genua.

Sichere Segmentierung für die AdBlue-Produktion

Eine leistungsfähige Industrial Firewall hilft Unternehmen der chemischen Industrie, ihre IT/OT-Netzwerke sicher zu segmentieren – und die Anforderungen der NIS-2-Richtlinie zu erfüllen.

SCHUTZ FÜR DIE ANLAGENSTEUERUNG IM CHEMIEPARK

von Dr. Wilhelm Greiner, freier Fachjournalist

SecurITy made in Germany

Im niederländischen Geleen steht einer der größten Chemieparks Europas. Auf dem 880 Hektar großen Gelände des Chemieparks „Chemelot“ – eine Anspielung auf Camelot, die sagenumwobene Burg von König Artus und seiner Tafelrunde – arbeiten rund 8.500 Beschäftigte von über 200 Unternehmen an Chemieprodukten und deren Weiterentwicklung.
In 60 Fabriken erzeugen sie rund 7,5 Millionen Tonnen Chemieprodukte pro Jahr. Dabei ist Chemelot nicht nur Industrie-, sondern auch Forschungsstandort: Rund 3.000 Fachkräfte und 1.200 Studenten forschen hier an der Zukunft chemischer Produkte.

Projekt-Steckbrief

Der Kunde:
Unternehmen und Anlagenbetreiber Im Chemiepark Chemelot in Geleen, Niederlande.

Die Aufgabe:
Anlagen der chemischen Produktion sind konsequent vor Betriebsstörungen und Cyberangriffen zu schützen. Dazu müssen für Produktionssysteme höchster Kritikalität Netzsegmente eingerichtet und der Datenverkehr strikt kontrolliert werden.

Die Lösung:
genuwall steht für „Security Made in Germany“ und nutzt Know-how aus dem Geheimschutzbereich. Die Industrial Firewall segmentiert Industrienetze und schützt Produktionsanlagen verlässlich vor unerlaubtem Zugriff.

Damit im Industrie- und Forschungsalltag stets „die Chemie stimmt“, braucht es zweierlei: Anlagen für den verlässlichen Betrieb der Produktion und eine hochsichere Vernetzung, um die Maschinen und Anlagen zu steuern. Schließlich gilt die Chemiebranche laut der neuen EU-Richtlinie NIS 2 (Network and Information Security Directive 2) als wichtiger Sektor. Das bedeutet: Anlagen der chemischen Produktion sind konsequent vor unbefugtem Zugriff zu schützen, sonst drohen dem Betreiber hohe Strafen – und im Ernstfall haftet das Management für lückenhafte oder unterlassene Maßnahmen.

Herausforderung: Schutz kritischer Anlagen

Das Damoklesschwert der NIS-2-Richtlinie verschärft ein Dilemma, mit dem praktisch alle produzierenden Unternehmen kämpfen: Einerseits erfordert es der zeitgemäße Produktionsbetrieb, Industrieanlagen zu vernetzen. Nur so kann das OT-Personal (Operational Technology) die Anlagen aus der Ferne – per Netzwerk, ggf. sogar via Internet – überwachen und steuern. Und nur so können Betreiber Sensordaten für KI-Auswertungen im Sinne einer „Smart Factory“ sammeln. Andererseits birgt jede Vernetzung auch Risiken, erfolgen doch Angriffe auf Unternehmensinfrastrukturen in aller Regel vom Internet aus. Hier lauern Gefahren wie Ransomware-Angriffe, Industriespionage und – insbesondere in der Industrie – Sabotage.

Daher gilt es, Systeme hoher bis höchster Kritikalität (Level 0 bis 3 im Purdue-Referenzmodell) strikt gegenüber weniger kritischen Einrichtungen abzuschotten – also z. B. gegenüber der ERP-Software (Purdue-Level 4) oder dem Office-LAN (Level 5). Für höchstmöglichen Schutz sorgen hier Industrial Firewalls.

Um kritische Infrastruktur besser vor Cyberangriffen und Störungen zu schützen, hat die Europäische Union die NIS-2-Richtlinie eingeführt

Die NIS-2-Richtlinie verpflichtet Organisationen, nachweislich angemessene Maßnahmen umzusetzen, die Sicherheit und Widerstandsfähigkeit ihrer Netzwerke und Informationssysteme gewährleisten. Diese Maßnahmen umfassen Risikomanagement, technische und organisatorische Maßnahmen, Meldung von Vorfällen sowie Einhaltung und Durchsetzung.

