CHEMCOLOGNE

3 | 2020

DAS CHEMIE-MAGAZIN FÜR DIE REGION

compact

BSI-PRÄSIDENT ARNE SCHÖNBOHM IM KLARTEXT:

Muss sich die Chemiebranche besonders intensiv vor Cyber-Angriffen schützen?

CHEMCOLOGNE INITIIERT „CHEMTELLIGENCE“:

Neues Format für Innovationsprozesse in der Chemieindustrie

SCHWERPUNKT

Cyber Security und Anlagensicherheit in der chemischen Industrie

BUCHEN®
IM AUFTRAG DER ZUKUNFT

XERVON®
IM AUFTRAG DER ZUKUNFT

Ihre Chance auf eine erfolgreiche Zukunft

Die Unternehmen von BUCHEN und XERVON zählen zu den leistungsstärksten Komplettanbietern von Instandhaltungslösungen für die chemische und petrochemische Industrie und zahlreiche weitere Branchen. Wir bieten Ihnen herausfordernde Aufgaben und Einsatzgebiete in einem spannenden industriellen Umfeld sowie umfassende Weiterbildungsmöglichkeiten und attraktive Konditionen bei einem renommierten Unternehmen in Familienbesitz.

Wir suchen Sie für unterschiedlichste Aufgaben in den Bereichen:

- Industriereinigung
- Gerüstbau
- Isolierung
- Rohrleitungsbau
- Maschinentechnik
- EMSR-Technik
- Schweißtechnik/Stahlbau
- Oberflächentechnik/ industrieller Korrosionsschutz
- Logistik
- Informationstechnologie
- Verwaltung

Schauen Sie in unser Stellenportal und kommen Sie in ein starkes Team! Jetzt bewerben!
> rms-karriere.de

Wir bilden auch aus!
Mit Übernahmegarantie bei guten Leistungen.
Jetzt bewerben!

KLARTEXT

SCHWERPUNKT

Cyber Security und Anlagensicherheit in der chemischen Industrie

CHEMCOLOGNE INTERN

WIRTSCHAFTSNACHRICHTEN

UPDATE

von Daniel Wauben, Geschäftsführer ChemCologne e. V.

2020 ist in vielerlei Hinsicht ein verrücktes Jahr, das durch die Corona-Pandemie überall seine Spuren hinterlassen hat. Über weite Strecken wurden auch die Abläufe bei den ChemCologne-Mitgliedsunternehmen erheblich beeinflusst, was höchste Anforderungen an deren Krisenmanagement stellte. Und auch bei ChemCologne hat Covid-19 in diesem Jahr einiges durcheinandergewirbelt und die Durchführbarkeit unserer Aktivitäten deutlich erschwert. So mussten wir schweren Herzens den Kooperationstag ausfallen lassen und hatten mit Terminverschiebungen bei „Meine Position ist spitze!“ zu kämpfen. Im November waren wir schließlich gezwungen, mit unserer Mitgliederversammlung auf ein Online-Format auszuweichen.

Dem Jahr 2021 sehen wir verhalten optimistisch entgegen. Nicht zuletzt die guten Nachrichten über mehrere kurz vor der Einführung stehende Impfstoffe sollten uns Anlass zur Hoffnung geben, dass sich Schritt für Schritt die Abläufe in der Chemiebranche wieder normalisieren. Viele Unternehmen richten deshalb den Blick klar nach vorne – auch wir: Die Zukunftsthemen der Branche haben sich 2020 weiterentwickelt. Um nur einige zu nennen: Energiewende, Nachhaltigkeit und Kreislaufwirtschaft sowie die fortschreitende Digitalisierung werden auch 2021 im Fokus stehen.

Bei diesen und auch bei einigen weiteren Herausforderungen für die Branche möchte ChemCologne zukünftig wertvolle Impulse setzen. Deshalb haben wir das Open-Innovation-Format „Chemtelligence“ initiiert. Dort können Lösungsanbieter gemeinsam mit den Chemie-Unternehmen an neuartigen Prozessen arbeiten und so Mehrwerte schaffen. Mehr dazu in unserer Rubrik „ChemCologne intern".

Wir wünschen nun allen Mitgliedern und Lesern einen den Umständen entsprechend friedvollen und schönen Jahresausklang und freuen uns 2021 wieder auf gemeinsame Aktivitäten. ●

Impressum

Herausgeber: ChemCologne e. V., Neumarkt 35 – 37, 50667 Köln · www.chemcologne.de
info@chemcologne.de · Tel. +49 (0) 221 2720 530, Fax +49 (0) 221 2720 540
Ausgabe: 3|2020 vom 1. Dezember 2020
Fotos: Sonstige (10), ChemCologne (3), pixabay (1), Shutterstock (1), Ralf Baumgarten (1)
Redaktion: benekom Meerbusch, Dirk Rehberg, Inga Kristin Kunnen, Rita Viehl (Layout)
Magazin-Design und Titelmotiv: HolleSand, S. Espelage & A. Kuhn GbR, Köln
Druck: Bergner und Köveker, Krefeld

Jetzt mal Klartext, Herr Schönbohm, …

… muss sich die Chemiebranche besonders intensiv vor Cyberangriffen schützen?

Arne Schönbohm

CCC: Experten gehen davon aus, dass die zunehmende Digitalisierung zu steigenden Sicherheitsrisiken führt. Im jüngsten BSI-Lagebericht erklären Sie zudem, dass Corona die Cyber-Gefährdungslage erhöht. Warum ist das so und wie kann der Digitalisierungsschub für mehr Cyber-Sicherheit genutzt werden?

Schönbohm: Im Zusammenhang mit Corona wird gern von einem Brennglas gesprochen, das wirtschaftliche und gesellschaftliche Umstände beleuchtet und ins öffentliche Bewusstsein rückt. Drei Veränderungen sieht das BSI unter diesem „Corona-Brennglas“: Zum einen zeigt der mit Corona verbundene Digitalisierungsschub deutlich, wie wichtig eine funktionierende und sichere IT ist. Zum anderen hat Corona leider auch gezeigt, wie flexibel und anpassungsfähig Cyber-Kriminelle sind. Schließlich und drittens zeigte Corona auch, dass sich das BSI schnell auf die Krisensituation eingestellt und mit zielgruppengerechten Empfehlungen und Gegenmaßnahmen wirkungsvoll reagiert hat. Das BSI hat bewiesen, dass es seinem Anspruch nachkommt, Gestalter einer sicheren Digitalisierung in Deutschland zu sein. Relevant ist am Ende die Frage, wie mit dem Digitalisierungsschub durch Corona zukünftig umgegangen wird. Es war in der Anfangszeit der Pandemie vollkommen nachvollziehbar, dass zunächst Usability im Vordergrund stand, um die Arbeitsabläufe zu garantieren. Jetzt allerdings muss es zur neuen Normalität gehören, dass IT-Sicherheit bei allen digitalen Prozessen in Unternehmen und Institutionen nachgezogen bzw. bei neu aufgesetzten Prozessen von Beginn an mitgedacht wird. Digitalisierungsvorhaben wie die Einrichtung und Ausweitung des Home-Office-Betriebs oder Home-Schooling gelingen nur, wenn die Akzeptanz der Anwenderinnen und Anwender vorhanden ist. Dafür ist Cyber-Sicherheit die zentrale Voraussetzung.

CCC: Studien zeigen, dass nicht zuletzt die Chemieindustrie besonders stark von Cyberkriminalität betroffen ist. Worin liegt dies Ihrer Meinung nach begründet?

Schönbohm: Wir stehen schon seit Jahren in einem engen und vertrauensvollen Austausch mit der Chemiebranche. Unsere Arbeit in der NAMUR ist Ausdruck davon. Dabei mussten wir allerdings beobachten, dass IT-Sicherheit zu häufig noch nur als eines von vielen Risiken, die die Produktion bedrohen, wahrgenommen wird. Bei circa einer Milliarde Schadprogrammen, die wir im Zeitraum Mai 2019 bis Mai 2020 ermittelt haben, greift das zu kurz. Cyber-Kriminalität hat die Bedrohungslage deutlich verändert. Gezielte, über längere Zeiträume andauernde Angriffskampagnen gehören nun auch zur Realität des Chemiesektors. Dabei denken und arbeiten Cyber-Kriminelle gewinnorientiert, fokussieren sich meist auf umsatzstarke Firmen, die ein vergleichsweise geringes Sicherheitsniveau aufweisen. Denken Sie an den Spruch „den Letzen beißen die Hunde“. Um das zu verhindern, ist es nie zu spät. Vergleichsweise einfache technische und organisatorische Schutzmaßnahmen helfen, Cyber-Angriffe abzuwehren. Der BSI-IT-Grundschutz nimmt das Unternehmen an die Hand und führt sie Schritt für Schritt durch die IT-sichernden Prozesse. Hierzu geben wir gerne Auskunft, auch im Rahmen unserer Allianz für Cyber-Sicherheit, bei der jede Firma Mitglied werden kann.

