RECOMMENDATIONS: INTEGRATORS

Security Requirements for mechanical engineers and integrators

Machines and plants in factory automation and other areas are more and more connected with each other and with systems from the business IT. Due to this, they are facing the same threats as conventional IT systems do. There is a long history of incidents where attackers found a way over the office IT or remote access points into production sites. To cope with these threats requires proper measures during planning, integration and operation.

The responsibility to handle vulnerabilities can not only be the duty of vendors or suppliers of single components that are used in a machine or plant. Also the asset owner running a site can not guarantee secure operation all by himself. Mechanical engineers and integrators are the essential link between vendors and asset owners. It is their duty to establish proper measures and processes in order to guarantee an adequate security level at the time of installation until the machine or plant is being operated and to keep up maintenance and a suitable information flow regarding security.

The essential role of mechanical engineers and integrators is pointed out in the guideline VDI/VDE 2182 'IT-security for industrial automation'\(^1\). This guideline describes a process model for implementing proper security controls in industrial automation with real-life scenarios for sample application. Its process-oriented, cyclic approach covers the complete life cycle and the cooperation necessary between vendors, integrators and asset owners. There is also a special focus on the information exchange between these. Figure 1 on the following page gives an overview of the dependencies that are covered in VDI/VDE 2182.

1 Secure by Design

Mechanical engineers and integrators should adopt and apply the 'Requirements for networked industrial components' defined by the BSI. These requirements cover the following aspects regarding development life cycle, technical details and documentation:

- policies for secure development
- security analyses
- general prerequisites for secure operation
- security of services and interfaces
- account and user management, security of passwords and other credentials
- secure baseline configuration (secure by default)
- backup & restore
- remote access
- malware protection
- patch management

\(^1\) VDI/VDE 2182, [http://www.vdi.de/technik/fachthemen/mess-und-automatisierungstechnik/richtlinien/](http://www.vdi.de/technik/fachthemen/mess-und-automatisierungstechnik/richtlinien/)
2 Secure integration (secure in deployment)

In addition to functional aspects, cyber security should be considered as an essential part of planning and integrating a machine or plant. Some general design decisions can be made independently from individual customer requirements, such as:

- Horizontal and vertical segmentation, e.g. by using dedicated firewalls or by defining minimal requirements for firewalls already present at the customer site
- Implementation of additional security controls (e.g. device control, application white-listing, logging mechanisms, etc.)

There should also be an analysis whether the combination of multiple components can result in new vulnerabilities which can not be foreseen by their respective vendors.

3 Individual modifications (secure in deployment)

During the process of integration, a machine or plant should be subject to modifications aiming at accurately fitting them to both general as well as security-related requirements at the customers site. Therefore especially the following measures are necessary, which might require mutual efforts of integrator and asset owner:

- System hardening of the machine or plant and all components in its context (HMI, engineering workstation, etc.)
- Adjustment and activation of security mechanisms, followed by thorough tests regarding both functionality and security
- Definition of policies for the personnel covering topics such as awareness or usage of removable media
- Compilation of an inventory list of all components (hardware, software) being used in the machine / site including their version numbers which can be used in the asset owner's security management
• Update of the customer’s network map

• By providing useful information, e.g. on requirements and identified remaining risks for machines or plants, the integrator can give vital input for the asset owner’s security management. If such an ISMS is not established by the customer, the integrator should point out the necessity of it. Generic publications, such as the 'ICS Top 10 Threats and Countermeasures' by the BSI, can be used as a guideline for getting started with security of industrial control systems.

A Site Acceptance Test (SAT) can be combined with a security analysis in order to evaluate the security of the machine or plant at the time of installation.

4 Secure Operation

The most important duty after a machine or plant has been integrated is to keep on providing information necessary for the asset owner in order to support secure operation of the site. This includes information of vulnerabilities found in the integrator’s code as well as in components used from other vendors (e.g. PLC or software libraries). It should be the integrator’s duty to provide such information since only he has a full insight to the machine’s internals and only he can tell which vulnerabilities are relevant and which are not.

A short-term providing of software patches is an important step towards security responsibility. But in most cases, the installation of patches is not possible or would result in high costs. Therefore it is much more important to give the right information out to the asset owners. If an asset owner is aware of a vulnerability that he rates as critical, he might be able to implement alternative security controls which can eliminate or at least mitigate the resulting risk. Further information on this can be found in the BSI recommendation 'Vulnerability Handling'².

Patches, updates and other software components have to be made accessible on a trustworthy basis. Technical measures, such as checksums or certificates, should be deployed to offer secure downloads. In addition, the security of the website which offers these downloads should be taken care of in order to prevent e.g. waterhole attacks.

Patches should be included in new machines or plants short-term. Asset owners should be given early access to information regarding support and maintenance (e.g. end of service life).

5 Further reading

In addition to the publications mentioned before, the following is recommended for further reading.

• BDEW Whitepaper, http://www.bdew.de/internet.nsf/id/it-sicherheitsempfehlunge

By means of the BSI publications, the Federal Office for Information Security (BSI) publishes documents about current topics in the field of cyber security. Comments and advice from readers can be sent to info@cyber-allianz.de.