genua.

Secure Remote Access from a Single Source

A mammoth project in the field of security: The life science company Bayer has standardized remote access to its many different plants and locations worldwide. With help from genua, an experienced cyber security partner, Bayer has been able to introduce important functionalities for its regulated production lines.

By Frank Jablonski, freelance journalist

SecurITy made in Germany

The damage caused to the German economy by cyber attacks skyrocketed again in 2024 – by approximately 29 percent, reaching 266.6 billion euro. For comparison, that is significantly more than half the German national budget. In the meantime, almost every company in Germany has been affected. While theft of customer data or intellectual property, such as patents and research findings, can become very expensive, the digital sabotage of industrial plants or operating procedures has the potential to compromise the plants‘ integrity and thus put people‘s lives at risk. This level of potential damage is particularly relevant to the process industry.

Project Description

The Customer:
Bayer AG

The Task:
To standardize the way in which suppliers and maintenance staff remotely access machines and plants within the Bayer Group, while also ensuring transparency and raising the level of security.

The Solution:
The introduction of genubox as a remote maintenance solution in combination with the genua logging system as well as secure file transfer as part of a comprehensive and tailored genubox security solution.

A Challenge for the Process Industry: Remote Access and OT Security

Manufacturers of chemicals, pharmaceuticals and food are no longer only ensuring the functional safety of their plants – now, they must also protect the integrity of their networks. Commissioning equipment without being on site, performing diagnoses remotely and carrying out monitoring functions from home have gradually become standard for suppliers and service providers. This is because quick external access increases plant availability – but it also leads to a whole host of different access methods and security concepts. The applications employed to enable the use of appropriate, cost-effective devices and methods from the IT world in process plants have become an almost impenetrable jungle, especially at large locations. For an industry that demands the highest standards when it comes to the integrity and security of plants, this is a growing problem.

The Search for a Standardized Solution

An excellent example of how complexity can be reduced while also maximizing security for plant operation is the company Bayer. “The then CISO had the idea of drawing up an OT security program. The aim was for this to create transparency within the overall company regarding how the individual Bayer sites address this topic,” says Jani Alexander Krämer, Information Technology Security Analyst at Bayer. The combination of being hugely beneficial to the company while also posing a high risk of damage made remote access top priority. Therefore, the most important objective of the OT security program implemented at the time was initially to come up with a standardized technical solution for remote access to machines and plants at the different Bayer locations.

> “At the start of a standardization project, there are thousands of reasons why things don’t work. With genua’s support, we always ultimately found solutions that all parties were satisfied with.”
>
> **Jani Alexander Krämer,**
> **Information Technology Security Analyst at Bayer**

The right partner for the job was soon found in IT/OT security experts genua from Kirchheim near Munich. The company, which has since become part of the Bundesdruckerei Group, protects plants and communication processes in networked and automated production systems. The experts design a secure IT/OT infrastructure, work with the users to select the appropriate security products for ensuring network security, and implement these. If necessary, the on-site team also receives training and support.

A Fixed Appointment Is Mandatory

The rendezvous solution from genua prevents one-sided access by the external remote maintenance service. Connections to the plant for analysis or maintenance must take place via a rendezvous server located in a noncritical "demilitarized zone" (DMZ) or with a virtual location in a cloud. The external maintenance service and the person responsible at the operating company each establish a connection to this meeting point at a fixed time. This active step carried out by the user creates the continuous connection required for the flow of information for maintenance purposes. This enables machine values and error messages to be read out and dealt with. Meanwhile, the access remains restricted to a specific time period and area. The external service can only move within the predefined target system and in the predefined role. genua implements this using an application-specific SSH rather than VPN access that covers the whole network.

Almost 100 genuboxes have been installed for Bayer in Germany alone. To start with, it was mostly rack hardware or on-premises technology, but now, virtualized service boxes are increasingly being installed in the cloud – in roughly a quarter of all Bayer's applications.

"When I arrived at Bayer, the genua solution had already been tested in the laboratory and rolled out to 70 locations worldwide. The big challenge we've since overcome internally at Bayer was to create a service out of the technology and turn that into a successful roll-out project – not an easy task in a large company," Krämer remembers.

"With approximately

2,000

service providers, you want to know precisely who is doing what."

The background to this is that many Bayer companies and important suppliers were already using their own security solutions. In cases where the technical implementation of the remote access focused on functionality more than security, people were very willing to switch to the new system. “In many cases, however, it took some work to convince them to accept genua as the mandatory standard solution in the company. Especially where suppliers with their own good solutions were forced to change to genua,” says Krämer.

One topic where assessments differed was the audit trail. “Many companies work in a GXP or GMP environment. In such cases, we have to meet high requirements regarding documentation. We must be able to prove, without a single omission, who was on which system when, and what changes were made,” adds Carsten Rocks, Global Program Lead “Manufacturing IT Security“. In Bayer‘s CISO organization, he develops special security controls for the OT world.

In contrast, the access solutions of mechanical engineers, for example, worked with a pooled back office of third-party companies. As a result, in some cases, it was not possible to tell which operator was behind an account – an unacceptable situation from an auditing perspective.

