WHITEPAPER

SECURITY IS OUR PROMISE

INDUSTRIAL SECURITY RIGHT FROM THE START

The complexity of automated machines and systems is constantly growing. More and more components are networked with each other and exchange information - even across company boundaries. The larger the network, the higher the risk that imported malware goes unnoticed and can follow its target. Industrial security must be the basis for industrial networks and not just an add-on. With this whitepaper, we want to explain the risks of digitalized production environments and at the same time offer solutions for countering the dangers and minimizing the risks.

WHAT ARE THE DANGERS AND RISKS?

- Theft of personal data and company data
- Sabotage in order to damage the installations or endanger the environment
- Manipulation to reduce product quality or produce complete rejects
- Encryption of data to extort ransom money

We recommend for every company to carry out a detailed risk analysis in order to determine which risks and areas of attack actually exist and which protective measures are suitable for them.
According to the state of the art, 100% protection is not possible. The goal of the risk analysis is to recognize the possible dangers and to evaluate the effects on the companies enterprise. It makes sense to consider individual machines and systems specifically.

THE USUAL CHALLENGES

- Production plants contain components that dont have their own protective mechanisms (for example, user authentication)
- Partially extremely heterogeneous and complex systems
- External network access is required for suppliers, service partners and employees.
- Human error: makes configuration errors, inserts found USB sticks into the company computer, opens compromised e-mail attachments or surfs on contaminated websites.
- External commissioners or service technicians connect their computer to the company network
- Unhappy employees want to harm the company

Complete protection is not technically possible. Therefore, a security strategy also includes thoughts of how to react in the case of damage. This applies on one hand for forensics to determine the cause and damage of a successful attack - and on the other hand to the define of the measures that are necessary for a rapid restoration of operations.

INDUSTRIAL SECURITY IS AN ONGOING PROCESS

Industrial Security or Cybersecurity is not a single project that has to be completed and checked off - it is a continuous process, which has to be continuously checked and developed according to the constantly changing threat situation.

SAFETY AS A ROLE MODEL

A comparison with safety or functional safety shows how the procedure for industrial security will develop. Today, safety is the standard and machine builders and automation engineers can handle it. It is no longer imaginable today to develop a machine without risk analysis of the safety technology - or that the safety elements installed in it have no corresponding certification. Rather, standards and norms specify how safety components must be developed and applied. Although these legally mandatory requirements do not yet exist for the security of information technology in industry, the methods are known as „security by design". However, they must be applied. The key element here is to consider possible threats during the development process and the design of the automation system. *„With Safety, nobody thinks of building a machine first to make it safe in a second step,"* explains Siegfried Müller, CEO of MB connect line.

RISK ANALYSIS AT THE BEGINNING

A risk analysis can only be carried out on the basis of a concrete application. It is necessary for each new investment. For this purpose, the various possible attack vectors within the plant are considered. These are essentially internal and external interfaces. To the outside, for example, this is the network connection. This can be the company network of the operator or a direct Internet connection via LAN, WLAN or mobile radio. Inside, this can include a USB connection to an HMI device or PLC, a network connection within the system or another possible pluggable interface such as a Profibus plug. All these interfaces are potential entry points for malware or attacks. Apart from the physicality here, someone can exploit weak points in the user logon.

> *„The risk is not only the hacker from the outside. Even own employees can harm the company out of play instinct or intentionally"*

Reports Siegfried Müller from his many years of exerience. After all possible interfaces have been identified, it is time to define possible damage. This can be damage in the event of malfunctions, for example wrong recipes for food are mixed, or a failure or standstill of the system. All interfaces and risks should be listed accordingly and one measure planned in each case.

SECURITY ON MULTIPLE LEVELS

At the beginning it was mentioned that complex networks are difficult to control. The solution is to segment the networks and create secure zones by strictly regulating the exchange of data between the network segments. The concept of segmentation is based on the „Defense-in-depth" approach. This means a defense against cyber attacks across multiple lines. „Once an attacker has overcome the first hurdle, he should only have access to a limited segment and soon encounter the next hurdle," explains Siegfried Müller, adding: „This effectively prevents a malfunction or malware from spreading immediately across the entire network. The „Defense-in-depth" method is also the basis of the IEC 62443 standard currently being developed.

The communication zones are ideally formed by grouping together systems or plant components that functionally belong together and continuously exchange data with each other. Network members that share little or no data are separated by firewalls. A so-called whitelist is used in the firewalls to determine which communication partners are allowed to exchange certain data and use services. Anything that is not explicitly allowed is blocked.
A correct and complete configuration of an IT firewall is of course necessary and requires IT experience and network knowledge on the part of the automation provider. Configuration errors often lead to security gaps.