CCC: Muss sich die Chemiebranche demnach besonders intensiv vor Cyberangriffen schützen? ▶

Über Arne Schönbohm

Arne Schönbohm ist seit dem 18. Februar 2016 Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), das als die Cyber-Sicherheitsbehörde des Bundes Informationssicherheit in der Digitalisierung für Staat, Wirtschaft und Gesellschaft gestaltet. Der gebürtige Hamburger (Jahrgang 1969) studierte Internationales Management in Dortmund, London und Taipeh und ist seit mehr als zehn Jahren in führenden Positionen im Bereich der IT-Sicherheit tätig. Darüber hinaus arbeitete Schönbohm als Sicherheitsexperte und Berater verschiedener politischer Entscheidungsträger auf Bundes- und Landesebene, so war er unter anderem Mitglied der Cyber Security Coordination Group der EU.

Schönbohm: Der Chemiebranche kommt aufgrund ihrer Produkte eine besondere Verantwortung für Mensch und Umwelt zu. Ein Betriebsausfall aufgrund von Ransomware, also einer Erpressersoftware, die die Unternehmensdaten verschlüsselt, ist nicht nur geschäftsschädigend, sondern kann im schlimmsten Fall auch Auswirkungen auf die direkte Umgebung des Werkes haben oder zu Lieferengpässen dringend benötigter Produkte führen. Produktionsanlagen, die durch Cyber-Kriminalität in einen so genannten undefinierten Zustand und unter die Störfallverordnung fallen, müssen dann abgeschaltet werden. So kam es in 2017 zu einem Angriff auf Chemieanlagen im Mittleren Osten, der unter dem Namen „Trition/Trisis/hatman" bekannt wurde. Hier wurden sicherheitsgerichtete Steuerungen kompromittiert. Diese letzte Verteidigungslinie bietet also keinen umfassenden Schutz vor versierten Angreifern. Wenn Unternehmen den BSI IT-Grundschutz umsetzen, macht es das den Angreifern sehr schwer, Schaden zu verursachen.

CCC: Der Diebstahl von sensiblen digitalen Daten bzw. Informationen gilt als einer der häufigsten Vorfälle in Sachen Cyberkriminalität innerhalb der Industrie. Warum sind die Unternehmen hierfür besonders anfällig?

Schönbohm: Grundsätzlich gilt: Cyber-Angriffe können alle Branchen treffen. Cyber-Kriminelle sind darauf aus, durch Cyber-Angriffe viel Geld zu verdienen. Sie gehen skrupellos vor und drohen u.a. damit, abgeflossene Daten an Mitbe-

Hintergrund

Die Chemieindustrie ist kein Sektor der Kritischen Infrastrukturen. Je nach Ausgang des parlamentarischen Verfahrens im Rahmen des IT-Sicherheitsgesetzes 2.0 (IT-SIG 2.0) können demnächst Chemie-Unternehmen, insbesondere Anlagen der Störfallverordnung (und hier vor allem hohe Gefahrenkategorien – dazu gehören viele Chemiebetriebe in Deutschland), als „Unternehmen im besonderen öffentlichen Interesse" ähnlichen Regulierungen unterliegen wie Kritische Infrastrukturen. Dazu kann das BSI zum jetzigen Zeitpunkt – aus Respekt vor dem Parlament und der noch laufenden Ressortabstimmung – jedoch keine Aussagen treffen. Das BSI ist seit 2018 Mitglied der NAMUR (Interessengemeinschaft Automatisierungstechnik der Prozessindustrie, www.namur.net), in der viele Fragestellungen der Digitalisierung der Prozessindustrie (in Nicht-KRITIS Bereichen) mit bearbeitet werden. Aktuell arbeitet das BSI beispielsweise zusammen mit der NAMUR an einem IT-Grundschutz-Profil für PLT-Sicherheitseinrichtungen in Produktionsanlagen der chemischen Industrie.

▶ werber zu verkaufen oder zu veröffentlichen. Deutsche Firmen – insbesondere die „hidden champions" des Mittelstands – investieren sehr viel in Forschung, sind technologisch führend, so dass Werksspionage ein lohnendes Geschäft sein kann. Wenn die Investitionen in die IT-Sicherheit da vergleichsweise mithalten können, würde ich mir weniger Sorgen machen müssen. Ich nenne Ihnen ein Beispiel, das Schule machen sollte: Krankenhäuser. Sie können aus dem Krankenhauszukunftsgesetz Mittel für die Digitalisierung beantragen. 15 Prozent davon müssen dann in die IT-Sicherheit fließen. Wer das berücksichtigt investiert nachhaltig in die Digitalisierung des eigenen Unternehmens.

CCC: Wie schätzen Sie den Entwicklungsstand der Chemieindustrie in Bezug auf Cyber Security und Anlagensicherheit aktuell ein?

Schönbohm: Das lässt sich nicht verallgemeinern oder pauschal beantworten. Der Umsetzungsstand von wirksamen Cyber-Sicherheitsmaßnahmen in den Unternehmen hängt stark vom Reifegrad und der Unternehmensgröße ab. Meine Erfahrung ist: Da wo das Thema in der Chefetage angekommen und zur Priorität gemacht wird, dort läuft es gut. Ich kann jedem Unternehmen an dieser Stelle nur den IT-Grundschutz des BSI ans Herz legen, insbesondere den für Produktionsanlagen. Er gibt umfangreiche Hilfestellungen. Es ist wie mit allen guten Gewohnheiten: Zuerst muss man den Anfang machen und dann Prozesse immer wieder einüben. Informationssicherheit ist die Voraussetzung einer erfolgreichen Digitalisierung. Für Informationssicherheit steht das BSI. Wir wollen die sichere Digitalisierung in der Chemieindustrie mitgestalten und unterstützen. ●

Cyber Security und Anlagensicherheit in der chemischen Industrie

Chancen ergreifen und Risiken minimieren

Das Internet of Things (IoT), Cloud Computing, Industrie 4.0 – die digitalen Errungenschaften unserer modernen Zeit bringen für Unternehmen sowohl ungeahnte Möglichkeiten als auch nie dagewesene Risiken mit sich. Das gilt für die gesamte Industrie im Allgemeinen ebenso wie für die Chemiebranche im Speziellen. Cyberattacken wie Phishing-Angriffe und Schadstoff-Software haben in den vergangenen Jahren stark zugenommen und gefährden nicht nur die Verfügbarkeit der IT-Infrastruktur, sondern vor allem auch die Anlagensicherheit und so mitunter komplette Produktionen.

Für die Chemieindustrie ist das Thema Cyber Security und Anlagensicherheit demnach eines, das nicht nur wettbewerbsentscheidend, sondern existenziell ist. Auch das Vertrauen in die Branche hängt in hohem Maße von der Sicherheit ihrer Anlagen ab. Hinzu kommt: Laut einer Bitkom-Studie (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien) aus dem Jahr 2018 ist die Chemie- und Pharmabranche die am stärksten betroffene in puncto Spionage, Sabotage und Datendiebstahl. Rund 74 Prozent der befragten Chemie- und Pharmaunternehmen waren von Cyberangriffen betroffen; weitere 22 Prozent vermuteten, betroffen zu sein.

Häufig werden Daten gestohlen

Dabei fand bei 23 Prozent der von Bitkom befragten Unternehmen ein Diebstahl sensibler digitaler Daten statt. Auch physische Dokumente (21 Prozent) und Endgeräte wie Notebooks oder Smartphones (32 Prozent) wurden bei den betroffenen Unternehmen entwendet. Darüber hinaus berichtete jedes dritte Unternehmen davon, dass IT-Systeme und Betriebsabläufe sabotiert worden seien. Experten sind sich einig: Industrieunternehmen, insbesondere aus der Chemie- und Pharmabranche, müssen wachsam sein und in puncto Cyber Security und Anlagensicherheit aufrüsten, um aktuellen und zukünftigen Gefahren zu begegnen. Nicht nur aus wirtschaftlichen Gesichtspunkten, sondern auch aus der Verantwortung für Mensch und Umwelt heraus. In dieser Ausgabe von ChemCologne Compact werfen wir daher einen Blick auf den aktuellen Stand der Dinge innerhalb der Branche: Wir erfahren, welche Auswirkungen Cyberangriffe auf die Unternehmen haben, durch welche Maßnahmen sich Prozessanlagen schützen lassen und welche Rolle der Mensch bei dieser Thematik spielt.

