Keywords
- *Cybersecurity*
- *Anlagensicherheit*
- *IT/OT*
- *Netzwerksicherheit*

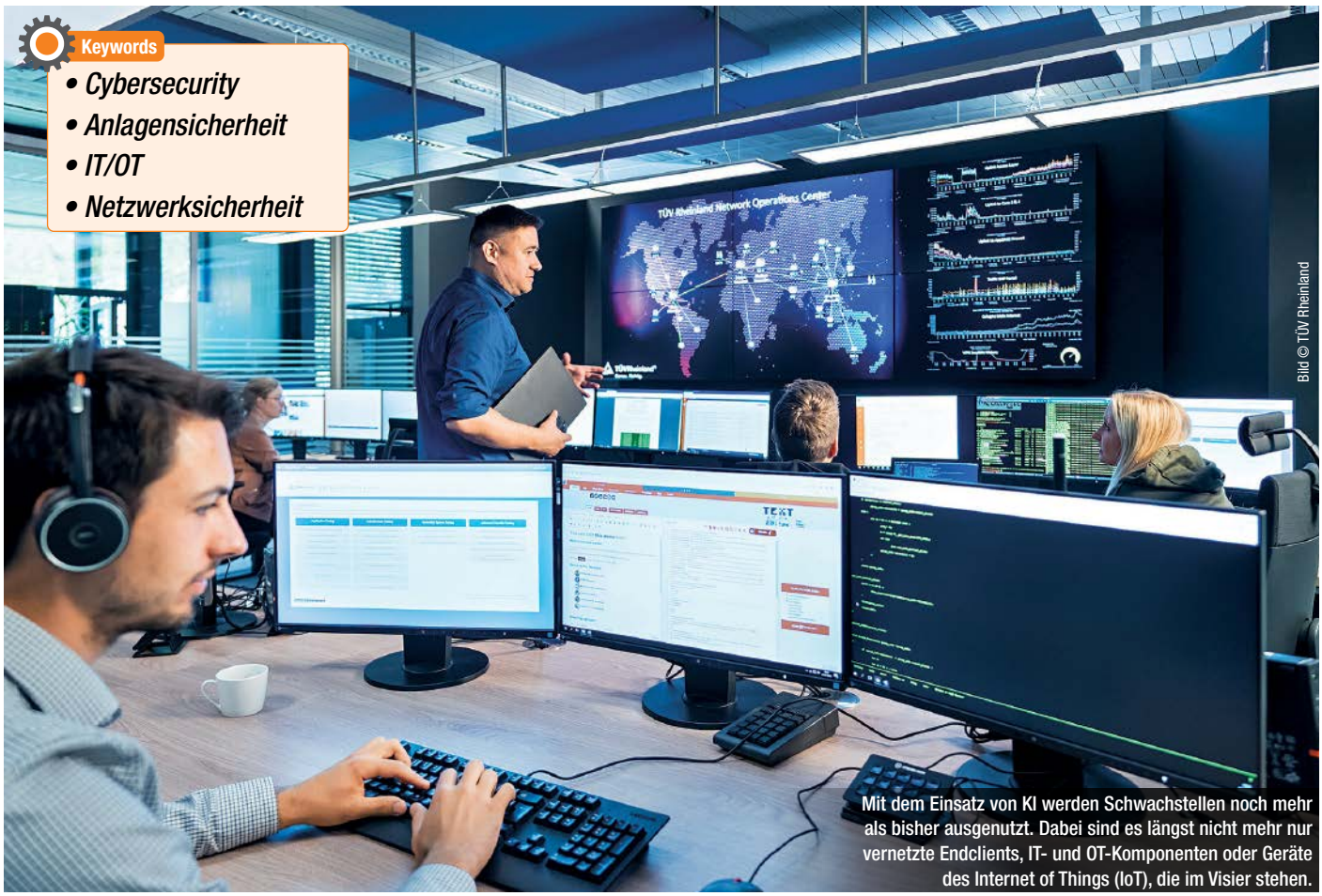

Bild © TÜV Rheinland

Mit dem Einsatz von KI werden Schwachstellen noch mehr als bisher ausgenutzt. Dabei sind es längst nicht mehr nur vernetzte Endclients, IT- und OT-Komponenten oder Geräte des Internet of Things (IoT), die im Visier stehen.

Cybersecurity in Chemieanlagen

Den Standard IEC 62443 und die Richtlinie KAS 51 harmonisiert anwenden

Die Vernetzung von teilweise alten Systemen birgt die Gefahr von Cyberbedrohungen, die die Sicherheit, Verfügbarkeit und Integrität von Anlagen gefährden. Zudem sind Fachkräfte für Cybersecurity von Betriebstechnik begrenzt verfügbar und auf dem Arbeitsmarkt heiß umkämpft. Eine Analyse zeigt, wie Betreiber mit den möglichen Gefahren für Chemieanlagen mit etablierte Sicherheitspraktiken wie bspw. KAS 51 und IEC 62443 umgehen können.