FUNCTIONALITY AND AVAILABILITY ARE PRIORITY NUMBER ONE

In contrast to the classic IT, the availability of a production line is the most important. This can be explained with a simple comparison: the control of a machining center or a filling machine must react within milliseconds. Whereas it doesn't matter if an office-pc user has to wait for five seconds for a virus scanner. Besides, various systems are used in the production lines, such as industrial controls, control panels and drives, that have no safety features. They offer open access to data and user programs without authentication required. Furthermore „never touch a running system". If e.g. a XP-computer is in a network, its software-plc is approved for a certain service package, updates are taboo due to functional reasons. In the norm IEC 62443 the subject protection of legacy systems can be found under the term „Zones & Conduits". „Conduit" describes the junction between two security zones.

Finally a few principles and general measures with which a minimum protection can be achieved:

- Complex, secure passwords instead of „1234" or „password"
- Replace standard passwords of the manufacturers (condition on delivery)
- Secret passwords instead of post-it at the computer
- Install available patches and updates immediately
- Assign roles to users (Admin only for admins!)
- Segment networks in logical units
- Use 2-factor authentication

THE SECURITY-COMPETENCE OF MB CONNECT LINE

WE STAND FOR SECURE CONNECTIONS

We as a manufacturer of hard- and software for remote maintenance systems and industrial IoT-applications commit ourselves to our customers to develop secure products and services. We guarantee a reliable and fast reaction to emerging security flaws. Our association work and our memberships – e.g. at the Cluster Mechatronik & Automation Bayern e.V., TeleTrusT – IT Security Association Germany and the European Cyber Security Organisation (ECSO) show that the subject industrial security is very important to us. To meet our requirements in this very sensible area, we are constantly working on being able to offer „state of the art" security technology to our customers and users.

SecurITy made in Germany
Trust Seal
www.teletrust.de/itsmig

We are a member of the IT Security Association of Germany (TeleTrusT) and we develop our products under the defined guidelines of TeleTrusT, which allows us to represent the "Security Made in Germany" label. TeleTrusT is a network of excellence, which includes domestic and foreign members from industry, administration and science as well as topical related partner organizations.

Allianz für Cyber-Sicherheit

Furthermore, we are a member of the Alliance for Cybersecurity and we actively cooperate with the Federal Office for Information Security. This enables our development engineers to counteract security threats not only reactively, but above all preventively as quickly as possible.

Nobody can guarantee 100% safety. But you can do the best you can. No exploitable vulnerabilities - this is the result of a tool-protected and manual penetration test by mbCONNECT24 - carried out by the IT security service provider NIXU.

By using Open Source technologies, MB connect line not only stands for maximum security when using the mbCONNECT24 portal, but also for flexibility with the integration of external hardware. Our remote maintenance system works with X.509 certificates, OpenSSL and TLS-encryption. Our servers are hosted in maximum security data centers worldwide.

SECURITY BY DESIGN

The security consideration isn't only important for the development process of an automation project but also for the used products and components. The MB connect line solutions are being developed strictly according to the „Security by Design" principle. Basis for us are the norms specified in the IEC62443. „At the beginning we have put the complete development process to the test", says Siegfried Müller and explains further: „One of our requirements here was the guarantee of a boot process of the operating system, to make it impossible to implant a manipulated firmware on the system". The so-called secure-boot process ensures that only firmware signed by the manufacturer will be accepted. For this, adjustments of the hardware design might be necessary which are only feasible at the beginning of a development.

SECURITY BY DEFAULT

This means that a high degree of security already exists in delivery condition. In concrete terms, this means that all relevant security features of a system are activated and the user – depending on the application – might deactivate security features if required, however the user doesn't have to deactivate them first in any case. With MB connect line that means that e.g. we do without simplified standard passwords and instead deliver each system with an individual password – or the firewall blocks everything at the beginning and the user deblocks single participants within the specific application.

INDUSTRIAL ROUTER

The industrial routers mbNET and mbNET.rokey are equipped with a secure hardware-element (kryptochip) and a secure boot concept, so that units can only boot with signed and trustworthy firmware. The data in the memory are encrypted – and not readable without the key that is saved in the kryptochip.

AUTOMATION FIREWALL

Also during the development of the firewal mbNETFIX the main goal was to minimize attack vectors. Especially with embedded systems a user interface is often being implemented via webserver for the configuration. These webserver implementations mostly show many vulnerabilities and are a potential weak point. The mbNETFIX does without the interface via webserver. The configuration is done by own software, which then communicates with the firewall by using a secure protocol (SSH). By default the communication only takes place via the secured USB port. There is no configuration service at the ethernet interfaces and is therefore not attackable.

CERTIFIED DEVELOPMENT PROCESS

Secure systems and units require a secure development process. Of course the MB connect line development engineers are certified accordingly. For this we rely on an expert certification program of the Technical Supervisory Association (TÜV) in the field of secure software development and on expert knowledge in the field of the IT-security (TeleTrusT T.P.S.S.E.).

> *„IT-security is a management decision for us and clearly the foundation for our future success. The understanding of IT and OT together is the challenge which we gladly accept",*

Siegfried Müller puts it straight.