Langfristig aufstellen, Schäden vermeiden

Fakt ist: Die deutsche Wirtschaft, auch und vor allem die Chemieindustrie, führt mit zahlreichen Innovationen den Weltmarkt an. Ein Umstand, der die Branche besonders attraktiv für Cyberangriffe macht. Unternehmen, die sich beim Thema Anlagensicherheit und Cyber Security zukunftsfähig aufstellen, können vielleicht nicht jeden Ernstfall verhindern, aber sicherlich bedeutsame Schäden abmildern oder sogar ganz vermeiden. ●

Interview mit den YNCORIS IT-Experten Axel Welter und Marco Knödler

Cyber Security schon bei der Planung im Blick haben

Digitale Prozesse nehmen auch in industriellen Produktionsanlagen zu. Das hat viele Vorteile, birgt jedoch gleichzeitig potenzielle Angriffspunkte auf deren IT und OT (Operational Technology). Bei Konzepten zur IT- und OT- Sicherheit spielen Planer und Betriebsmannschaften eine entscheidende Rolle.

CCC: Herr Welter, Herr Knödler, wie haben Sie mögliche Risiken für die IT- und OT von YNCORIS identifiziert?

Axel Welter: Wir betreiben im Chemiepark Knapsack keine klassischen Chemieanlagen, sondern Strom- und Gasnetze, die für unsere Kunden unerlässlich für ihre Produktion sind. Deshalb gelten wir als kritische Infrastruktur und sind bereits seit 2018 nach ISO 27001 zertifiziert. Das war ein umfangreiches Projekt, hat uns aber geholfen, die Sicherheit unserer IT und OT strukturierter und kontrollierbar zu machen. Dazu zählen unter anderem technische Vorkehrungen, wie das Separieren von Netzen, aber auch organisatorische Maßnahmen, wie Richtlinien und Verfahrensanweisungen zur Informationssicherheit. Da wir die Zertifizierung jedes Jahr erneuern müssen, stellen wir unser Konzept immer wieder auf den Prüfstand.

CCC: Bringt eine solche Zertifizierung auch andere Betriebe weiter?

Welter: Auf jeden Fall. Während des Zertifizierungsprozesses müssen Sie mögliche Gefährdungen beurteilen. Also zum Beispiel: Wie wirkt sich ein Brand oder eine Sabotage auf einen Anlagenteil aus? Die Norm gibt zudem einen Katalog vor, der zeigt, mit welchen Maßnahmen sich solche Einwirkungen vermeiden oder deutlich einschrän- ▶

ken lassen. Die ISO 27001 ist daher aus unserer Sicht auch für Unternehmen, die nicht unter die BSI-Kritisverordnung (KritisV) fallen, ein ausgezeichnetes Instrument, um die eigene IT- und OT-Sicherheit auf den Prüfstand zu stellen.

Marco Knödler: Aus Anlass der Terroranschläge vom 11. September 2001 in den USA wurde von der Störfallkommission (SFK) der Leitfaden SFK-GS 38 „Maßnahmen gegen Eingriffe Unbefugter" auf Betriebsbereiche entsprechend der Störfall-Verordnung erarbeitet. Angriffe über die elektronische Vernetzung der Unternehmen, also „Cyberattacken", wurden auf Basis der damals gebräuchlichen Technologie für weniger gefährdend erachtet. Eine Gefährdung durch Drohnen zum Beispiel war zum Zeitpunkt der Erstellung des SFK-Leitfadens noch nicht abzusehen. Mittlerweile werden vor dem Hintergrund der technologischen Entwicklungen und der geänderten Bedrohungslage in der Kommission für Anlagensicherheit (KAS), aber auch in anderen Gremien, Anforderungen und Maßnahmen konzeptionell und inhaltlich überarbeitet und entsprechend umgesetzt. Der Leitfaden KAS 51 geht im Rahmen von "Maßnahmen gegen Eingriffe Unbefugter" auch auf Anforderungen an die IT-Security ein. Sie gibt zudem Empfehlungen wie Risiken identifiziert, analysiert und bewertet werden können.

CCC: Gibt es aus Ihrer Sicht Mindestanforderungen an die OT?

Knödler: Anlagenbetreiber müssen immer in der Lage sein, ihre Anlage sicher abzuschalten – auch im Fall eines Cyber-Angriffs und zwar selbst dann, wenn Angreifer Bedienelemente blockieren oder falsche Anzeigen generieren. Es ist daher wichtig, im Rahmen der Gefahrenabwehr- und Notfallpläne die Wirkung solcher Angriffe auf die Automatisierungstechnik zu betrachten und entsprechende Maßnahmen festzulegen.

CCC: Was sind aus Ihrer Sicht die Knackpunkte bei der Sicherheit von IT und OT?

Knödler: Es ist der Blick und die Kommunikation über den Tellerrand der eigenen Disziplin gefragt. So rücken klassische IT, Automatisierung und OT, immer näher zusammen – das tun die Kollegen aus den Fachbereichen zunehmend auch. So wie die Technik verschmilzt, müssen auch Prozesse, Methodik und die Menschen miteinander im Einklang sein.

Welter: Viele Unternehmen gehen zum Beispiel davon aus, dass sie vor Cyberangriffen geschützt sind, wenn ihre Prozessleittechnik nicht am Büro-Netzwerk angeschlossen ist. Doch auch mobile Konfigurationsgeräte oder Feldgeräte, die über drahtlose Kommunikationswege an das Prozessleitsystem angeschlossen sind, können Einfallstore für Bedrohungen darstellen.

CCC: Können Sie uns ein Beispiel nennen?

Welter: Ob Webcams oder Aufzugssteuerungen, wer sich auskennt, kann im Internet offen zugängliche Steuerungssysteme finden. Deshalb ist es so wichtig, sich detailliert Gedanken über den sicheren Betrieb unter IT- und OT-Gesichtspunkten zu machen – oder sich Rat von Experten einzuholen, um nichts zu übersehen.

CCC: Das heißt: Der Mensch ist der entscheidende Faktor?

Welter: Richtig. Ganz gleich wie viele technische und organisatorische Maßnahmen sie ergreifen, wenn Sie nicht jeden Einzelnen in Ihrem Unternehmen für IT und OT-Sicherheit sensibilisieren, bleibt immer eine Lücke, die sich Angreifer zunutze machen könnten.

Knödler: Gerade in der täglichen Arbeit des Betriebspersonals benötigen wir geschärfte Sinne für die Sicherheit – hier heißt es schulen und trainieren. Selbst in OT-Systemen, die nach bisher bewährten Verfahren geschützt sind, können erfolgreiche Angriffe nicht hundertprozentig ausgeschlossen werden. Auch wenn die Hürden für Angreifer auf PLT-Betriebs- und -Sicherheitseinrichtungen hoch sind, haben Cyber-Kriminelle schon ihre Fähigkeit dazu bewiesen. Die handelnden Menschen im Sinne der Sicherheit mitzunehmen - sowohl im Hinblick auf "Safety" als auch auf "Security", ist meiner Ansicht nach, neben robuster Technik, der maßgebliche Faktor zum Erfolg. Es gilt, sich gegenseitig zu sensibilisieren und zu informieren sowie Konzepte zu entwickeln, um im Sinne der Anlagensicherheit handlungsfähig zu bleiben und eine von einem Security-Vorfall betroffene Anlage jederzeit in einen sicheren Zustand zu bringen.

CCC: Wie stellen Sie Ihr Unternehmen für die Zukunft auf?

Knödler: Um in der Diskussion und stetig auf einem Stand der Technik zu bleiben, der der dynamischen Bedrohungslage angepasst ist, sind ein reger und enger Austausch unter Betreibern, der Dialog mit Vertretern von Behörden und unabhängigen Dritten (ZÜS); (Anm. d. Red.: Zugelassene Überwachungsstellen) sowie Dienstleistern unerlässlich. Wir möchten dies aktiv mitgestalten. Deshalb sind wir in verschiedenen Gremien und Arbeitskreisen tätig, zum Beispiel bei NAMUR und IGR. Unser Ziel ist es, mit unserer Erfahrung nicht nur die eigenen Anlagen, sondern auch die möglichst vieler Betreiber zukunftsfähig zu halten. Aktuelle Arbeitsergebnisse wie beispielsweise die gemeinsame Arbeit bei der Erstellung des NAMUR-Arbeitsblattes NA 163 und entsprechendem IT-Grundschutzprofil für Prozessanlagen des BSI zeigen den Erfolg. Wir tragen bei, für den Anwender in der Praxis Handhabbares und Umsetzbares zu beschreiben und erden uns stetig an der betrieblichen Praxis. ●

Über Axel Welter und Marco Knödler

Axel Welter ist Informationssicherheitsbeauftragter in der YNCORIS IT und hat viele Jahre Prozessleitsysteme betreut. Marco Knödler leitet den Bereich MSR-Technik bei YNCORIS. Er engagiert sich in Gremien wie Interessengemeinschaft Regelwerke Technik (IGR) und NAMUR für mehr „Sicherheit" im Sinne von "Security" (Informationssicherheit) und "Safety" (Anlagensicherheit).