Access Always Registered and Recorded

Krämer, who performs a kind of service manager role at Bayer, worked with service provider Atos to implement and deploy the necessary programs, adaptations and employee training worldwide.

“genua were and continue to be on hand to help with their technical expertise. Their technical support steps in as level three if there are problems with the service that the provider cannot solve,” explains Krämer, who handles coordination and any classic issues that are escalated.

Now, the genua logging system used at Bayer ensures that users can track all connections – meaning it is always transparent who has logged in, when, what work was carried out and who oversaw it. The recording function that has also been integrated was even developed at the express request of Bayer‘s then management team.

For genua, it has become a unique selling point to record not only logs but also the actual maintenance process in detail. Once the work is complete, the session recording can be archived similarly to a video.

Secure Updates Performed Externally

An additional implementation that has also been carried out recently in close collaboration with the Bayer team concerns the secure file transfer part. Receiving files from outside the organization is one of the requirements that make heads of security break out in a cold sweat. Yet updating or repairing firmware, for example, is precisely what can get a reactor control system or a packaging machine going again in no time at all. In an independent project, this requirement was addressed and scanning for malicious software established. It is now possible to connect an ICAP server that is part of the genubox security solution and checks data connections and files for malicious software before they enter the network. “It is a fantastic expansion that we planned with genua based on the locations‘ feedback and then implemented with the help of our provider,” says Rocks, delightedly.

The implementation of features such as this, which have been requested by end users, is another reason for the high level of acceptance at Bayer: “We regularly receive positive feedback from our users. The productive nature of the collaboration is also clear from the fact that the solution is no longer used only for remote maintenance but now also for internal administration. In addition, we often receive constructive suggestions as to how the service can be expanded further and which additional features would be helpful,” says Krämer.

Seamless Integration

“The main benefit of a remote maintenance solution is the cost saving due to on-site visits by suppliers now rarely being necessary. This saves time and money and helps us to respond quickly – which is particularly valuable in the event of a malfunction, because there‘s no need for someone to be on site,” says Krämer. “In relation to this, I‘d add the increased flexibility. At some locations, employees also intensively use the solution for access when they‘re working from home, for example,” says Rocks. The genua solution gives every Bayer location the choice as to whether the access is, for example, arranged via time-controlled remote maintenance, or whether the security approval is only granted from within the company. It depends on factors such as the division and whether a production line is subject to GMP or GXP rules, how the network has been segmented and whether special IT solutions are in use.

Existing systems can also be used. Connecting to a cloud identity provider such as Okta or Azure Active Directory enables the full integration of genua remote maintenance into a central user management system with commonly used multi-factor authentication. Companies benefit from scalable client, role and rights concepts and users can authenticate themselves via their usual method.

Almost

100

have been installed for Bayer in Germany alone.

To start with, hardware versions of genubox were used in most cases. Since then, the company has increasingly opted for virtualized service boxes in the cloud.

Development Continues

To closely link the security of the company's own plants to crucial success factors such as availability and flexibility, other functions are already being planned: "We are placing a lot of hope in web-based remote maintenance. In fact, the heads of various locations have written to me directly to register their interest after hearing about it," says Krämer. The work required to implement it should be relatively minimal, as only one additional web server will need to be installed in the demilitarized zone. This server will have its own security requirements and need its own security review, but "genua is definitely taking a step in the right direction with this, because the biggest problem for external companies is not letting any third-party executables run on their company computers. In contrast, a browser-based solution can be used in all companies without having to fulfill lots of preconditions," explains Rocks.

A test setup for web-based remote maintenance is currently in progress and the solution is being put through its paces to ensure that it works as planned. "I think it will be the biggest new feature to be hopefully rolled out this year," says Krämer. It will be one more thing in the toolbox of the people working intensively to protect the plants and thus ensure that the rapid rise in damage events is curbed effectively in the future.

> "The genua solution has been very well received by Bayer users and provides a lot of added value."
>
> **Jani Alexander Krämer,**
> **Information Technology Security Analyst at Bayer**

Further Information:

www.genua.eu/remote-maintenance

0325-01-EN

About genua

genua GmbH secures sensitive IT networks in the public and enterprise sectors, at KRITIS organizations and in the classified industry with highly secure and scalable cyber security solutions. The company focuses on comprehensive network protection and internal network security for IT and OT. The range of solutions includes firewalls and gateways, VPNs, remote maintenance systems, internal network security, and cloud security through to remote access solutions for mobile working.

genua GmbH is a company of the Bundesdruckerei Group. With more than 400 employees, it develops and produces IT security solutions exclusively in Germany. Since the founding of the company in 1992, regular certifications and approvals from the German Federal Office for Information Security (BSI) provide proof of the high security and quality standards of the products. Customers include, among others, Arvato Systems, BMW, the German Armed Services, THW as well as the Würth Group.

genua GmbH

Domagkstrasse 7 | 85551 Kirchheim, Germany
+49 89 991950-0 | info@genua.eu | www.genua.eu