parallele zu Corona aufzugreifen: Cyber Security ist wie Hände waschen bei Corona: Je mehr es tun, desto besser wirkt es.

■ www.namur.de

NAMUR Award

Innovative Prozess- und Betriebsführung

Der NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie – ist die Förderung junger Talente während ihres Studiums sehr wichtig. Die Mitgliedsunternehmen bieten ein vielfältiges Angebot an Ausschreibungen für Werkstudenten und Praktikanten und ermöglichen oft auch das Durchführen von Abschlussarbeiten in ihren Häusern.

Auch 2020 vergibt die NAMUR wieder je einen Preis für hervorragende und wegweisende Diplom/Master- bzw. Promotions-Arbeiten zum Themenkreis „Innovative Prozess- und Betriebsführung". Die Arbeiten sollten aus den Fachgebieten Automatisierungstechnik, Elektrotechnik, Messtechnik einschließlich Online-Analytik, Prozessnahe Informationstechnik, Regelungstechnik oder Prozessleittechnik stammen und die wichtigsten Ziele der NAMUR wie „Sichere Prozesse durch Automatisierungskompetenz" und „Kosteneinsparungen durch Nutzung von Synergieeffekten" unterstützen.

Förderung praxisrelevanter Entwicklungen

Zur Entwicklung und Anwendung leistungsfähiger Methoden der Prozessautomatisierung sind sowohl vertiefte Kenntnisse der Automatisierungstechnik als auch der Verfahrens- und Prozesstechnik erforderlich. Um die Attraktivität dieses zukunftsträchtigen, interdisziplinären Arbeitsgebietes weiter zu erhöhen und junge Absolventen zu ermutigen, sich darin zu vertiefen, prämiert die NAMUR seit vielen Jahren die beste Diplom-/Masterarbeit sowie die beste Promotionsarbeit. Damit wird sowohl die Darstellung der Bedeutung der Automatisierungstechnik und Digitalisierung in der Prozessindustrie als auch die Gewinnung qualifizierten Nachwuchses gefördert und das kontinuierliche Aufgreifen von Zukunftsthemen mit Bedeutung für die Prozessführung unterstützt.

Aufruf zur Einreichung 2020

Lehrstuhlinhaber entsprechender Fachgebiete können Anträge für die beste Abschlussarbeit einreichen. Neben einem formlosen Antrag des Lehrstuhls gehören zu den Bewerbungsunterlagen:

- ein erweiterter Abstract für die Vorauswahl mit Motivation zum Thema, Kernaussagen und Ergebnissen der Arbeit
- die Diplom-/ Masterarbeit bzw. Promotionsarbeit sowie optional zugehörige Veröffentlichungen.

Die Unterlagen müssen bis zum 30. Juli 2020 per E-Mail an office@namur.de gesendet werden.

Die Preisverleihung findet im Rahmen der NAMUR-Hauptsitzung am 6.November 2020 statt. Auch in diesem Jahr wird wieder zusätzlich der Lehrstuhl prämiert, aus dem die jeweilige Arbeit kommt. Die Dotierung beträgt 2.000 EUR für die ausgewählte Diplom-/Master-Arbeit und 3.000 EUR für den betreuenden Lehrstuhl bzw. 3.000 EUR für die ausgewählte Promotionsarbeit und 5.000 EUR für den betreuenden Lehrstuhl zur Verwendung für die Förderung des Nachwuchses in der Prozessautomatisierung. (vo)

■ www.namur.de

Webinar am 28. Mai 2020 um 14:00 Uhr

Plattformgetriebenes Molekulares Design

Die überwiegende Mehrheit der zehn wertvollsten Unternehmen der Welt sind solche mit digitalen Plattformen. Diese Plattformen stellen eigene Ökosysteme dar, in denen wertschöpfende Interaktionen zwischen Personengruppen stattfinden, die auf der Grundlage von Echtzeitanalysen von Datenströmen basieren. Doch wie weit entfernt von dieser neuen Realität, die im letzten Jahrzehnt entstanden ist, sind Forschungsorganisationen im Bereich des Molekularen Designs? Die Schrödinger Molecular Design Platform vereint physikbasierte prädiktive Modellierung, maschinelles Lernen, bzw. „Deep Learning" und Unternehmensinformatik. Präsentiert wird das Webinar von Jörg Weiser, Managing Director von Schrödinger Deutschland.

Die zentralen Lernziele des einstündigen Webinars sind u.a. der aktuelle Stand von Simulationen in der chemischen und pharmazeutischen Forschung, Fähigkeiten von datenbasierten Modellen und wissenschaftlichen Berechnungen und Möglichkeiten der Innovation durch eine erweiterte molekulare Design-Plattform.