VTU: Cyber Security in Prozessanlagen

Neue Gefahren erfordern neue Strukturen: Prozessleitsysteme sicher erneuern

Angriffe auf die Steuerungsebene von Produktionsbetrieben, wie sie jüngst bei namhaftem Unternehmen stattgefunden haben, verursachen Gefahren und kostenintensive Produktionsausfälle. Um solche Szenarien künftig zu vermeiden, sind Unternehmen und deren Engineering-Partner gefordert, sich intensiv mit dem Thema Cyber Security in Bezug auf Prozessanlagen auseinanderzusetzen.

Blickt man zurück auf die Prozessleitsysteme der 90er und 00er-Jahre, war die Gefahr noch überschaubar: Der Aufbau dieser vorigen Generationen von Netz- und Informationssystemen war meist herstellergebunden. Selten waren direkte Schnittstellen zwischen Produktionsanlagen und IT-Landschaft vorhanden; Cyber-Angriffe beschränkten sich somit auf die Büro-IT. Heute, Jahrzehnte später, sorgen die voranschreitende Digitalisierung, eine wachsende Automatisierungstiefe sowie das Industrial Internet of Things (IIoT) dafür, dass Information Technology (IT) und Operational Technology (OT) wesentlich stärker vernetzt sind. „Das bietet zwar viele Möglichkeiten, erhöht parallel aber auch die Auswirkungen von Angriffen auf die Steuerungsebene", weiß Stefan Müllner, Senior EI&C Engineer bei der VTU Engineering GmbH. „Dies bringt einige Herausforderungen bei der Erneuerung von Prozessleitsystemen mit sich."

Herausforderung Cyber-Security

Über VTU Engineering

VTU Engineering erarbeitet gemeinsam mit der IT- und Betriebsmannschaft in Unternehmen ein ganzheitliches Cyber-Security-Konzept und unterstützt zusätzlich mit ressortübergreifender Kompetenz aus Automations-, Elektrotechnik-, Mess- und Regeltechnik bei der Automatisierung von Prozess- und Fertigungsanlagen. Die Sicherstellung der Produktionsverfügbarkeit spielt dabei in Planung und Umsetzung von der Feldebene über SPS und Prozessleitsystemen bis hin zu Manufacturing Execution Systems (MES) eine wesentliche Rolle.

Enge Zusammenarbeit zwischen IT und OT ist erforderlich

Sind Prozessleitsysteme (PLS) am Ende ihres Lebenszyklus angekommen, werden sie gegen neue getauscht. Für eine erfolgreiche Erneuerung und im Anschluss den sicheren Betrieb eines PLS muss schon zu Beginn eines Migrationsprojekts überlegt werden, wie die Organisation hinter den Security-Maßnahmen aussehen soll. Die Verantwortung kann und darf dabei nicht ausschließlich bei der IT-Abteilung liegen, sondern muss auf OT-Fachkräfte ausgeweitet werden. Nur durch die enge Zusammenarbeit zwischen IT und OT können Prozessleitsysteme langfristig gegen Gefahren abgesichert werden.

„Nicht nur die ausführenden Systemintegratoren sollten über ein umfassendes Sicherheitsbewusstsein verfügen. Auch dem Bedien- und Wartungspersonal muss dieses, falls nicht vorhanden, durch Schulungen vermittelt werden", so Müllner.

Hardware: Sichere Systemarchitektur durch Segmentierung

Zur Erreichung der Security-Anforderungen spielt der Detailvergleich von Hard- und Softwarekomponenten marktführender PLS-Hersteller eine fast schon untergeordnete Rolle. Viel wichtiger sind individuelle Vernetzung und Umsetzung durch den Engineering-Partner unter Beachtung der spezifischen Kundenanforderungen. „Ein versierter Partner sollte bei der Auslegung des Gesamtsystems potentielle Angriffsstellen sowie die Ausbreitungsmöglichkeiten innerhalb des Systems auf ein Minimum reduzieren, trotzdem aber auch alle gewünschten Daten komfortabel zur Verfügung stellen können", erklärt Müllner die Vorgehensweise. Durch die Seg- ▶

mentierung der Systeme, den Einsatz von Firewalls und weiterer aufeinander abgestimmte Sicherheitsebenen können Gefahren eingedämmt werden. Redundante Systeme bei Servern und Prozessormodulen sorgen dafür, dass beim Ausfall des einen Hardware-Systems ein anderes dessen Aufgaben ohne Verzögerung übernehmen kann.
Müllner: „Darüber hinaus ist es sinnvoll, eine eigene Simulationszone in die Architektur aufzunehmen. Darin lassen sich neue Softwarekomponenten, Patches und Updates vorab und ohne Einfluss auf das Produktivsystem testen."

Software: Virenscan und Datensicherung für die Prozessanlage

Für die größtmögliche Cyber Security sollte neben den eigentlichen Softwarepaketen des Prozessleitsystems auch eine Anti-Schadsoftware installiert werden. Um Wartungsfreundlichkeit zu garantieren, sind dabei Lösungen zu bevorzugen, bei denen alle Installationen zentral aktualisiert werden können – und zwar ohne dabei direkte Verbindungen zu Updateservern im Internet herzustellen. „Denn auch solche Verbindungen", weiß Müllner „bieten Einfallstore für eine Vielzahl von Angriffen." Zur lückenlosen Erfassung von Änderungen an jeglicher installierten Software eignet sich ein Versionierungs-Tool.
Darüber hinaus sollte ein geeigneter Prozess zur Datensicherung und Wiederherstellung implementiert werden, der idealerweise statische als auch dynamische Daten sichert. Sicherheitsrelevante Benutzereingriffe, unsichere Zustände und Angriffe müssen protokolliert werden können. Um der steigenden Komplexität der zu definierenden Rollen – beispielsweise Administrator, Supervisor und Operator – der entsprechenden Rechtevergabe und Passwörter zu begegnen, sollte laut Müllner zudem ein zentrales User-Management etabliert werden.

Ganzheitliche Dokumentation und Budgetierung

Unternehmen müssen zudem von Beginn des Migrationsprojektes an beachten, dass sich die Security-Aufgabenpakete über die gesamte Lebensdauer des PLS erstrecken. Es gilt, diese vorsorglich nicht nur für die Migration, sondern auch für den laufenden Betrieb des Systems zu budgetieren.
Abschließend rundet eine Dokumentation zusätzlich zu den ordnungsgemäßen Bestandteilen einer Prozessanlage das Security-Konzept ab – inklusive der Definition unterschiedlicher Sicherheitsebenen, Netzwerkteilnehmer, Schnittstellen, Portlisten und Patch-Managements.
VTU-Engineer Stefan Müllner unterstreicht vor diesem Hintergrund: „Auch ein systematisch beschriebenes Desaster-Recovery-Konzept in einer Art ‚Was wäre wenn?'-Stil ist ein absolutes ‚Must have' im Rahmen eines umfassenden Security-Konzepts." ●

TÜV Rheinland über die reale Bedrohung durch Cyberattacken

Prozessindustrie im Visier der Hacker

Die funktionale Sicherheit in der chemischen Prozessindustrie nimmt einen hohen Stellenwert ein. Dabei geht es weniger um die Verfügbarkeit von Anlagen, sondern vielmehr um eine Sicherstellung der Integrität des Produktionsprozesses. Manipulationen oder Fehlfunktionen dürfen Mensch und Umwelt unter keinen Umständen gefährden. Der Cyberspace wächst mit der physikalischen Welt zusammen und Computersysteme steuern Produktionsanlagen. Somit haben Hackerangriffe zunehmend negative Folgen für die Sicherheit dieser Anlagen.
Viele Unternehmen sind nicht auf die wachsende Bedrohung durch Cyberattacken vorbereitet.

Ist das Chaos nur ein paar Mausklicks entfernt?

Bereits 2012 beschrieb der österreichische Schriftsteller Marc Elsberg in seinem Roman „Blackout" die Folgen eines flächendeckenden Stromausfalls in ganz Europa, hervorgerufen durch einen einfachen Hackerangriff. Cyberattacken verbinden viele Menschen mit Dystopien. „Wir müssen uns den großen Knall gar nicht ausmalen, um auf die Ge- ▶

VERSTEHEN. DURCHDENKEN. LÖSEN.

Ob Einzellösung oder komplexes Anlagenprojekt: Wir hören Ihnen aufmerksam zu, analysieren Ihre Anforderungen bis ins Detail und unterstützen Sie genau so, wie Sie es brauchen. So sichern wir Ihre Produktion, heben Ihre verborgenen Potenziale und begleiten Sie in eine erfolgreiche Zukunft – engagiert, effektiv, effizient. Damit Ihre Chemie immer stimmt. **Always at your site.**

YNCORIS
Industrial Services

www.yncoris.com

► fahren für Staaten, Infrastrukturen und Unternehmen hinzuweisen. Sie sind schon längst real", sagt Wolfgang Kiener, Cybersecurity Experte bei TÜV Rheinland. 2005, vor über 15 Jahren, standen weltweit Anlagen in 13 vernetzten Daimler-Chrysler-Werken still und 50.000 Fabrikarbeiter konnten nicht mehr arbeiten – angegriffen von einem Wurm. 2010 fand der unter‚Stuxnet' bekannte Angriff auf iranische Atomanlagen statt. Vor zwei Jahren legten Hacker Maersk, die größte Containerschiffreederei der Welt aus Belgien, still. Der Schaden betrug rund 300 Millionen Euro, Umsatz und Aktienkurs wurden nachhaltig negativ beeinflusst.
Im April 2019 wurde bekannt, dass der Dax-Konzern Bayer bereits 2018 Opfer eines zielgerichteten Spionageangriffs war. Kurz darauf, im Juli 2019, dann die Meldung, dass unter anderem Großkonzerne wie BASF, Siemens und Roche, Opfer von Industriespionage durch einen Cyberangriff waren.

