cav

CHEMIE PRODUKTION ANLAGEN VERFAHREN

02-2025

36 TITEL
SICHERE BEPROBUNG VON CHEMIKALIEN

10 KI UND CYBERSECURITY
TRENDS DER DIGITALEN CHEMIEPRODUKTION

18 FERNZUGRIFF
CYBERRISIKEN SICHER AUSSCHALTEN

26 NOTDUSCHEN
ERSTE HILFE ODER ERNSTE GEFAHR?

MIT BRANCHEN-SPECIAL PHPRO

PROZESSTECHNIK FÜR DIE **CHEMIE**INDUSTRIE
WWW.PROZESSTECHNIK-ONLINE.DE/CHEMIE

Zero Trust Application Access ermöglicht sicheren Fernzugriff

Remote-Access-Cyberrisiken zuverlässig ausschalten

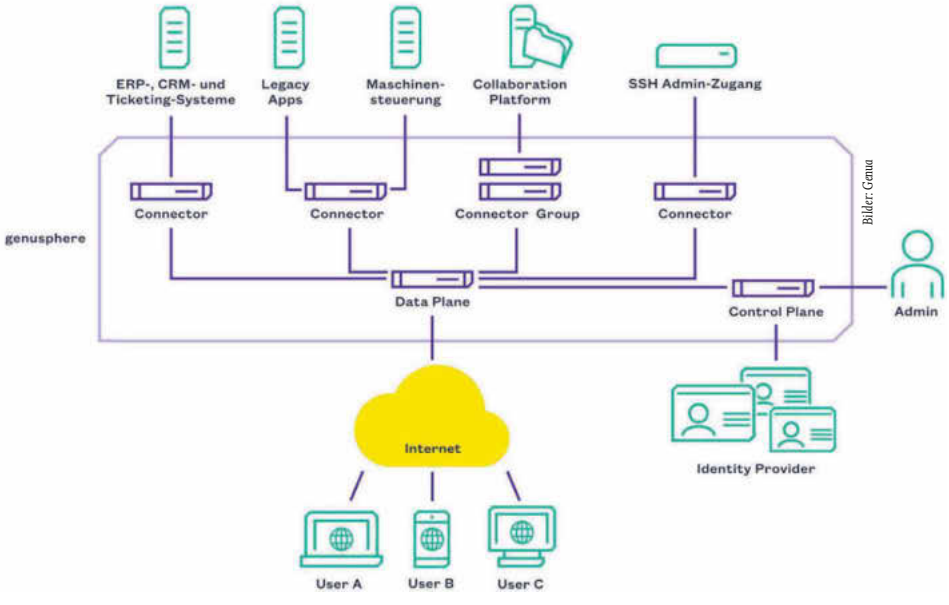
Mit Zero Trust Application Access lässt sich ein hochsicherer, identitätsbasierter und anwendungsspezifischer Zugriff auf unternehmensinterne Applikationen ohne VPN realisieren. Ideal, um zum Beispiel externen Dienstleistern temporär einen sicheren Zugang zu dedizierten Anwendungen bereitzustellen.

Die Anforderungen an die Netzwerksicherheit haben sich in der modernen Arbeitswelt grundlegend geändert. Mitarbeiter, Dienstleister und Kunden greifen vermehrt von extern und mit verschiedenen Endgeräten auf Applikationen in Unternehmensnetzwerken zu. Gleichzeitig wachsen OT und IT verstärkt zusammen, sodass auch Maschinen und Anlagen etwa in Fabriken oder Chemieparks aus dem Internet erreichbar sind. Die Vorteile liegen auf der Hand: Zum Beispiel lassen sich die Systeme effizienter betreiben, da sie beispielsweise ohne Vor-Ort-Präsenz konfigurierbar sind. Hinzu kommt, dass Unternehmen verstärkt Cloud-Angebote nutzen – etwa, um durch den Einsatz virtualisierter Netzwerkprodukte ihre IT-Infrastruktur flexibler skalieren zu können.

Die Kehrseite: Diese Entwicklungen hebeln bisherige Perimeter-basierte Sicherheitsarchitekturen zunehmend aus. Und durch die verstärkte Exponierung sensibler Assets entstehen neue Angriffsvektoren, über die Cyberkriminelle Unternehmen attackieren können. Das wiegt schwer, da Cyberbedrohungen auch im industriellen Sektor weltweit seit Jahren massiv zunehmen. Industriespionage, Manipulation oder gar Zerstörung von Anlagen sind mögliche Folgen.

