genua.

Sicherer Fernzugriff aus einem Guss

Ein Mammut-Projekt in Sachen Sicherheit: Das Life-Science-Unternehmen Bayer hat den Fernzugriff auf seine vielen unterschiedlichen Anlagen und Standorte weltweit vereinheitlicht. Mit genua als erfahrenem Partner für Cyber-Sicherheit an der Seite konnte Bayer für seine regulierten Produktionen wichtige Funktionalitäten einführen.

von Frank Jablonski, freier Journalist

SecurITy made in Germany

Der Schaden in der deutschen Wirtschaft durch Cyber-Angriffe ist auch 2024 wieder sprunghaft gestiegen. Um etwa 29 Prozent auf nun 266,6 Milliarden Euro. Zum Vergleich: Das ist deutlich mehr als die Hälfte des bundesdeutschen Haushaltetats. Mittlerweile ist fast jeder Betrieb hierzulande betroffen. Während Diebstahl von Kundendaten oder geistigem Eigentum wie Patenten und Forschungsergebnissen sehr teuer werden können, sind bei der digitalen Sabotage von Industrieanlagen oder Betriebsabläufen potenziell die Integrität der Anlagen und damit auch Menschenleben gefährdet. Ein Industriezweig, bei dem die mögliche Schadenhöhe besonders relevant ist, ist die Prozessindustrie.

Projekt-Steckbrief

Der Kunde:

Bayer AG

Die Aufgabe:

Transparenz, Vereinheitlichung und mehr Sicherheit beim Zugriff von Zulieferern und Instandhaltern bei Fernzugriff auf Maschinen und Anlagen innerhalb des Bayer-Konzerns.

Die Lösung:

Einführung von genubox als Remote-Maintenance-Lösung in Kombination mit dem genua-Logging-System sowie einem Secure-File-Transfer als Bestandteil einer umfassenden und individuell angepassten genubox-Sicherheitslösung.

Fernzugriff und OT-Sicherheit: Eine Herausforderung für die Prozessindustrie

Chemie-, Pharma- und Lebensmittelhersteller sichern daher nicht mehr ausschließlich die funktionale Sicherheit der Anlagen, sondern auch ihre Netzintegrität. Inbetriebnahme ohne persönliche Anwesenheit, Ferndiagnosen und Überwachungsfunktionen vom heimischen Büro aus, wurden nach und nach zum Standard bei Zulieferern und Dienstleistern. Denn der rasche Zugriff von außen sorgte für eine höhere Verfügbarkeit der Anlagen – aber eben auch für unterschiedlichste Zugangsmethoden und Sicherheitskonzepte. Um sinnvolle und kosteneffiziente Geräte und Methoden der IT-Welt in den Prozess-Anlagen zu nutzen, wuchsen die Anwendungen vor allem an den großen Standorten zu einem nahezu unüberschaubaren Dschungel. Für eine Branche, die höchste Ansprüche an die Integrität und Sicherheit der Anlagen stellt, ein zunehmendes Problem.

Einheitliche Lösung gesucht

Ein herausragendes Beispiel, wie die Komplexität verringert und gleichzeitig eine größtmögliche Sicherheit für den Betrieb der Anlagen erreicht werden kann, ist das Unternehmen Bayer. „Vom damaligen CISO ging die Initiative aus, ein OT-Security-Programm aufzusetzen. Das Ziel lautete, Transparenz im Unternehmen darüber herzustellen, wie der Umgang in den einzelnen Bayer-Betrieben bei diesem Thema ist“, sagt Jani Alexander Krämer, Information Technology Security Analyst bei Bayer. Die Kombination aus großem Nutzen für den Betrieb und gleichzeitig hohem Schadpotenzial schob das Thema Fernzugriff nach ganz oben auf die Prioritätenliste. So lautete die zunächst wichtigste Bestrebung des damaligen OT-Security-Programms, eine einheitliche technische Lösung für den Fernzugriff auf Maschinen und Anlagen an den unterschiedlichen Standorten von Bayer zu erarbeiten.