„Die Bedrohungen nehmen zu, und die Gefahr von Cyberangriffen auf Prozessanlagen und kritische Infrastrukturen steigt."

Die genannten Angriffe stellen nur einen kleinen Ausschnitt dar. Bedeutender ist die tendenzielle Entwicklung: Von einem Wurm, der durch Zufall in 13 Werken zu Ausfällen führt, bis hin zu Cybercrime, Spionage, Terrorismus und Cyberwar. „Es geht nicht darum, Angst zu schüren. Aber Unternehmen sollten handeln. Die Bedrohungen nehmen zu und die Gefahr von Cyberangriffen auf Prozessanlagen und kritische Infrastrukturen steigt", weiß Wolfang Kiener. Im Schnitt dauert es heute rund 200 Tage bis ein Unternehmen einen Angriff überhaupt erkennt. Und je länger es dauert, eine Bedrohungslage zu identifizieren und entsprechend zu reagieren, desto größer wird der Schaden.

Cyberrisiken für Industrieanlagen weltweit unterschätzt

Ein wesentlicher Angriffspunkt für Cyberattacken ist Operational Technology (OT), also Computersysteme, die Motoren, Ventile, Pumpen, Ampeln, Stromnetze und ganze

Steuerung der Prozesse über Computersysteme

Industrieanlagen steuern. Auch ältere, Maschinen und Anlagen, die ursprünglich gar nicht dafür ausgerichtet waren, vernetzt zu werden, sind nun mit dem Internet direkt oder indirekt verbunden. Dadurch entstehen Schwachstellen. In einer weltweiten Studie zur Cybersicherheit in Industrieanlagen, die TÜV Rheinland zusammen mit dem unabhängigen Marktforschungsunternehmen Ponemon Institute durchgeführt hat, wurden 2.200 Fachleute für Cybersicherheit aus den Branchen Automobil, Gesundheit und Pharma sowie Logistik und Verkehr, Maschinenbau, Öl und Gas zum Stand der industriellen Sicherheit befragt. Eines der Hauptergebnisse: Die Cyberrisiken für Industrieanlagen werden weltweit unterschätzt. Zudem fehlt es an einem ganzheitlichen Blick auf die Sicherheit von Industrieanlagen. Wie sehr Cyberrisiken OT-Systeme gefährden, zeigen diese beispielhaften Ergebnisse:

- Mehr als die Hälfte der Befragten (57 Prozent) sagt, dass ihre Unternehmen fest mit Angriffen auf die OT-Systeme rechnen.
- Knapp die Hälfte (48 Prozent) sind überzeugt, dass Cyberbedrohungen für OT-Systeme ein größeres Risiko als für die IT-Umgebung darstellen.
- Fast zwei Drittel (63 Prozent) der Befragten geben an, dass in ihren Unternehmen die Sicherheitsmaßnahmen für IT- und OT-Systeme nicht aufeinander abgestimmt sind.
- Für knapp die Hälfte der Befragten (47 Prozent) haben die Cyberbedrohungen von OT-Systemen im vergangenen Jahr zugenommen. Dabei geht es um Angriffe wie Phishing, Social Engineering und Erpressersoftware, sogenannte Ransomware.

OT-Security erfordert strukturelle Veränderung

„Viele Firmen wissen, dass sie in der Absicherung ihrer Anlagen hinterherhinken und wollen aufholen", ist sich Wolfgang Kiener sicher. Die wichtigste Hürde ist die Veränderung der Strukturen. Momentan liegt die Verantwortung für OT-Security häufig noch in der IT-Abteilung. Dabei ist Operational Technology ein eigenständiger Bereich, der ein eigenes Budget und Expertentum verlangt. Ziel muss es immer sein, einen Angriff möglichst schnell zu entdecken und entsprechend darauf reagieren zu können", so Kiener.
Industriespionage, Erpressung oder einfach Sabotage: Es gibt viele Motive für solche Angriffe. Funktionierende Schutzvorkehrungen geben zwar keine hundertprozentige Sicherheit, können den einen Blackout im Ernstfall aber mit höherer Wahrscheinlichkeit verhindern. ●

Schülerwettbewerb „Meine Position ist spitze!“ 2020

Ungetrübte Freude trotz Corona

2020 findet er bereits zum sechsten Mal statt: der Schülerwettbewerb „Meine Position ist spitze!“, initiiert von ChemCologne. 21 Schülerinnen und Schüler ab 16 Jahren bekommen die Möglichkeit, den Arbeitsalltag von Führungskräften aus den ChemCologne Mitgliedsfirmen kennenzulernen und für einen Tag im Chefsessel zu sitzen. Dabei war in diesem Jahr alles ein wenig anders, denn aufgrund der Corona-Bestimmungen konnten noch nicht alle geplanten Aktionstage stattfinden. Auch das Auftakttreffen fand nicht persönlich, sondern virtuell statt. Die Gewinnerinnen und Gewinner der diesjährigen Aktion ließen sich ihre Vorfreude aber nicht nehmen und befanden „Meine Position ist spitze!“ als „einmalige Gelegenheit“.

Knapsack: Vier Schüler im Chefsessel

Chefin im Chempark Krefeld

Im Chempark Krefeld durfte die 16-jährige Sila Cakir den Posten von Chempark Leiter Lars Friedrich übernehmen und war damit für einen Standort mit über 8.000 Mitarbeitern zuständig. Mit dem Chef der Werkfeuerwehr besprach sich die Schülerin zu Investitionen in neue Fahrzeug-Stellflächen. Im Anschluss stand die Besichtigung des umgebauten Ausbildungszentrums auf dem Terminplan. Nachmittags übergab sie auf einer Pressekonferenz eine Spende an ein Theaterprojekt der Edith-Stein-Schule. Ein spannender Tag für die 16-Jährige. Lars Friedrich freute sich über die Möglichkeit, „Interesse für einen Beruf in der chemischen Industrie zu wecken“.

Umweltschutz-Chef bei Shell

Sven Breuer aus Bornheim übernahm bei der Shell Rheinland Raffinerie die Leitung der Umweltschutzabteilung und des Gewässerschutzes. Nach einer Sicherheitsunterweisung bekam der 17-jährige Schüler symbolisch den Schlüssel von Umweltschutz-Chef Dr. Frank Beyer übergeben. Zu Svens Aufgaben zählten unter anderem ein Anlagenrundgang, die Prüfung von Betreiberpflichten sowie die Entnahme einer Grundwasserbeprobung. Durch den Tag bei Shell habe sich sein Plan gefestigt, ein mathematisch-naturwissenschaftliches Studium aufzunehmen.

Laborleiterin bei LANXESS in Dormagen

Die 17-jährige Schülerin Fernur Tekgül übernahm für einen Tag die Leitung eines Entwicklungs-Labors von Elisabeth Gau bei LANXESS. Nach einer kurzen Begrüßung widmete sie sich ihren neuen Aufgaben: einer Laborbesprechung mit Probennahme

Sila Cakir (2. v.l.) überreicht Spenden als Chempark-Leiterin in Krefeld

und einem Rundgang durch den Betrieb. Zudem lernte sie die Produktanforderungen sowie die einzelnen Arbeitsabläufe von Chemikanten und Laboranten kennen. „Gar nicht so einfach, noch einmal zurück in die Schule zu gehen, wenn man schon einmal auf dem Chefsessel saß“, sagte Tekgül am Ende des Tages.