Angriffe auf Produktionen – Operational Technology (OT-Systeme) – sind keine Seltenheit mehr. Es liegen unzählige Beispiele dafür vor, dass solche Angriffe bereits erheblichen Schaden verursacht haben. Stuxnet gilt als einer der bekanntesten Angriffe auf OT-Systeme. Stuxnet war ein sogenannter Computerwurm, der speziell zum Angriff auf ein System zur Überwachung und Steuerung (SCADA-System) entwickelt wurde. Dieser Angriff gilt als professionelle Sabotagesoftware gegen iranische Atomanlagen.

Ein weiteres Beispiel ist Triton, ein Schadprogramm (hochentwickelte Malware), das 2017 bei einer Cyberattacke auf saudische Petrochemieanlagen entdeckt wurde. Bei dem Vorfall wurde ein Steuerungsmodul angegriffen, welches in einem Notfall im letzten Moment eine Anlage außer Betrieb nehmen soll. Weltweit wird das Steuerungsmodul in vielen Anlagen (Öl-, Gas- und Kernkraftwerken) eingesetzt. Das zeigt, dass die organisierte Cyberkriminalität einen extremen Reifegrad erreicht hat.

Chemieanlagen sind in hohem Maße von automatisierten Systemen und digitalen Technologien abhängig, die den Produktionsprozess steuern und überwachen. Diese Abhängigkeit macht sie anfällig für Cyberbedrohungen, die von externen Akteuren oder sogar internen Quellen ausgehen können. Die Gefahr besteht nicht nur in finanziellen Verlusten durch Stillstandszeiten, sondern auch in potenziell katastrophalen Folgen für Umwelt und Gesundheit der Menschen.

Die chemische Industrie steht besonders im Fokus der Cyberkriminalität. Denn ihre Anlagen gelten als „lohnenswertes Ziel“ für den Angreifer und ein Angriff kann zu erheblichen Schäden in wirtschaftlicher Hinsicht sowie an Reputation, Umwelt, Leib und Leben führen. Entsprechend hoch fallen Lösegeldforderungen hier aus (Stichwort Ransomware). Zudem steigt aus Sicht des Hackers bei einem erfolgreichen Angriff auch der Reputationsgewinn in der Szene. Technisch betrachtet ergeben sich

zudem zwei gegenläufige Effekte, die zu weiter steigenden Risiken beitragen: Zum einen sind Anlagen teilweise sehr groß, sehr komplex und werden selten ausgetauscht – mit anderen Worten: Sie sind alt. Alte Soft- und Hardware macht es dem Angreifer allerdings einfach sie anzugreifen. Gleichzeitig werden die Systeme jedoch immer stärker digitalisiert und vernetzt. So wird aktuell vielfach darüber diskutiert, Mess-, Steuerungs- und Regelungstechnik (MSR) in die Cloud zu verlagern. Das Ziel: weitere Effizienzgewinne und Prozessoptimierungen. Wenn allerdings alte Technik mit neuen Komponenten verbunden wird und zudem wegen des Fachkräftemangels nicht ausreichend Know-how zum Schutz bereitsteht, ergibt sich ein hohes Cyber-Risiko.

Standards und Best Practice

Die Entwicklungen in der Industrie, der Technik und die besorgniserregende Zunahme von Cyberangriffen haben auch die Regierungen weltweit erkannt. Mit der voranschreitenden Digitalisierung von Prozessen in der Automatisierung geht die Entwicklung einer Vielzahl von Standards in verschiedenen nationalen und internationalen Gremien einher. Doch welche Standards passen zum eigenen Schutzbedarf – und wie lassen sich die Standards anwenden?

Antworten für die deutsche Chemieindustrie

Die Kommission für Anlagensicherheit (KAS 51) definiert Richtlinien gemäß der Störfallverordnung (StörfallV) zum Schutz der Chemieanlagen und betrachtet verschiedene Sicherheitsaspekte. Gemäß der StörfallV ist es eine grundlegende Verpflichtung, mögliche Gefahren durch unbefugte Eingriffe zu berücksichtigen (§ 3 Abs. 2 Nr. 3 der StörfallV). Diese Berücksichtigung sollte sicherstellen, dass gefährliche Stoffe in den Betriebsbereichen so geschützt sind, dass ernsthafte Gefahren oder Schäden gemäß den Vorgaben der StörfallV vernünftigerweise ausgeschlossen werden können. Zusätzlich gibt es auch Vorschriften, wie die Gefahrstoffverordnung (GefahrstoffV) und das Sprengstoffrecht, die darauf abzielen, bestimmte Stoffe vor dem Zugriff unbefugter Personen zu schützen. Die getroffenen Schutzmaßnahmen müssen dabei angemessen sein und den potenziellen Auswirkungen durch unbefugte Eingriffe gerecht werden.

Im Bereich des physischen Schutzes legt die KAS 51 Richtlinien für den Zugang zu sensiblen Bereichen fest, einschließlich Überwachungssystemen, Zäunen und Sicherheitspersonal. Hierbei ist eine lückenlose Überwachung der Anlagenperimeter von entscheidender Bedeutung, um unbefugten Zugriff zu verhindern.

