RECOMMENDATION: IT IN PRODUCTION

Industrial Control System Security

Insider threat

In the past, industrial control systems were almost only threatened by local attacks due to a lack of networking. However, this inside threat issue has not become obsolete due to the presence of new cyber threats. It has rather become more relevant due to increasing division of responsibilities. Here, the focus is not only on attacks against the industrial systems of an operator. Since all service providers and business partners involved form an additional attack vector as potential inside threats, the entire supply chain must also be taken into consideration.

Potential inside threats include all persons with (privileged) access to IT components, IT services, installations, documents, or any other possibly critical information and devices. The following groups of persons must be mentioned in particular:

- Persons with direct physical access to control systems (e.g. operators, engineers)
- Persons with privileged rights (e.g. administrators)
- Persons with indirect access, e.g. even to the office network or administration buildings
- Employees of service providers (e.g. maintenance or software development), suppliers, etc.

Inside threats pose a risk that can never be ruled out completely because of their nature. Therefore, it is important to take appropriate precautions in order to manage the threats accordingly. However, both the internal employees and external employees must not get the impression that they are under general suspicion.

This document contains a number of recommendations on how to handle inside threats. In doing so, it absolutely makes sense to consider this topic together with other topics such as remote actions and maintenance. However, such topics are not the focus of this document, since separate BSI publications on cyber security are being drawn up in this regard.

1 Possible attacks

The following types of attack must be taken into account when considering inside threats:

- Loss and/or theft of information (data leakage) through accesses to file servers, data storage media, or IT systems. Along with electronic documents, physical documents must also be taken into consideration, of course. The reasons for data...
thefts include both industrial espionage and whistle-blowing (disclosure of shortcomings; cf. Wikileaks).

- Social engineering – particularly in order to prepare follow-up attacks, e.g. by determining contact persons, process descriptions, IT architectures, recipes, or control programs. Persons with access to certain areas may additionally incite employees to actions, such as installation of software using external removable data media, configuration changes to IT systems, or disclosure of cryptographic keys, in order to open attack paths.

- Sabotage – particularly motivated by political or economic interests – constitutes a possible form of attack entailing an increased risk caused by inside threats. For example, this includes manipulating control components or implanting malware or spyware. Such malware may furthermore be implanted (accidentally) through negligent behaviour.

2 General organisational safeguards

The following organisational safeguards (security controls) are suitable for preventing the risk caused by inside threats. These safeguards should be taken into account within security management and in the security concepts to be defined.

- Inventory: Listing all potential inside threats, as well as their privileges constitutes an elementary safeguard. This includes documenting all access options and/or accounts for users, administrators, and external employees, whereby function/group accounts in particular are analysed critically. Especially for external employees, valid Service Level Agreements and other agreed arrangements (e.g. Security Policies) should be collected. Such a process of collection is implemented as an ongoing process and/or as a part of security management. It should be performed in combination with IT asset management, i.e. the administration of the networks, systems, applications, documents (e.g. file servers), as well as the personnel in an overall view. In so doing, aspects such as remote action and maintenance should be addressed as well. For example, system analyses, interviews, and on-site visits may be used for collection.

- Definition of policies for different groups of employees: This includes behavioural rules regarding the use of removable storage media or provisions regarding the handling and disclosure of documents. Employees must be trained according to these policies and their awareness for them must be raised. External employees should be obliged to comply with the policies of the commissioning company and should be trained and/or instructed accordingly. In so doing, local – e.g. geopolitical – circumstances should be taken into consideration particularly regarding companies which operate and/or distribute internationally.

- Identity and authorisation management: If authorisations are no longer necessary, they must be revoked immediately (IT & physical authorisations). This also includes the process of changing the passwords of the respective group/function accounts. Appropriate processes ensuring a secure and consistent condition must be defined for newly hired employees in particular, as well as for employees leaving the company, and employees switching roles within the company ("Starters, Leavers & Movers"). For example, this includes the return of IT devices, authentication tokens, or ID badges. The personnel deployed is subjected to regular checks – above all in the particularly critical areas (background check). Furthermore, employees should be made aware of the duties and responsibilities, as well as the consequences of non-compliance.
• Establishing a change management: Ad hoc changes ("on demand") to systems must be ruled out explicitly. Security-critical processes should take into consideration the principle of separated roles (separation of duties), as well as the two-man rule in particular.