Nichtnutzung ist keine Option

Die Vorteile von kombinierten IT/OT-Strukturen nicht zu nutzen, ist für viele Unternehmen jedoch keine Option. Daher stellt sich die Frage: Wie lassen sich ihre IT- und daran gekoppelte OT-Systeme bestmöglich absichern? Und gleichzeitig Möglichkeiten schaffen, Legacy-Web- und Windows-Applikationen weiter zu betreiben, spezielle Steuerungsanwendungen von Maschinen und Anlagen, Admin-Interfaces sowie restriktiv eingesetzte Applikationen zu erreichen und sichere temporäre Zugänge für externe User einzurichten?



So funktioniert Genusphere: User und Connector bauen eine verschlüsselte Verbindung zur Data Plane auf. In der Control Plane sind die identitätsbasierten Zugriffsberechtigungen hinterlegt.

Zero Trust Application Access

Eine Antwort lautet Zero Trust Application Access, kurz ZTAA. Der Zero-Trust-Ansatz geht grundsätzlich davon aus, dass keine Person und kein Gerät standardmäßig vertrauenswürdig ist. Stattdessen wird jeder Zugriff methodisch und wiederholt überprüft, selbst wenn der Nutzer dem System bereits bekannt ist. Zero-Trust-Lösungen lassen sich zudem so konfigurieren, dass sie für interne und externe Nutzer gleichermaßen anwendbar sind. Dadurch lässt sich ein guter Schutz auch vor Insider-Bedrohungen und kompromittierten Konten realisieren. ZTAA agiert zudem nach dem Prinzip der minimalen Rechtevergabe. Verbindungen zwischen Usern – externen wie internen – und Anwendungen werden anhand von Identität, Rolle und Geschäftsrichtlinien (Policies) hergestellt. So erhalten Anwender abhängig von diesem Dreiklang nur Zugriff auf einzelne, für sie freigegebene Applikationen – anstatt auf weitreichende Ressourcen im Netzwerk.

Sicherer Zugriff per Webbrowser

Für die oben genannten und weitere Anwendungsfälle hat der deutsche IT-Security-Spezialist Genua die skalierbare ZTAA-Lösung Genusphere entwickelt. Das Besondere daran: Genusphere benötigt anwenderseitig keine Installation einer speziellen Software,

etwa eines VPN-Clients. Ein Standard-Webbrowser wie Google Chrome oder Microsoft Edge reicht, um sicher auf explizit freigegebene Ressourcen im Unternehmensnetzwerk zuzugreifen.
Eine Client-lose Zugriffslösung bietet für moderne Arbeitsumgebungen einige Vorteile. An erster Stelle sind hier die Unabhängigkeit von Gerät und Betriebssystem, geringer Wartungsaufwand sowie hohe Flexibilität und Skalierbarkeit zu nennen. Geringe Kosten und einfache Integration sprechen ebenfalls für browserbasierte Lösungen.
Genusphere baut auf Kubernetes auf – einer ursprünglich von Google entwickelten Open-Source-Plattform zum Verwalten von Container-Anwendungen. Der Container-basierte Ansatz ist von Grund auf für optimale Skalierbarkeit und Hochverfügbarkeit ausgelegt. Bei Genusphere erfolgt die Anbindung an das Zielsystem über Docker-Container, während die Verwaltung über ein zentrales Online-Administrationsportal erfolgt.
Eine Kernfunktion ist das implementierte Treffpunkt-Konzept: Nach einer vom Endgerät aus per Browser initiierten Verbindungsanfrage erfolgt der eigentliche Verbindungsaufbau von innen nach außen. So ist sichergestellt, dass für jeden Zugriff zuverlässig die definierten Zero-Trust-Regeln durchgesetzt werden.
Die Verbindungen sind grundsätzlich durchgängig mit HTTPS verschlüsselt. Fernsteuerung per RDP (Remote Desktop Protocol) oder VNC (Virtual Network Computing) sowie der Shellzugriff per SSH (Secure Shell) sind ebenfalls über Webbrowser nutzbar. Die Lösung ist mit Sicherheitsfunktionen wie Multi-Faktor-Authentisierung und Zero Trust Access Control ausgestattet.