Der Drohnenschutz gewinnt an Bedeutung, da diese Technologie potenziell für Angriffe oder Spionagezwecke genutzt werden kann. Die KAS 51 sieht vor, dass Chemieanlagen entsprechende Abwehrmaßnahmen implementieren, um unbemannte Luftfahrzeuge zu erkennen und zu neutralisieren. Dies kann durch den Einsatz von Drohnenabwehrsystemen, Frequenzstörungen und Frühwarnsystemen erreicht werden.

Im Bereich der Cybersecurity setzt die KAS 51 auf eine umfassende Strategie zur Abwehr von Cyberbedrohungen. Dies umfasst die Implementierung von robusten Firewallsystemen, regelmäßigen Software-Updates, klare Segmentierung der jeweiligen Netzwerke von Unternehmens-IT und der OT-Ebene sowie Zugriffskontrollen. Besonders betont wird die Schulung des Personals im Umgang mit Cyberbedrohungen, um menschliche Fehler zu minimieren. Zudem wird empfohlen, eine ständige Überwachung der Netzwerke durchzuführen, um ungewöhnliche Aktivitäten frühzeitig zu erkennen und zu unterbinden.

Die internationale Normenreihe IEC 62443 nimmt im Rahmen der Cybersecurity von Chemieanlagen ebenfalls eine maßgebliche Position ein. Die IEC 62443 definiert umfassende Standards und Anforderungen (falls eine Zertifizierung angestrebt wird) für die Cybersicherheit industrieller Automatisierungssysteme, einschließlich Chemieanlagen. Insbesondere legt dieser Standard den Schutz vor Cyberbedrohungen fest und bietet eine strukturierte Herangehensweise zur Sicherung von Automatisierungssystemen. In Verbindung mit KAS 51 erweitert die Integration von IEC 62443 die Schutzmechanismen auf den Bereich der industriellen Netzwerke und die Prozessautomatisierung.

Indem Betreiber von Chemieanlagen den Standard IEC 62443 und die Richtlinie KAS 51 harmonisiert anwenden, können sie eine umfassende und effektive Verteidigung gegenüber Cyberbedrohungen sicherstellen und somit die Verfügbarkeit, Integrität und Sicherheit ihrer Geschäftskontinuität gewährleisten.

NIS-2 Richtlinie: auch für Chemiebranche relevant

Die Europäische Union reagiert mit der NIS-2-Richtlinie auf die wachsende Zahl von Cyberbedrohungen: Die neue „Network and Information Security Directive“ führt strengere Vorschriften zur Cybersicherheit für mehr Sektoren und Unternehmen ein. Das Ziel bleibt jedoch gleich: Der Schutz von (kritischen) Infrastrukturen und eine höhere Widerstandsfähigkeit gegenüber Cyberangriffen. Dabei konzentriert sich die NIS-2-Richtlinie nicht nur auf den Produktionsbereich (OT), sondern auf das gesamte Unternehmen.

Die größte Änderung zum IT-Sicherheitsgesetz 2.0 ist der erweiterte Unternehmensscope. Dazu steigen die Anforderungen an die Cybersicherheit: Betroffene Unternehmen müssen angemessene Maßnahmen nach „aktuellem Stand der Technik“ in Bereichen wie dem Risikomanagement, Business Continuity Management (BCM), der Sicherheit in der Lieferkette oder auch Reaktion auf Vorfälle ergreifen.

Hinzu kommen gestärkte Durchsetzungskräfte der nationalen Regulierungsbehörden, höhere Strafen für Verstöße und verschärfte Meldepflichten. Letztere sehen vor, dass Unternehmen Sicherheitsvorfälle unverzüglich, jedenfalls aber innerhalb von 24 Stunden nach Kenntnisnahme mit einer sogenannten Frühwarnung und innerhalb von 72 Stunden mit einer detaillierten Meldung bekanntgeben müssen. Bis zum 17. Oktober 2024 müssen die EU-Mitgliedstaaten die Direktive in nationales Recht überführen; auf dieser Grundlage werden Unternehmen dann zur Umsetzung verpflichtet.

Schlusswort

Aktuell zeigt sich, dass viele Unternehmen in der chemischen Industrie ihre Bemühungen zur Verbesserung der Cybersecurity verstärken. Organisatorische Anpassungen und die Definition von klaren Verantwortlichkeiten ist für die nachhaltige risikoorientierte Steuerung von Cyberrisiken in der chemischen Industrie unabdingbar. Es ist unmöglich, alle Sicherheitslücken zu schließen, insbesondere wenn veraltete Technologien verwendet werden. Neben präventiven Schutzmaßnahmen ist eine entscheidende Maßnahme die umfassende Überwachung der Infrastruktur. Das Hauptziel besteht darin, Angriffe möglichst schnell zu identifizieren und darauf adäquat vorbereitet zu sein.

Felix Brombach,
OT Security Consultant,
TÜV Rheinland i-sec

Artjom Schmidt,
Head of Business Development und Portfolio,
TÜV Rheinland i-sec

Wiley Online Library

TÜV Rheinland i-sec GmbH, Köln
Tel.: +49 221 - 806 - 4050
service@i-sec.tuv.com · www.tuv.com