Vier Schüler an der Spitze im Chemiepark Knapsack

Auch im Chemiepark Knapsack konnten vier Schülerinnen und Schüler für einen Tag wichtige Führungspositionen übernehmen. Stella Nohr erlebte bei Yncoris hautnah, welche Herausforderungen und Aufgaben Thomas Sengelmann als Personalleiter zu bewältigen hat. Die Schülerin entwickelte unter anderem ein Rekrutierungskonzept. Bei CABB in Hürth übernahm der 17-jährige Ibrahim Erdem die Rolle von Betriebsleiter Jürgen Bruck und nahm Termine wie eine Produktionsbesprechung wahr. Marco Mencke, Geschäftsführer der Rhein-Erft Akademie, räumte den Chefsessel für Klara Weth aus Kerpen. Die Schülerin war begeistert von der Offenheit, mit der ihr die Kollegen begegneten. Der 16-jährige Konrad Schick wurde in seiner Rolle als Standortleiter bei Bayer Crop Science, eigentlich der Job von Dr. Frank Zurmühlen, gleich am Morgen mit der Moderation eines Führungstreffens betraut. Für ihn war der Tag „eine interessante Möglichkeit, ein Stück Wirklichkeit kennenzulernen“. ▶

► Geschäftsführerin bei INEOS in Köln

Claire Dollhausen nahm bei INEOS in Köln den Platz von Dr. Axel Göhrt als Geschäftsführerin Produktion und Technik ein. Er ist unter anderem für die Sicherheit am Standort und den Anlagenbetrieb zuständig. So übernahm seine Stellvertreterin für einen Tag seine Teilnahme an Meetings und erhielt bei einer Werkrundfahrt einen Überblick über die Produktionsanlagen. „Ich durfte mich bei den Besprechungen selbst einbringen", freute sich die Schülerin. Dr. Göhrt: „Wir beteiligen uns gerne an dieser Aktion von ChemCologne, da sie jungen interessierten Menschen eine gute Gelegenheit bietet, einen Einblick in die Abläufe unseres Unternehmens zu erhalten."

Claire Dollhausen

Fokussiert auf den Nachwuchs – auch in Krisenzeiten

Auch wenn diese Beispiele nur stellvertretend für alle Teilnehmerinnen und Teilnehmer der Aktion „Meine Position ist spitze!" in 2020 stehen, so wird deutlich: Auch in Krisenzeiten verlieren die Unternehmen der Chemiebranche das Thema Nachwuchskräfte nicht aus dem Blick.
„Wir sind allen Schülerinnen und Schülern sowie den teilnehmenden Unternehmen dankbar für ihre Flexibilität und ihr Engagement", so ChemCologne-Geschäftsführer Daniel Wauben. „Ein gemeinsames, positives Signal in der Krise." ●

ChemCologne initiiert „Chemtelligence"

Neue Online-Plattform im Open-Innovation-Format soll den Innovationsprozess in der Chemiebranche beschleunigen

Schon seit einigen Jahren fungiert ChemCologne in Zeiten des Wandels als Treiber für Brancheninnovationen. Vernetzungen und Kooperationen sind dabei ein entscheidendes Kriterium bei Lösungsfindungen. Was vor Jahren mit dem „ChemCologne Kooperationstag" als Netzwerk-Veranstaltung für Studierende und Unternehmen der Chemiebranche an Hochschulen begann, hat sich seit 2017 zunehmend zu einer intensiven Zusammenarbeit mit Start-ups weiterentwickelt. Diese erhalten die Möglichkeit sich mit neuen und visionären Lösungsansätzen den etablierten Unternehmen der Chemiebranche vorzustellen und so ihre Kunden von morgen kennenzulernen. Denn die Chemieunternehmen suchen zunehmend externe Lösungsanbieter, um an ihrer Wettbewerbsfähigkeit zu arbeiten. Dabei ist die Zusammenarbeit mit Start-ups ein wichtiger Baustein und der Kooperationstag eine gute Gelegenheit, um auf der Suche nach neuen Impulsen für das eigene Unternehmen fündig zu werden. Die Veranstaltungsreihe war in den vergangenen Jahren der Startpunkt zahlreicher Kooperationen und Projekte.
Seit 2018 prämiert ChemCologne zusätzlich erfolgreiche Aktivitäten von Start-ups mit dem „Chem Start-up-Award". Die Themenschwerpunkte sind dabei so vielfältig wie die Herausforderungen, welche die Chemieindustrie umtreiben – darunter Kreislaufwirtschaft, digitale Produktion, Biotechnologie und neue Materialien.

CHEMTELLIGENCE

Um auf diese konkreten Herausforderungen der Chemieunternehmen zukünftig noch effektiver einzugehen, hat ChemCologne nun das Open-Innovation-Format „Chemtelligence" initiiert. In diesem Rahmen werden Challenges der Unternehmen identifiziert und auf einer Online-Plattform sichtbar gemacht. Dort können sich Lösungsanbieter – wie Start-ups, Studierende, Forscher, Wissenschaftler oder Experten – für die jeweiligen Themen bewerben, gemeinsam mit den Unternehmen an neuartigen Prozessen arbeiten und so Mehrwerte schaffen.

Motor für innovative Lösungen

„Diese Verknüpfung von internem Wissen mit externer Expertise fördert einmal mehr die Innovationskraft der rheinischen Chemieunternehmen. Unser Ziel ist es, den Status des Rheinlands als führende Chemie-Region in Europa auf diesem Wege weiter zu untermauern", sagt ChemCologne-Geschäftsführer Daniel Wauben und unterstreicht: „Mit ‚Chemtelligence' unterstützt ChemCologne die Chemieunternehmen der Region mit einer zusätzlichen Facette dabei, Innovationspotenziale zu heben und Transformationsprozesse für eine erfolgreiche Zukunft anzustoßen." ●

Innovationsmotor ChemLab endet – Nachfolgeprojekte Industry Hub und Smart Industrial City nehmen Fahrt auf

Herausforderung gemeinsam meistern

Mit einem hochkarätigen Plenum und spannenden Einblicken in Innovations- und Digitalisierungsthemen beendete das ChemLab seine 2,5-jährige Projektlaufzeit. Während dieser Tage reihenweise Veranstaltungen Corona-bedingt abgesagt werden müssen, hatten die Veranstalter vom Rhein-Kreis Neuss, der Stadtmarketing- und Wirtschaftsförderungsgesellschaft Dormagen (SWD) und des CHEMPARK-Betreibers Currenta bei ihren Planungen von Anfang an auf ein hybrides Veranstaltungsformat gesetzt.

275 Zuschauer per Live-Stream

So konnten am 23. November neben den 20 Protagonisten in der Nordhalle Zons 275 Zuschauer per Live-Stream an der Veranstaltung teilnehmen und miterleben, wie CHEMPARK-Leiter Lars Friedrich ein positives Resümee für die Currenta und die chemische Industrie zog: „Für uns als CHEMPARK ist Digitalisierung neben der stofflichen und industriellen Nutzung von erneuerbaren Energien eines der wichtigsten Zukunftsthemen. Chemische Industrie und digitale

Lars Friedrich mit positivem Resümee

Gründerszene liegen nach zweieinhalb Jahren ChemLab näher beieinander. Und auch wir als CHEMPARK konnten von den zahlreichen Impulsen für mehr Digitalisierung in der Chemie, die aus dem ChemLab kamen, profitieren."

In einer von Anja Backhaus moderierten Runde mit NRW-Wirtschafts- und Digitalminister Prof. Dr. Andreas Pinkwart, dem Covestro-Vorstandsvorsitzenden Dr. Markus Steilemann, RWTH-Universitätsprofessorin Prof. Dr. Gabriele Gramelsberger sowie Christoph Goertz, Innovationsberater und Unternehmer mit Silicon Valley-Erfahrung entwickelte sich eine spannende Diskussion zur Vision des Rheinland Valleys mit den Chemie- und Industrie-Schwerpunkten in Dormagen und im Rhein-Kreis Neuss. Wirtschafts- und Digitalminister Pinkwart lobte: „Damit die Industrie aus der Corona-Krise gestärkt hervorgeht, müssen wir Innovationen und Investitionen auf den Weg bringen – in neue Technologien, in die Qualifikation und in die Weiterbildung der Beschäftigten. In Dormagen zeigt die Chemiebranche beispielhaft, wie es gehen kann: Durch eine enge Zusammenarbeit zwischen Stadt, etablierten Unternehmen und innovativen Start-ups stellt sich die Region für eine erfolgreiche Zukunft auf."

Hans-Jürgen Petrauschke, Landrat des Rhein-Kreises Neuss, kommentierte zum ChemLab-Nachfolgeprojekt Industry Hub: „Innovationen benötigen ein Umfeld, in dem sie entstehen können und ein Netzwerk aus Unternehmen, Startups und anderen Akteuren, um sie voranzubringen. Mit dem Projekt Industry Hub möchten wir die digitale Transformation weiter in den Unternehmen stärken, um damit einen Beitrag zu leisten unsere Wirtschaft im Strukturwandel zukunftsfähig zu machen."

Und Dormagens Bürgermeister Erik Lierenfeld verwies auf die aktuellen Planungen der Stadt zum Projekt Smart Industrial City: „Der Verweis auf die Herausforderungen unserer Wirtschaft reicht uns nicht. Daher haben auch wir uns als Stadt Dormagen auf den Weg gemacht, um Deutschlands erste Smart Industrial City zu werden. Mit dem Digitalen Zwilling, dem Digitalen Bauantrag und dem Einsatz von KI im Bereich der Mobilität möchten wir nun auch die ersten Verbesserungen für unsere Bürger und Unternehmen erzielen. Die SWD wird daher nun kontinuierlich die digitalen Standortfaktoren weiter ausbauen und gezielte Akzente beim Thema Nachhaltigkeit setzen."