Einfache Integration

Die Genua-Lösung setzt auf ein feingranulares Berechtigungsmanagement und lässt sich in vorhandene Sicherheitsarchitekturen einbinden. So unterstützt Genusphere die Identity Provider Microsoft Entra ID (vormals Azure AD) und Keycloak. Single Sign On (SSO) erhöht dabei den Nutzerkomfort. Die Regeln bauen auf den Identitäten der User aus der Benutzerverwaltung auf und sind der Schlüssel zu einer hochsicheren und flexibel skalierbaren Architektur.
Ein Dashboard mit genauen Metriken bietet Administrierenden jederzeit den Überblick über Nutzung und Betrieb. Gleichzeitig können sie mithilfe zahlreicher Regeln/Policies, logischen Verknüpfungen und Sub-Policies die Zugänge dynamisch anpassen. Wichtig dabei: Nicht ausdrücklich freigegebene Ressourcen sind sicher vor unbefugten Zugriffen geschützt. Selbst kompromittierte Nutzerkonten können sich somit nicht im Netz bewegen. Genusphere kann daher für Remote-Work-Umgebungen typische Cyberrisiken zuverlässig ausschalten.
Durch den identitätsbasierten und anwendungsspezifischen Zugriffsschutz baut Genusphere eine zuverlässige Mikro-Perimeter-Sicherheit auf. Zugriffe werden revisionssicher protokolliert und sind so lückenlos nachvollziehbar. Mithilfe der Genua-Lösung können Systemadministratoren konsequent hochsichere Zero-Trust-Konzepte durchsetzen. Nicht zuletzt zahlt Genusphere auf die Digitale Souveränität von Unternehmen ein. Denn sie behalten die Hoheit über ihre Daten. Firmen können Genusphere selbst betreiben, oder hierfür spezialisierte Genua-Partner ins Boot holen. Übrigens lässt sich die ZTAA-Lösung auch mit einem VPN kombinieren – dadurch entsteht eine zusätzliche Sicherheitsebene. (br)
www.prozesstechnik-online.de
Suchwort: Genua

NACHGEFRAGT › **GENUSPHERE IN DER CHEMIE**

Steve Schoner, Senior Product Manager bei Genua

Wie unterstützt Genusphere standortunabhängiges Arbeiten in der Chemieindustrie?
Schoner: Mithilfe von Genusphere können Mitarbeiter von Chemieunternehmen gezielt über einen Standard-Webbrowser auf für sie freigegebene Anwendungen zugreifen.
Der Zero-Trust-Ansatz von Genusphere stellt sicher, dass nur autorisierte Personen Zugriff auf sensible Informationen haben. Cyberkriminelle haben keine Chance, sich über ein gehacktes Nutzerkonto im Netzwerk auszubreiten. Das schiebt Manipulation, Gefährdung von Anlagen und Cyberspionage einen sicheren Riegel vor.

Wie kann Genusphere dabei helfen, die Zusammenarbeit zwischen verschiedenen Abteilungen und Partnern in der Chemieindustrie zu fördern?
Schoner: In der Chemieindustrie sind vielschichtige Lieferketten und komplexe Kooperationsprozesse eher die Regel als die Ausnahme. Genusphere kann die Zusammenarbeit zwischen dem Unternehmen und verschiedenen Partnern und Lieferanten vereinfachen – und gleichzeitig sicherer machen. Denn die Mitarbeiter der verschiedenen Akteure können explizit nur auf die Anwendungen zugreifen, für die eine Berechtigung für sie eingerichtet ist. Diese kann zusätzlich an bestimmte Bedingungen geknüpft sein – etwa Lieferstatus, Einwahlort, Zeitpunkt etc. Das Regelwerk kann durch den Betreibenden sehr flexibel ausgelegt werden.

Lässt sich Genusphere in bestehende Sicherheitsinfrastrukturen der Chemieindustrie integrieren?
Schoner: Genusphere unterstützt die Identity-Provider Microsoft Entra ID und Keycloak. Chemieunternehmen können so ihre bestehenden Sicherheitsmaßnahmen einfach erweitern und stärken, anstatt neue, separate Systeme zu implementieren. Durch die flexible Skalierbarkeit von Genusphere kann die Lösung an die spezifischen Bedürfnisse des Unternehmens angepasst werden. So ist es möglich, eine maximale Effizienz und Sicherheit zu erzielen. Hinzu kommt: Genusphere ist kein starres Korsett. Die Lösung lässt sich auch im Betrieb dynamisch an veränderte Bedingungen anpassen, sodass Unternehmen agiler agieren können.