

Cybersecurity in Production – The Eight Most Important Things to Know

CYBERATTACK AFTER CYBERATTACK, THE CYBERCRIMINAL "BUSINESS" IS FLOURISHING.

Whereas cybercriminals have so far set their sights primarily on traditional IT, they are now also turning their attention to operational technology (OT). After all, manufacturing and production systems are worthwhile targets. In the following, you will learn eight important things to know about cybersecurity for your production processes.

1.

Cybercriminals Attack Production Systems



When people talk about cybercrime in general, they think of traditional data theft, that is, customer data is captured via a cyberattack on a company's IT infrastructure or via infamous phishing emails and then misused.

But in fact, according to the German Insurance Association (Gesamtverband der Deutschen Versicherungswirtschaft, or GDV), the manufacturing industry is also a popular target for cybercriminals. Citing a Forsa study, the association writes that 26 percent of companies surveyed from the

electrical, chemical, and food industries, as well as mechanical engineering and the plastics processing industry, have already been harmed by cyberattacks. A whopping 71 percent said their operations would be rather severely to very severely limited by an IT outage lasting several days.

Important note: The threats of legal consequences and customers possibly filing claims for damages exist, in addition to incurring material damages and experiencing a loss of public image.

2.

Cybercrime "Business Models"



According to the German Federal Criminal Police Office (Bundeskriminalamt), "cybercrime is one of the most dynamically shifting criminal phenomena. Perpetrators adapt flexibly to technical and social developments, act on a global scale, and attack where they see an opportunity for financial profit."

The general public is generally aware of major cases of data theft, in which hackers penetrate companies' IT systems to steal customer data. This data is then usually marketed on the darknet and used for further criminal activities.

Credit card data or, even worse, access data to other systems obtained via phishing emails are used directly to make financial transactions or to break into corporate networks.

Corporate extortion is another model that unfortunately is equally thriving. Cybercriminals penetrate the systems, block them, and release them only after being paid a ransom, usually in Bitcoin. IT&Production magazine, citing a study by the German industry association Bitkom, writes that the number of such cases has nearly quadrupled from 2019 to today. This model is a major threat to manufacturing companies.

3.

3 Growing Risks Posed by the IoT and WFH Models



IT systems such as the ones in management, marketing, and sales have been more or less separate from those in OT (production-oriented operational technology) until now. Due to the ongoing convergence of IT and OT (think: IoT and Industry 4.0), systems are growing ever closer together – and the threat level is intensifying as a result.

The pandemic-related boom in working from home is also broadening the attack surface. In most cases, home networks in the private sphere are significantly less well protected than systems in the company, and experience shows that awareness for IT security is less pronounced at home, making working from home a risk factor.

4.

4 The "Professionalization" of Cybercrime



Cyberattacks have become a very attractive "business," which in turn means cyberattacks are also becoming more and more professional. One sign of this is the ever more perfect phishing emails, which are often hardly recognizable anymore, even to the trained eye. Another example is emails





that appear to be internal messages, for instance, from the CEO, that prompt recipients to take certain actions, such as making wire transfers (CEO fraud). The speed of such attacks is also impressive; it often takes just a few steps to penetrate a third-party system.

1) <https://www.gdv.de/resource/blob/67186/b85a48cd0808c19fb6681158fa563114/cyberreport-ausgabe-als-pdf-data.pdf>
2) https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html
3) <https://www.it-production.com/news/hoher-schaden-fuer-die-deutsche-wirtschaft/>



According to the GDV (German Insurance Association), 56 percent of manufacturing companies surveyed in the study rate the risk of cybercrime for their industry as high to very high, whereas only 42 percent rate it as such for their own company.

According to the study ...

-  → 62 percent say that their company is too small to be the focus of cybercriminals
-  → 55 percent say that their data is not interesting to cybercriminals
-  → 77 percent say that their IT systems are comprehensively protected
-  → 54 percent say that they have never been victims of cyberattacks.

These, as the GDV calls them, “delusions and reassurance pills” show that awareness of the dangers posed by cybercrime is still low in the manufacturing industry.



Cybercriminals pull out all the stops when it comes to gaining access to their victims' systems so that they can harm them in one way or another. Here's a brief overview – without any claim of completeness:

Injecting malware:

Malware has almost become the most traditionally recognized form of malicious software in the field of cybersecurity. These malicious programs are injected via the Internet, and all it takes to inject them is clicking a link in a fake email. The “infection” can also be carried out via USB flash drives. Hackers can use such malware to gain control over (production) systems or use the access they gain for purposes of industrial espionage. Ransomware is a subset of malware that partially or completely blocks systems, which are then only unlocked after a ransom is paid.

Compromising extranet and cloud components:

Many companies today use cloud-based services from external service partners (think: SaaS, IaaS, and online store solutions). If the external service providers' systems are not optimally secured – this also applies to ensuring the various clients are securely separated – they represent a security risk.

Control components connected via the Internet: Sadly:

Sadly Stuxnet had already gained notoriety in this area in 2010. This computer worm focuses on industrial systems for monitoring and controlling technical processes for automated manufacturing (SCADA). And it gets worse: There's even a search engine that can be used to find systems with open TCP/IP ports. It can be used to run security analyses but is also extremely popular among hackers.