> „Zu Beginn eines Standardisierungsprojektes gibt es tausend Gründe, warum alles nicht geht. Mit der Unterstützung von genua haben wir am Ende immer für alle Parteien Lösungen gefunden, mit denen alle zufrieden waren.“
>
> **Jani Alexander Krämer,**
> **Information Technology Security Analyst bei Bayer**

Mit den IT-/OT-Security-Experten von genua aus Kirchheim bei München war früh der passende Partner gefunden. Das Unternehmen, mittlerweile Teil der Bundesdruckerei-Gruppe, schützt Anlagen und Kommunikationsvorgänge in vernetzten und automatisierten Produktionssystemen. Die Expertinnen und Experten konzeptionieren eine sichere IT-/OT-Infrastruktur, wählen gemeinsam mit den Anwendern die passenden Sicherheitsprodukte für die Netzwerksicherheit aus und implementieren sie. Bei Bedarf wird zudem das Team vor Ort trainiert und unterstützt.

Feste Verabredung ist Pflicht

Die Rendezvous-Lösung von genua stellt sicher, dass es keine einseitigen Zugriffe vom externen Fernwartungs-Service gibt. Verbindungen in die Anlage zur Analyse oder Wartung müssen über einen Rendezvous Server abgewickelt werden, der in einer unkritischen, sogenannten demilitarisierten Zone (DMZ) oder virtuell in einer Cloud liegt. Zu diesem Treffpunkt bauen der externe Wartungs-Service und ein Verantwortlicher auf Seite des Betreibers zu einem fest verabredeten Zeitpunkt eine Verbindung auf. Mit diesem aktiven Schritt des Anwenders entsteht die durchgängige Verbindung, die zum Informationsfluss der Wartungszwecke notwendig ist. Maschinenwerte und Fehlermeldungen können so ausgelesen und bearbeitet werden. Dabei bleibt der Zugriff zeitlich und räumlich beschränkt. Der externe Service bewegt sich nur im zuvor definierten Zielsystem und Rollenbild. Hierzu nutzt genua ein anwendungsgenaues SSH statt eines netzwerkumfassenden VPN-Zugriffs.

Allein bei Bayer in Deutschland sind fast 100 genuboxen installiert. Betraf das zu Beginn hauptsächlich Rack-Hardware oder On-Premises, werden mittlerweile immer mehr virtualisierte Serviceboxen in der Cloud installiert – bei Bayer in etwa einem Viertel aller Anwendungen.

„Der Hauptnutzen einer Remote-Maintenance-Lösung ist die Kostenersparnis, da die On-Site-Besuche durch Zulieferer quasi entfallen. Das spart Geld und Zeit, denn niemand muss vor Ort sein."

Jani Alexander Krämer,
Information Technology Security Analyst bei Bayer

„Als ich zu Bayer kam, war die genua-Lösung bereits im Labor getestet und an 70 Standorten weltweit ausgerollt. Die große Herausforderung, die wir in der Folge Bayer-intern gemeistert haben, ist, aus der Technik einen Service zu bauen und ein erfolgreiches Rollout-Projekt daraus zu gestalten – in einem Großunternehmen eine nicht ganz einfache Aufgabe“, blickt Krämer zurück.

Hintergrund ist, dass viele Betriebe bei Bayer und bedeutende Zulieferer bereits eigene Sicherheitslösungen im Einsatz hatten. Dort, wo der Schwerpunkt der technischen Umsetzung des Fernzugriffs eher auf der Funktionalität statt auf der Sicherheit lag, war die Bereitschaft groß, auf das neue System zu wechseln. „In vielen Fällen war allerdings auch Überzeugungsarbeit notwendig, genua als verpflichtende Standardlösung im Unternehmen zu akzeptieren. Gerade, wenn Lieferanten mit eigenen guten Lösungen gezwungen waren auf genua umzusteigen“, sagt Krämer.

„Bei schätzungsweise rund

2000

Dienstleistern will man genau wissen, wer was macht.“

Ein Beispiel für die unterschiedliche Einschätzung betraf das Thema Audit-Trail. „Viele Betriebe arbeiten im GXP- oder GMP-Umfeld. Hier unterliegen wir hohen Anforderungen an die Dokumentation. Wir müssen lückenlos nachweisen, wer zu welchem Zeitpunkt, auf welchem System war und welche Änderung vorgenommen wurde“, ergänzt Carsten Rocks, Global Program Lead „Manufacturing IT Security“. In der CISO-Organisation von Bayer entwickelt er spezielle Security-Controls für die OT-Welt.