■ https://bit.ly/2RDSE77

Attacken

Volker Oestreich

„Mir geht es gut!" Das muss ich mir nicht immer wieder sagen, ich weiß es. Ich habe in meinem ganzen Leben (und das sind immerhin über 70 Jahre) niemals besondere Einschränkungen erlebt – nicht unbedingt im Luxus gelebt, aber immer ohne Entbehrungen. Als Kind konnte ich mit meinen Freunden spielen, in der Schule gab es die altersgemäßen Herausforderungen, das Studium war intensiv begeisternd, der Beruf verzeichnete viele Höhen. Natürlich gab es auch Risiken: Der Keuchhusten, den ich als Kleinkind durchmachte, war lebensbedrohlich, das erste Fahrrad Marke „Uralt" viel zu groß und nach heutigen Maßstäben verboten unsicher, die beruflichen Veränderungen aufreibend oder risikobehaftet. Aber immer hat es noch gereicht für einen Theaterbesuch oder ein Bier in der Kneipe.

Und auf einmal ist alles anders. Covid-19 hat zugeschlagen und verändert unser Leben. Persönliche Freiheiten sind eingeschränkt, direkte Kontakte zu Kollegen, Freunden und Verwandten sind drastisch reduziert. Die Wirtschaft steht vor ungeahnten Herausforderungen – und auch neuen Chancen. Statt des „Business as usual" lernen wir, schnell mit Veränderungen umzugehen, Maßnahmen zu ergreifen und Zukunft zu gestalten. Das Homeoffice wurde in kurzer Zeit für viele Beschäftigte zur Alternative – und meist hat es irgendwie funktioniert. Für Straßenbahnfahrer, Bäcker oder Chemiefacharbeiter klappt das noch nicht ganz so gut – aber auch das wird sich ändern. Grenzenlose Vernetzung und künstliche Intelligenz gehören zu den Schlüsseln hierfür, und die Coronakrise wird vielleicht die Umsetzung beschleunigen.

Doch wo viel Licht ist, ist bekanntlich auch Schatten. In Zeiten, in denen informationstechnische Systeme global über Internet und Mobilfunk vernetzt sind, steigt die Bedrohung von Cyberattacken. Die Geschäftsmodelle krimineller Banden und Einzeltäter passen sich den neuen Möglichkeiten an und nutzen diese: Die Sorge der Bevölkerung über das Coronavirus wird genutzt, um Computerviren über Fake-E-Mails zu verbreiten. Mitarbeiter im Homeoffice können zu neuen Einfallstoren für Cyberangriffe werden.

Cyberkriminalität gehört zu den größten globalen Bedrohungen – für den Einzelnen, für Unternehmen, für Institutionen und kritische Infrastrukturen. Während Unternehmen bei Attacken Imageschäden, finanzielle Verluste und Datendiebstahl fürchten müssen, droht kritischen Infrastrukturen der Ausfall mit erheblichen Auswirkungen für die Bevölkerung.

Cybersecurity wird damit zu einer besonderen Herausforderung im privaten Alltag genauso wie in geschäftlichen Abläufen. Der Schutz der IT-Infrastrukturen muss ein wichtiger Bestandteil der Digitalstrategie von Unternehmen sein – mit permanentem Weiterentwicklungsbedarf. Denn so schnell, wie sich der Cyberraum verändert, passen auch Cyberkriminelle ihre Angriffsmethoden an.

In dieser Ausgabe des *CHEManager* bilden deshalb Maßnahmen zur Cybersecurity wieder einen redaktionellen Schwerpunkt. Denn: Das Prinzip Hoffnung hat ausgedient, strukturelle Vorkehrungen zum Umgang mit Cyberattacken sind angesagt. Wer das Internet of Things nutzen will, muss vermeiden, dass es für ihn ein Internet of Horrors wird. Und wer in der Prozessindustrie sichere Fernwartung betreiben will, sollte auf Einladungen zum Rendezvous warten. Wie das alles funktioniert und einzurichten ist, beschreiben unsere Autoren und das NAMUR-Arbeitsblatt NA 169 „Automation Security Management in der Prozessindustrie", in dem Schritte zum systematischen Aufbau eines Schutzkonzepts aufgezeigt werden. „Cybersecurity ist wie Hände waschen bei Corona. Je mehr es tun, desto besser wirkt es" betont Erwin Kruschitz, CEO von Anapur, und weist darauf hin, dass wir alle gefordert sind: „Wer glaubt, dass Cybersecurity Experten für die Sicherheit unserer Anlagen zuständig sind, der glaubt auch, dass Ärzte für unsere eigene Gesundheit zuständig sind."

Ich wünsche Ihnen, wie immer, ein gutes und erfolgreiches Studium Ihres aktuellen *CHEManager*. Bleiben Sie gesund und virenfrei! Wir bieten Ihnen heute und in Zukunft die Informationen, die Ihnen helfen, nachhaltig die Belange Ihres Unternehmens, Ihrer Mitarbeiter und Ihrer Umwelt zu verfolgen.

Ihr

voe@voe-consulting.de