Weitere Infos und Live-Stream unter: www.chemlab-nrw.de ●

ChemHub Knapsack ausgezeichnet

Der Aufsichtsrat der Zukunftsagentur Rheinisches Revier (ZRR) hat 20 von insgesamt 82 Projekten aus dem »Sofortprogramm PLUS« mit einem zweiten von drei Sternen ausgezeichnet – unter anderem den ChemHub Knapsack als eines von fünf Projekten aus dem Rhein-Erft-Kreis. Damit gilt der ChemHub Knapsack als „tragfähiges Vorhaben".

Der ChemHub soll in Form eines Forschungszentrums am Industriehügel in Hürth-Knapsack umgesetzt werden. Inmitten der bestehenden Industrie soll zu den Themen Power-to-X- Technologien, Biomasse und chemisches Recycling geforscht werden, mit dem Ziel, innovative Verfahren im industriellen Umfeld zu etablieren.

Die Auszeichnung mit einem dritten Stern verleiht der Aufsichtsrat des ZRR, sobald bei der Bundes- oder Landesregierung ein möglicher Förderzugang identifiziert werden kann. Erst dann gilt ein Projekt als „Zukunftsprojekt des Strukturwandels im Rheinischen Revier" und ist bewilligungsreif. ●

Susan-Stefanie Breitkopf übernimmt die Funktion der Arbeitsdirektorin

Neue Geschäftsführerin bei Currenta

Das Geschäftsführerteam beim Chempark-Manager und -Betreiber Currenta GmbH & Co. OHG in Leverkusen wird ab sofort erweitert: Susan-Stefanie Breitkopf – seit drei Jahren als Personalleiterin im Unternehmen – ergänzt das Duo um den Vorsitzenden der Geschäftsführung Günter Hilken und Frank Hyldmar. Die 52jährige Arbeitsrechtlerin mit langjähriger Erfahrung im Bereich Human Resources übernimmt die Funktion der Arbeitsdirektorin. In dieser Funktion tritt sie die Nachfolge von Pieter Wasmuth an, der das Unternehmen am 30. September 2020 verlassen hat, um neue berufliche Herausforderungen als Berater beim Currenta-Eigentümer Macquarie Infrastructure Real Assets (MIRA) zu übernehmen. Die gebürtige Hamburgerin Breitkopf absolvierte in ihrer Heimatstadt ein Studium der Rechtswissenschaft und war nach einer langjährigen Selbständigkeit als Fachanwältin für Arbeitsrecht elf Jahre lang in verschiedenen Positionen für Lanxess und anschließend zwei Jahre für Covestro tätig. Jetzt freut sich die verheiratete Mutter zweier Töchter auf ihre neue Aufgabe: „in meiner Zeit als Personalleiterin habe ich Currenta als ein hochinteressantes Unternehmen mit einem vielfältigen Spektrum an Dienstleistungen in den unterschiedlichsten Bereichen kennengelernt. Ich freue mich sehr auf die weitere Zusammenarbeit mit den Menschen hier und hoffe, dass ich mit meiner Erfahrung zum weiteren Erfolg des Unternehmens beitragen kann." ●

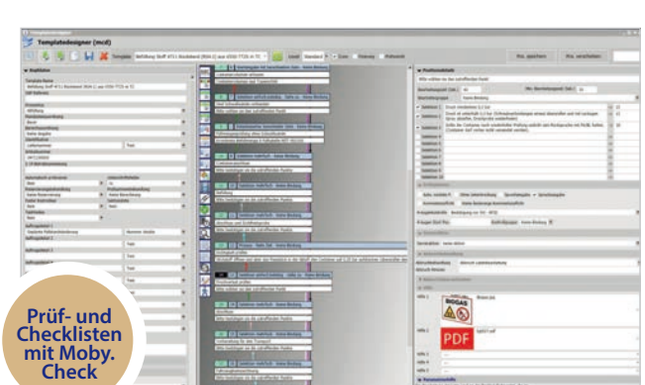
Susan-Stefanie Breitkopf

Softwarelösung Moby.Check: Prüf- und Checklisten werden digital

Siemens und Log.Go.Motion kooperieren

Siemens und der Spezialist für die Digitalisierung von Prozessen in Industrie und Logistik Log.Go.Motion haben einen Kooperationsvertrag geschlossen. Ab sofort wird Siemens die Softwarelösung Moby.Check exklusiv als Drittanbieter innerhalb der Prozessindustrie weltweit vertreiben. Mit Moby.Check können individuelle digitale Prüf- und Checklisten für Wartungs- und Instandhaltungsmaßnahmen sowie für Produktions- und Logistikabläufe erstellt, gesteuert und überwacht werden. Das Softwaresystem wurde für den industriellen weltweiten Einsatz entwickelt.

Moby.Check verfügt über eine einfache Navigation und ein flexibles Berechtigungskonzept. Auf einer individuell einstellbaren Oberfläche erstellt der Anwender am PC entsprechend seinen Anforderungen individuelle Prüf- und Checklisten ohne Programmieraufwand für die mobile Wartung und Instandhaltung. Templates und Schnittstellen zur Datenversorgung der Prüf- und Checklisten reduzieren mögliche Fehler und der Aufwand für die Erfassung von Daten entfällt. Ob Einzel- oder Mehrfach-Auswahl, Eingabe mit oder ohne Wertprüfung, ob freie oder vorgegebene Reihenfolge, Berechnungen oder Verzweigungen, der Anwender entscheidet, wie seine Prüfungen ablaufen sollen. „Wir freuen uns über die Partnerschaft mit Log.Go.Motion. Die Funktionssoftware Moby.Check ist ein weiterer Baustein im Siemens-Portfolio und unterstützt Anwender in der Prozessindustrie einfach und flexibel bei der digitalen Transformation", sagt Eckard Eberle, CEO Process Automation, Siemens AG. Und Dirk Emmerich, CEO Log.Go.Motion GmbH, erklärt: „Die Partnerschaft mit Siemens ermöglicht es, unser innovatives Softwareprodukt Moby.Check bei Kunden weltweit einzusetzen und passende Roll-Out-, Pflege- und Update-Services in zahlreichen Ländern vor Ort zu bieten. Hier ergänzen sich die Vorteile eines agilen und innovativen Start-ups mit der globalen Präsenz und Erfahrung von Siemens in der Prozessindustrie und Automatisierung." ●



Prüf- und Checklisten mit Moby. Check

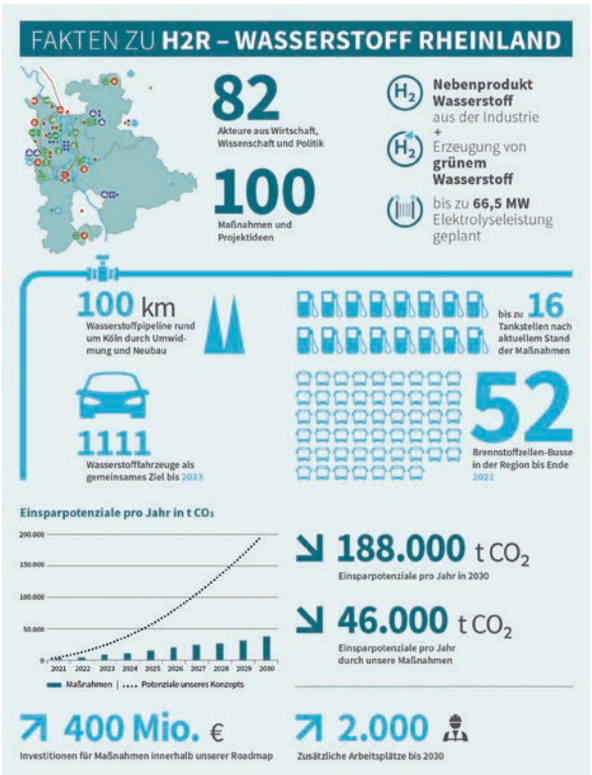
Digitalkonferenz informierte über aktuelle Wasserstoffaktivitäten im Rheinland

Schlüsselelement Wasserstoff

Im Rahmen einer großen Onlinekonferenz organisiert von KölnBusiness, der TH Köln und dem Netzwerk HyCologne – Wasserstoff Region Rheinland e.V. wurden Ende Oktober aktuelle Wasserstoffaktivitäten in der Region vorgestellt. Rund 300 Teilnehmer(innen) informierten sich im digitalen Format „Wasserstoff im Rheinland – Status und Perspektive" über die Entwicklungschancen des klimafreundlichen Energieträgers. Dabei zeigte sich: Die Region ist Pionier, wenn es um die Erzeugung, Verteilung, Nutzung und Expertise von Wasserstoff (H2) geht. Vom Abfallsammelfahrzeug, Gabelstapler oder Lkw mit Brennstoffzellenantrieb bis hin zum H2-betriebenen Blockheizkraftwerk – die Region Rheinland hat ein umfassendes Maßnahmenpaket zur Stärkung der Wasserstoffwirtschaft erarbeitet.