Industrial Firewalls für die AdBlue-Produktion

In Geleen wird Stickstoff produziert, der zum Beispiel für Düngemittel, sowie Melamin, einen Grundstoff für Harze, Klebstoffe und Beschichtungen benötigt wird. Ende 2022 wurde die Umgebung um eine Anlage zur Herstellung des Treibstoffzusatzes AdBlue erweitert. Eine Anforderung: Die AdBlue-Tanks sollten nach dem Stand der Technik geschützt und aus der Ferne kontrollierbar sein. Denn zwischen der Produktionsstätte und den AdBlue-Tanks lag auf dem weitläufigen Chemelot-Gelände eine Distanz von rund einem Kilometer, und auf dieser Strecke galt es zudem, diverse Abnehmer anzubinden.

Dazu waren einerseits die Anlagensteuerungen (Programmable Logic Controller, PLC) – hierfür setzt man auf HIMA HIMatrix Safety PLCs – mit dem Backbone-Netzwerk zu verbinden, andererseits mit dem SCADA-System zur Prozesssteuerung (Process Control System, PCS). Diese Bausteine befinden sich auf unterschiedlichen Purdue-Levels. Deshalb muss für den vorschriftsmäßigen Datenverkehr stets eine Firewall zwischengeschaltet sein.

Bisherige Lösung: zu komplex, zu wenige Ports

Seit Jahren setzte man an dieser Stelle auf die Firewall-Technik eines internationalen Anbieters. Doch dessen Industrial Firewalls haben zwei wesentliche Mankos: Die Firewall-Konfiguration ist komplex und die Geräte verfügen über nur zwei Ports. Deshalb ist für die Netzwerkverbindungen zwischen PLC und Backbone sowie zwischen PLC und PCS jeweils eine separate Firewall zu implementieren und aufwendig zu konfigurieren.

Aus diesem Grund machten sich die Betreiber im Frühjahr 2023 auf die Suche nach einer einfach konfigurierbaren Industrial Firewall, die beide Aufgaben zugleich übernehmen kann. Dabei wurde die HIMA Paul Hildebrandt GmbH zu Rate gezogen. Denn mit HIMA arbeitet man dort schon seit mehr als 25 Jahren bei Automationsprojekten sehr gut zusammen.

Bei der Recherche stieß man auch auf die Industrie-Firewall genuwall des deutschen IT- und OT-Security-Spezialisten genua aus Kirchheim bei München, die auch von Erik van Wouwe, Sales Manager Benelux bei HIMA, empfohlen wird. Van Wouwe weiß um die Qualität der deutschen Security-Technik, betreibt doch HIMA gemeinsam mit genua ein Security Lab in Brühl.

AdBlue reduziert den Schadstoffausstoß bei Dieselfahrzeugen. Ende 2022 wurde der Chemiepark Chemelot um eine Anlage zur Herstellung des Treibstoffzusatzes erweitert. Für Schutz gemäß NIS-2-Richtlinie sorgen Industrial Firewalls von genua.

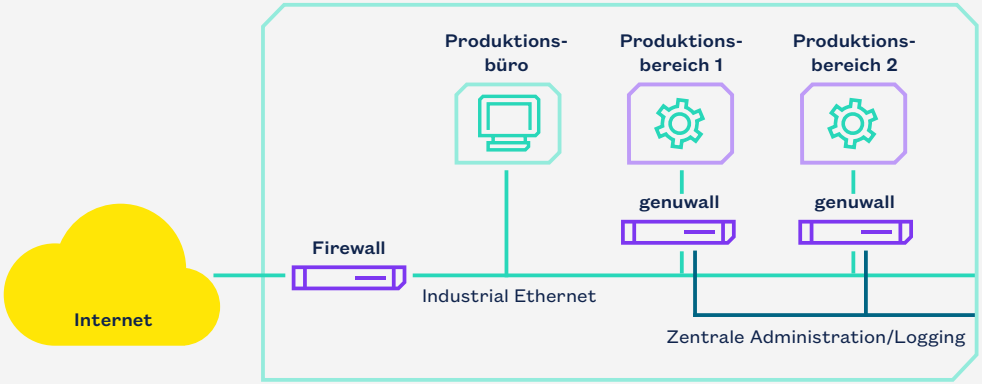
genuwall schützt mit Geheimschutz-Know-how

Die Industrial Firewall genuwall bietet „Security Made in Germany“ und nutzt dazu Know-how aus dem Geheimschutzbereich: Sie basiert auf der bewährten genua-Firewall genuscreen, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach dem internationalen Standard Common Criteria (CC) als „EAL 4+“ zertifiziert ist. Die Firewall eignet sich damit nachweislich für den Einsatz in Netzwerken der öffentlichen Hand wie auch in KRITIS-Umgebungen (Kritische Infrastruktur) – oder, im NIS-2-Sprachgebrauch, für wesentliche und wichtige Einrichtungen.