Demgegenüber arbeiteten die Zugriffslösungen von Maschinenbauern beispielsweise mit einem gepoolten Backoffice von Drittfirmen. Das führte dazu, dass in einigen Fällen nicht nachvollziehbar war, welcher Operator sich hinter einem Account verbirgt – aus Audit-Perspektive ein nicht akzeptabler Zustand.

Jeder Zugriff bekannt und aufgezeichnet

Krämer, der bei Bayer eine Art Service-Manager-Rolle einnimmt, sorgte gemeinsam mit dem Service-Dienstleister Atos für die weltweite Implementierung und Bereitstellung der notwendigen Programme, Anpassungen und Schulungen der Mitarbeiter. „genua war und ist dabei mit seiner technischen Expertise an unserer Seite. Ihr technischer Support springt auf einer Third-Level-Ebene ein, wenn es Probleme mit dem Service gibt, den die Dienstleister nicht lösen können“, erklärt Krämer, bei dem die Koordination und die klassischen Eskalationsthemen liegen.

Heute führt das bei Bayer eingesetzte genua Logging-System dazu, dass Anwender alle Verbindungen nachvollziehen können: So ist jederzeit transparent, wer sich angemeldet hat, zu welchem Zeitpunkt, welche Arbeiten erledigt wurden und wer sie überwacht hat. Die ebenfalls integrierte Aufzeichnungsfunktion wurde sogar auf ausdrücklichen Wunsch der damaligen Bayer-Verantwortlichen entwickelt.

Für genua hat es sich zu einem Unique Selling Point entwickelt, nicht nur Logs aufzuzeichnen, sondern detailliert den eigentlichen Wartungsvorgang. Nach Abschluss der Arbeiten kann das Session Recording ähnlich wie ein Video archiviert werden.

Sichere Updates von außen

Eine zusätzliche Implementierung, die ebenfalls in jüngerer Zeit in enger Zusammenarbeit mit dem Bayer-Team realisiert werden konnte, betrifft den Secure-File-Transfer-Part. Dateien von außerhalb der Organisation zu erhalten, gehört zu den Forderungen, bei denen sich Sicherheitsverantwortlichen die Nackenhaare aufstellen. Dennoch ist es gerade das Erneuern oder Reparieren beispielsweise einer Firmware, das eine Reaktor-Steuerung oder eine Verpackungsmaschine im Handumdrehen wieder flott machen kann. In einem eigenständigen Projekt wurde diese Anforderung adressiert und ein Malware-Scanning etabliert. Nun besteht die Möglichkeit, einen ICAP-Server anzubinden. Er ist Bestandteil der genubox-Sicherheitslösung und prüft Datenverbindungen und Dateien auf Schadsoftware, bevor sie in das Netzwerk gelangen. „Das ist eine hervorragende Erweiterung, die wir auf Basis des Feedbacks der Standorte mit genua planen und dann mithilfe unseres Providers implementieren konnten“, freut sich Rocks.

Allein bei Bayer in Deutschland sind fast

100

genuboxen installiert.

Anfangs kamen meist Hardware-Versionen der genubox zum Einsatz. Mittlerweile setzt das Unternehmen zunehmend auf virtualisierte Serviceboxen in der Cloud.

Auch wegen der Realisierung solcher Endnutzer-Wünsche ist die Akzeptanz bei Bayer hoch: „Wir bekommen regelmäßig ein gutes Feedback von unseren Anwendern. Dass sich eine fruchtbare Zusammenarbeit entwickelt hat, erkennt man auch daran, dass die Lösung nicht mehr nur für Remote Maintenance eingesetzt wird, sondern auch für interne Administrationen. Auch kommen immer wieder konstruktive Vorschläge, wie man den Service noch erweitern kann und welche zusätzlichen Features hilfreich wären“, sagt Krämer.

Nahtlose Integration

„Der Hauptnutzen einer Remote-Maintenance-Lösung ist die Kostenersparnis, da die On-Site-Besuche durch Zulieferer quasi entfallen. Das spart Geld und Zeit und hilft, schnell zu reagieren – wertvoll gerade im Störungsfall, denn niemand muss vor Ort sein“, sagt Krämer. „In diesem Zusammenhang würde ich die gesteigerte Flexibilität ergänzen. An einigen Standorten nutzen Mitarbeiter die Lösung intensiv auch für Zugriffe, wenn sie zum Beispiel im Home Office sind“, sagt Rocks. Die genua-Lösung bietet jedem Bayer-Standort die Wahl, ob der Zugriff beispielsweise über zeitgesteuerten Remote Maintenance eingerichtet wird, oder das Security Approval nur mit Freigabe von innen gewährt wird. Das hängt von der Division ab und ob beispielsweise eine Produktion GMP- oder GXP-Regeln unterliegt, welche Netzsegmentierungen vorgenommen wurden und ob spezielle IT-Lösungen im Einsatz sind.