• Enforcement of a stringent access control: Access to the company generally, as well as to different areas, should be restricted. It should be possible to unambiguously differentiate between employee and/or visitor ID badges with different authorisations (e.g. colour-coded).

• Key management: Keys for activating remote maintenance accesses using a key switch are locked at a central location and only issued if required. For this, a key log must be maintained containing information as to when which key was handed out and whom the respective key was handed out to and/or when the respective key was returned.

• Whistleblower: Above all, internal employees should be provided with an internal facility for indicating shortcomings in a confidential manner.

3 Additional technical safeguards

In addition, the following technical safeguards are suitable in order to establish protection against inside threats that is as comprehensive as possible overall. In so doing, it must be the goal to bundle these safeguards as centrally as possible – for example in the form of Security Information & Event Management (SIEM) and Identity & Access Management (IAM / IDM).

• Using sufficiently secure authentication mechanisms (e.g. tokens) allows for high levels of security. If possible, only individual accounts with sufficient authentication (e.g. multi-factor) should be used.

• When using access control systems, including digital badges, it is possible to check the specified access restrictions with the help of technical measures. Such digital badges may simultaneously be used as tokens for logging in to IT systems (synergy effects). Access controls may additionally be supported by video surveillance within the framework of the legal possibilities, for example.

• For control systems (e.g. programmable logic controllers, PLCs), any possibilities available should be used so that any operator intervention must be protected by an authentication or according to the two-man rule.

• Restricting the access options to resources using technical security components (firewalls, unidirectional gateways) ensures that the necessary data can be retrieved from other areas (e.g. office network) without this simultaneously resulting in critical possibilities for influencing IT systems.

• Mechanisms for timeouts of user sessions and password-protected screen savers available in IT systems should be used as far as possible.

• Implementation of virus protection on network- and possibly host-level for servers, workstations, and terminals: Depending on the scenario, application white-listing may also be implemented as an alternative in order to restrict the admissible applications and processes. (Removable) data storage media of external employees and/or from other areas of the company (e.g. office network) are subjected to a virus scan before being used in the production network, for example by using specific terminals (removable storage media checkpoint).

• Use of device control solutions in order to prevent any use of inadmissible removable storage media and USB devices.
Along with safeguards taken in order to prevent the occurrence of security incidents caused by inside threats, safeguards capable of revealing such incidents are of particular importance.

- Options for detecting manipulated and compromised systems and data are provided by automated monitoring of IT systems, as well as their configurations and log files. For example, CPU and memory utilisation, number/profile of processes, number and type of network connections, failed authentication attempts, established network routes, data volumes, or hash values obtained using the configuration data can be collected and monitored continuously.

- New IT systems and network components should be detected automatically within the network. This applies to both wired and wireless networks (e.g. WLAN access point).

4 Safeguards for external employees (third-party companies)

- Third-party companies appoint a contact person for IT security issues.

- Security incidents on the part of the third-party companies must be reported immediately to the specified contact person in the commissioning company.

- Legal non-disclosure provisions (non-disclosure agreements, NDA) are indispensable.

- Any subcontracting, as well as the use of outsourcing or external cloud services require the explicit written consent of the commissioning company.

- Third-party companies must have established identity management and an authorisation concept for their own IT.

- The website of the commissioning company should provide a service which technicians may use to register for a visit and where the technicians may/must acknowledge the provisions and policies as well.

- External service notebooks are subjected to a security check, and subsequent issuance of a visitor certificate in order to be able to access the network.

- Confidential data is only transmitted and stored by external employees in an encrypted manner.

- External companies must be certified in accordance with the established standards, such as IT-Grundschutz or ISO 27000.

- Third-party companies are only allowed to access particularly critical areas under certain conditions, e.g. accompanied by an internal employee or only during the day shift.

- Accesses to internal IT systems are configured with a time limit.

- Accesses and changes to critical IT system are subject to a sufficiently secure and detailed logging mechanism.

- Right to audit: The commissioning company is entitled to check the compliance with the security provisions and/or to have it checked by third parties.