Nachhaltige Wasserstoffinfrastruktur

An der Konferenz beteiligt waren neben den Organisatoren die EnergieAgentur.NRW, das Kölner Ingenieurbüro EMCEL, INEOS, Shell, das Deutsche Zentrum für Luft- und Raumfahrt (DLR), Thyssengas, Regionalverkehr Köln (RVK), die Hochschule Bonn-Rhein-Sieg, das Forschungszentrum Jülich, die Handwerkskammer zu Köln sowie die Nationale Organisation Wasserstoff- und Brennstoffzellentechnologie (NOW). In Vorträgen und Paneldiskussionen ging es unter anderem um die Nutzung von Wasserstoff, der als Nebenprodukt in der chemischen Industrie anfällt sowie um grünen Wasserstoff oder um den Aufbau von Infrastrukturen zur H2-Verteilung. In diesem Rahmen wurde auch die Roadmap der Initiative „H2R Wasserstoff Rheinland" präsentiert, die dem weiteren Ausbau der Wasserstoffwirtschaft in der Region dient. Die Roadmap weist den Weg für den Aufbau einer nachhaltigen Wasserstoffinfrastruktur bis ins Jahr 2035 und ist Bestandteil eines Konzeptes, das die Städte Brühl, Hürth, Köln und Wesseling sowie der Rheinisch-Bergische Kreis und der Rhein-Sieg-Kreis gemeinsam mit einem Expertenteam sowie mit breiter Unterstützung aus Wirtschaft, Wissenschaft, Kammern und Verbänden entwickelt haben. Das umfangreiche Konzept enthält rund einhundert Maßnahmen und Projekte, die von rund 80 Wasserstoff-Akteuren eingebracht wurden. Das Ziel der Initiative: Wasserstofftechnologien – insbesondere im Mobilitätsbereich – in die Phase der Markteinführung zu bringen. Damit unterstützt die Initiative auch die Anfang Juni 2020 veröffentlichte Nationale Wasserstoffstrategie der Bundesregierung. Die darin enthaltenen 38 Maßnahmen sollen Wasserstofftechnologien als Kernelemente der Energiewende etablieren.



Zentraler Baustein

„Wasserstoff ist ein zentraler Baustein zur erfolgreichen und nachhaltigen Transfor- ▶

mation der Sektoren Industrie, Energie und Verkehr", sagt Dr. Manfred Janssen, Geschäftsführer der KölnBusiness Wirtschaftsförderung. „Unsere Konferenz hat deutlich gemacht, dass wir dank der gemeinsamen Roadmap über einen geeigneten Instrumentenkasten für die damit verbundenen Aufgaben verfügen: Die Region hat eine optimale Grundlage für den weiteren Aufbau einer umfassenden Wasserstoffwirtschaft geschaffen. Das gilt es nun weiter voranzutreiben, um den Innovationsstandort nachhaltig zu stärken."

Neben der konkreten Unterstützung der einzelnen Akteure seitens KölnBusiness, soll das Format der Onlinekonferenz nun regelmäßig, mindestens einmal im Jahr, wiederholt werden. Dazu Dr. Frank Benzel vom Netzwerk HyCologne – Wasserstoff Region Rheinland: „In der Region wird seit mehr als zehn Jahren Pionierarbeit geleistet. Dabei war die erfolgreiche Zusammenarbeit unserer Mitglieder ein wesentlicher Erfolgsfaktor. Mit einer stetigen Erweiterung unseres Netzwerkes sowie mit überregionalen Kooperationen und Formaten wie der Onlinekonferenz wollen wir dazu beitragen, dass wir unsere Pionierrolle auch in Zukunft so weiterführen."
Welchen Beitrag Forschung und Lehre zur zukünftigen Gestaltung einer Wasserstoffwirtschaft leisten, unterstreicht Prof. Dr. Thorsten Schneiders vom Cologne Institute for Renewable Energy der TH Köln: „Das Knowhow im Rheinland ist einzigartig. Über einen Wissens- und Technologietransfer forcieren wir Entwicklungsfortschritte gemeinsam und tragen so dazu bei, Wasserstoff als Schlüsselelement zur Energiewende zu etablieren." ●

Shell will Geschäft umbauen und unterzeichnet Absichtserklärung mit dem Land NRW

Gemeinsam die Energiewende gestalten

Shell will sein Geschäft in Deutschland mit fortschreitender Energiewende umbauen. Das kündigte der Vorsitzende der Geschäftsführung der Deutsche Shell Holding GmbH, Dr. Fabian Ziegler, bereits Ende September während einer virtuellen Veranstaltung in Berlin an. „Wir unterstützen Deutschland, ein Land mit Netto-Null-Emissionen zu werden. Die Transformation von Shell in Deutschland hat begonnen und wird sich beschleunigen", sagte Ziegler.
Dazu hat Shell einen entsprechenden Plan entworfen, wie in Deutschland eigene Treibhausgasemissionen binnen eines Jahrzehnts um über ein Drittel gesenkt oder kompensiert werden können. Das entspricht rund 30 Millionen Tonnen pro Jahr und etwa einem Zehntel des CO2-Reduktionsziels der deutschen Bundesregierung bis 2030. Ziegler: „Wir glauben, dass das gelingen kann, wenn gleichzeitig die Politik für die notwendigen Rahmenbedingungen sorgt und Kunden vermehrt CO2-ärmere Produkte nachfragen."
So plant Shell unter anderem, in Deutschland führender Anbieter von grünem Wasserstoff für Industrie- und Transportkunden zu werden, die Elektrolyse-Kapazität in der Rheinland Raffinerie zu verzehnfachen und weitere H2-Projekte zu untersuchen. Daneben möchte sich das Unternehmen durch Offshore-Wind oder kombinierte Offshore-

Absichtserklärung: A. Pinkwart und F. Ziegler

Wind-/Wasserstoff-Produktion an der Erzeugung erneuerbarer Energien in Deutschland beteiligen und bis 2030 rund 1000 Schnellladesäulen an seinen Tankstellen errichten. Auch eine Transformation der Rohöl-Raffinerie im Rheinland in einen kohlenstoffarmen Energiepark wird angestrebt.

Nachhaltiger Energiestandort

Wie ernst es Shell meint, zeigt auch die Kooperation mit Nordrhein-Westfalen. So wurde im November der Rahmen für eine Zusammenarbeit und Koordinierung von Tätigkeiten von Shell Deutschland, der Landesregierung NRW und weiteren Partnern gesetzt. Ziel ist es, die Rheinland Raffinerie zu einem nachhaltigen Energie- und Chemiestandort weiterzuentwickeln. Im vom Kohleausstieg besonders betroffenen NRW kann Shell so einen integrierten Beitrag zur Dekarbonisierung und gleichzeitigem Aufbau einer „grünen" Industrie und zur Sicherung von Arbeitsplätzen leisten.
„Die Landesregierung will Nordrhein-Westfalen zum modernsten und umweltfreundlichsten Industriestandort Europas entwickeln. Das schaffen wir aber nur, wenn Unternehmen und Politik eng zusammenarbeiten. Mit der heute unterzeichneten Absichtserklärung knüpfen wir genau hier an und unterstützen den Wandel der chemischen Industrie im Rheinland", erklärte Wirtschafts- und Digitalminister Prof. Dr. Andreas Pinkwart. Die Absichtserklärung regelt die Zusammenarbeit von Landesregierung und Shell, um den Wandel der Rheinland Raffinerie bestmöglich zu unterstützen. Dazu gehört auch die Einrichtung eines Transformationsdialogs mit der Landesinitiative IN4climate.NRW sowie eines Beirats mit hochrangigen Vertretern aus Politik, Industrie und Wissenschaft.
Dr. Fabian Ziegler unterstrich dabei die Bedeutung der Werke in Köln-Godorf und Wesseling: „Wir arbeiten auf eine Mobilität hin, die keine fossilen Energien enthält. Die Rheinland Raffinerie ist Motor und Herzstück der Shell Aktivitäten in Deutschland und wird eine Schlüsselrolle spielen, um die Produkte bereitzustellen, die sich zusehends von unserem heutigen rohöldominierten Angebot unterscheiden und mehr und mehr zu regenerativen Lösungen wandeln werden." ●

YOU CAN'T BE #FULLYCIRCULAR. WHY NOT?

At Covestro, we're collaborating with other stakeholders to turn today's products into tomorrow's polymers.
Because we believe the future of chemistry is circular.

#PushingBoundaries covestro.com/circular-economy

CHEMPARK
Europas Chemiepark

51° N 7° E

Neuer Standort gesucht?

Willkommen im CHEMPARK!
Nutzen Sie unser Online-Investoren-Tool und finden Sie heraus, wie gut wir zueinander passen.

www.investoren.chempark.de