Breaking in via remote maintenance access:

A manufacturer's own technicians or experts often maintain machines remotely. The corresponding interfaces for doing so may be insufficiently protected. This allows hackers to gain access and do things such as seize control of the machines.

Compromising smartphones in the production environment:

Manufacturers of smartphones, or mobile devices in general, repeatedly urge users to install security updates. This alone is an indication of the dangers posed by private devices that are also used for business purposes. It's not for nothing that smartphones are also considered a “smart touchpoint” for cybercriminals.

DDoS attack:

These attacks overload the affected companies' systems with an overwhelmingly high number of requests or data transmissions until it causes a functional failure. The intent and purpose of these attacks is to merely harm or even blackmail companies.

Human error:

Human error or sabotage is arguably the most common cause of these attacks, therefore making it the greatest threat. Examples of these causes include innocently clicking a link in a fake email or a disgruntled or former employee deliberately injecting malware.



Companies can significantly reduce the dangers cyberattacks pose if they know how to disrupt the paths of attack. We provide an overview of potential protective measures below.

Quality and currency of software:

Make sure that you only use software solutions from reputable manufacturers. Also, make sure they're always kept up to date; don't miss any security updates.

Managing access rights:

Managing access rights is a task that is often underestimated. This applies unconditionally to employees who leave the company; all of their access rights must be revoked immediately.

State-of-the-art security measures:

If possible, implement a security solution that's recognized as state-of-the-art and is constantly maintained by the respective manufacturer via security updates.

Creating awareness:

It is vital for employees to be aware of IT security issues. This refers to both the level of awareness employees need to have when dealing with things such as phishing emails and also their ability to recognize the warning signs of potential compromise. The latter is important because a cyberattack should be responded to very quickly in order to be able to limit the amount of damage done.

Performing an IT security audit:

Subject your systems – all your systems, including those in production – to a security audit. This will help you identify any vulnerabilities that could be exploited to carry out cyberattacks. To do this, it's best to work with an external service provider who analyzes the systems in an unbiased manner as part of a "cold eyes" review.

Developing and implementing an action plan:

Use the results of the audit to develop a written action plan to be used in the event of a cyberattack on both you and your external service providers.



SAP applications are used throughout the company – not just in administration, marketing, and sales, but also in production. Examples include SAP PP for planning and controlling production or SAP Manufacturing Execution for controlling, monitoring, and automating manufacturing processes.

Experts are talking about an "SAP security dilemma." SAP applications usually form the backbone of the software environment, but it's difficult to connect them to common security systems. In doing so, the operating model selected to use the applications has no bearing on how much protection is required (Azure, AWS, Google Cloud, on-premises).

A common security solution is Microsoft Sentinel – a cloud-native solution for security information and event management (SIEM) and security orchestration, automation, and response (SOAR). Microsoft Sentinel provides intelligent, company-wide security and threat analysis and detects threats and attacks, responding to them accordingly.

For this solution, a connector for SAP systems developed by Microsoft and SAP with the participation of Arvato Systems is now available. This connector collects various SAP logs and delivers them to Microsoft Sentinel to run the aforementioned security analyses. This means that the SAP system can be automated to continuously monitor for suspicious behavior even after business hours.

This is also an efficient way to comply with the security requirements regarding SAP systems that were issued by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik).⁴

4) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/06_APP_Anwendungen/APP_4_2_SAP_ERP_System_Edition_2021.pdf?__blob=publicationFile&v=2

Your contacts for SAP Security in the manufacturing industry



Achim Reupert

Expert for IT security in the manufacturing industry

Tel: +49 5241 80-49541



Daniel Heer

Expert for IT security in the manufacturing industry

Tel: +49 5241 80-88577



About Arvato Systems

Global IT specialist Arvato Systems supports major companies through Digital Transformation. About 3,100 staff in over 25 locations epitomize in-depth technology expertise, industry knowledge, and focus on customer requirements. Working as a team, we develop innovative IT solutions, transition our clients into the Cloud, integrate digital processes, and take on IT systems operation and support.

We provide

- Comprehensive IT solutions for [Retail](#), [manufacturing](#), and [media industries](#) as well as for [utility companies](#) and the [public](#) as well as the [healthcare sector](#)
- Long-term experience in [Digital Transformation](#)
- Competence in key areas like [Artificial Intelligence](#), [Cloud Computing](#), [IT-Security](#), [Customer Experience](#), [E-Commerce](#) und [Business Process Management](#)
- Know-how in robust technologies and a strong partner ecosystem including companies like [Amazon Web Services](#), [Google](#), [Microsoft](#) und [SAP](#)
- A broad spectrum of infrastructure Services, including [Managed Services](#) and an according [Application Management](#)

As a part of the Bertelsmann-owned Arvato network, we have the unique capability to work across the entire value chain. Our business relationships are personal; we work with our clients as partners so that together we can achieve long-term success.

Arvato Systems – We Empower Digital Leaders.