Auch bestehende Systeme können genutzt werden. Die Anbindung an Cloud Identity Provider wie Okta oder Azure Active Directory erlaubt die vollständige Integration der genua-Fernwartung in eine zentrale Nutzerverwaltung mit unternehmensüblicher Multifaktor-Authentifizierung. Unternehmen profitieren damit von skalierbaren Mandanten-, Rollen- und Rechte-Konzepten und Nutzer können sich über ihr gewohntes Verfahren authentifizieren.

> „Die genua-Lösung wurde sehr gut von den Bayer-Anwendern angenommen und bietet einen großen Mehrwert.“
>
> **Jani Alexander Krämer,**
> **Information Technology Security Analyst bei Bayer**

Entwicklung geht weiter

Um die Sicherheit der eigenen Anlagen eng mit den entscheidenden Erfolgsfaktoren wie Verfügbarkeit und Flexibilität zu verknüpfen, sind weitere Funktionen bereits in der Planung: „In das Web-based Remote Maintenance legen wir viel Hoffnung. Tatsächlich haben mich Verantwortliche verschiedener Standorte bei Bekanntwerden direkt angeschrieben und Interesse bekundet“, sagt Krämer. Der Aufwand dafür sollte relativ gering sein, da lediglich ein zusätzlicher Web-Server in der demilitarisierten Zone installiert werden muss. Zwar hat dieser eigene Security-Anforderungen und erfordert eine eigene Security Review, dennoch „macht genua hier definitiv einen Schritt in die richtige Richtung, da das größte Problem für externe Firmen darin bestand, keine Third-Party Executable auf ihren Firmen-PCs laufen zu lassen. Eine browserbasierte Lösung hingegen kann in allen Unternehmen niedrigschwellig eingesetzt werden“, ergänzt Rocks.

Aktuell befindet sich das Web-based Remote Maintenance in einem Test-Setup und wird auf Herz und Nieren geprüft, damit es auch wie geplant funktioniert. „Das wird denke ich das größte neue Feature sein, das hoffentlich noch in diesem Jahr kommt“, sagt Krämer. Damit wird der Werkzeugkasten derjenigen wieder ein Stück weit größer, die sich intensiv um den Schutz der Anlagen kümmern, damit die rasante Zunahme an Schadensereignissen in Zukunft wirksam begrenzt wird.

> „Die Zusammenarbeit mit den Kolleginnen und Kollegen auf der genua-Seite funktioniert hervorragend, sehr offen, sehr lösungsgetrieben. Hier will niemand so viel wie möglich verkaufen, sondern das Beste für den Kunden.“
>
> **Carsten Rocks,**
> **Global Program Lead „Manufacturing IT Security“**

Weitere Informationen:

www.genua.de/fernwartung

0325-02-DE

Über genua

Die genua GmbH sichert sensitive IT-Netzwerke im Public- und im Enterprise-Sektor, bei KRITIS-Organisationen und in der geheimschutzbetreuten Industrie mit hochsicheren und skalierbaren Cyber-Security-Lösungen. Dabei fokussiert sich das Unternehmen auf den umfassenden Schutz von Netzwerken sowie auf die interne Netzwerksicherheit für IT und OT. Das Lösungsspektrum umfasst Firewalls und Gateways, VPNs, Fernwartungssysteme, interne Netzwerksicherheit und Cloud Security bis hin zu Remote-Access-Lösungen für mobiles Arbeiten.

Die genua GmbH ist ein Unternehmen der Bundesdruckerei-Gruppe. Mit mehr als 400 Mitarbeitenden entwickelt und produziert sie IT-Security-Lösungen ausschließlich in Deutschland. Seit der Unternehmensgründung in 1992 belegen regelmäßige Zertifizierungen und Zulassungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) den hohen Sicherheits- und Qualitätsanspruch der Produkte. Zu den Kunden zählen u. a. Arvato Systems, BMW, die Bundeswehr, das THW sowie die Würth-Gruppe.

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