Zur hochsicheren Segmentierung von Industrienetzen erkennt und verwirft genuwall unzulässige Datenpakete von OT-Protokollen (OPC UA, Modbus TCP, IEC 60870-5-104) bis auf Anwendungsebene. Damit schützt sie verlässlich vor unerlaubtem Zugriff. Die Firewall lässt sich per USB-Boot schnell installieren und integriert sich einfach in bestehende Netzwerkumgebungen. Das Management ist lokal wie auch – natürlich ebenfalls hochsicher – von zentraler Stelle aus möglich.

Eine Firewall, bis zu vier Purdue-Level

Neben den genannten Vorteilen der genuwall fiel dem verantwortlichen Ingenieur ein scheinbar banaler, aber für ihn wichtiger Punkt ins Auge: Die Firewall hat vier statt nur zwei Ports. „Die genuwall erlaubt es uns, Zonen einzurichten, also die Trennung zwischen PLC und SCADA-System sowie zwischen PLC und Netzwerk-Backbone mit einem einzigen Gerät umzusetzen,“ erläutert er. „Mit vier Firewall-Ports kann ich Equipment mit bis zu vier verschiedenen Purdue-Levels sicher anbinden. Es ist also nun nicht mehr für jeden Datenstrom eine separate Firewall nötig wie früher.“



Zonenbildung für sichere Produktionsbereiche mit genuwall.

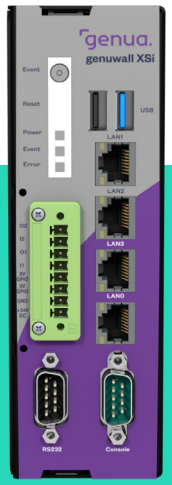
Für das AdBlue-Projekt ließen sich so die HIMA-PLCs über HIMAs SafeEthernet-Protokoll per genuwall sicher vernetzen, zugleich läuft die Kommunikation zwischen PLC und SCADA-System ebenfalls geschützt über Modbus TCP.

Diese Konsolidierung vereinfacht das Firewall-Management und die Wartung der Geräte. Dabei bewährt sich die genuwall durch leichte Bedienbarkeit. Nicht minder wichtig in einem Chemiepark: Da weniger Geräte zu verwalten sind, lassen sich auch Fehler einfacher isolieren und Geräte schneller abschalten – im Notfall möglicherweise ein entscheidender Zeitvorsprung.

Weniger Geräte, weniger Aufwand, weniger Kosten

Der Wechsel zu genuwall-Geräten des deutschen Security-Spezialisten genua ermöglicht es, den Firewall-Betrieb im Chemiepark Chemelot zu konsolidieren und damit Aufwand wie auch Kosten erheblich zu senken. Im aktuellen Projekt der AdBlue-Produktionsanlage ersetzt eine genuwall die zwei vormals nötigen Industrial Firewalls pro PLC. Die intuitive Bedienung erleichtert die Inbetriebnahme ebenso wie die Wartung.

Fünf genuwall-Geräte sind auf dem Chemelot-Campus bereits im Einsatz, fünf weitere sollen hinzukommen. Damit hat sich in Chemelot eine neue Tafelrunde zusammengefunden – nicht, um wie das historische Vorbild den Heiligen Gral zu suchen, sondern um einen der größten Chemieparks Europas verlässlich vor Betriebsstörungen und Cyberangriffen zu schützen.



Industrial Firewall genuwall des deutschen Herstellers genua mit Sitz bei München.

genuwall bietet vier Firewall-Ports und ermöglicht somit eine Zonenbildung.

Weitere Informationen:

genua.de/genuwall

0126-02-DE

Über genua

Mit ihren in Deutschland entwickelten und produzierten IT-Sicherheitslösungen ist die genua GmbH eine Wegbereiterin für digitale Souveränität. Behörden, geheimschutzbetreute Organisationen und KRITIS-Unternehmen vertrauen auf genua zum Schutz ihrer kritischen und hochsensiblen digitalen Infrastrukturen.

genuas Portfolio umfasst hochsichere, Backdoor-freie und skalierbare IT-Security-Produkte wie Firewalls, Gateways, quantenresiliente VPNs, Fernwartungssysteme und Komplettlösungen für VS-NfD-konformes mobiles Arbeiten. Viele Produkte sind auch als virtualisierte Variante für eine flexible Cloud-Integration verfügbar. Regelmäßige Zertifizierungen und Zulassungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) belegen das hohe Sicherheits- und Qualitätsniveau.

Mit ihren rund 500 Mitarbeitenden ist die genua GmbH Teil der Bundesdruckerei-Gruppe. Das Unternehmen ist vom BSI als „Qualifizierter Hersteller“ eingestuft und mit seinen Produkten im Kaufhaus des Bundes gelistet. Zu den Kunden zählen u. a. BMW, die Bundeswehr, das THW und die Würth-Gruppe.

Teil der Bundesdruckerei-Gruppe

genua GmbH

Domagkstraße 7 | 85551 Kirchheim bei München
+49 89 991950-0 | info@genua.de | www.genua.de