Required data for the risk assessment

# Use Case 2: Digital Substation

## 2.2.1 Identify scope

Typical questions to help determine systems to spot check

|  |  |
| --- | --- |
| Question | Answer |
| Is the operating system up to date? | No |
| How are software updates handled? Are suitable procedures in place? | Only Workstations. Through authorized personnel, connect to the network locally and update. |
| What about software security patches, how are these handled? Is there a patch management policy? | Only Workstations. Through authorized personnel, connect to the network locally and patch. |
| Are antivirus and malware protections up to date? | Yes |
| — Is there a procedure to update the OT systems? | No |
| — Is there a procedure in place for OT systems to react on known vulnerabilities? | No |
| Are passwords used and changed at the expected intervals? | Used but not changed |
| Are the default passwords changed? | Yes |
| Are there means to detect and identify cybersecurity incidents and intrusions? | No |
| Are there any security logs available (e.g. virus and malware detections)? Are they used? Reported? | Firewall and SCADA-workstation only |
| Do we have a security breach response plan in place? Is it known? | Yes, and yes (if something is weird, call someone) |
| Are admin rights limited? | yes |
| Is Email and web browser protection implemented? | No |
| Are there access controls for the wireless network (see [3.2]) | Not relevant, no wireless network |
| Is encryption used? Where? | No |
| Are personal USB and data storage devices allowed on the company network? Are USB sticks scanned? Cleaned? Blocked? | USB sticks are allowed, scanned, cleaned, not blocked. |
| How is data stored on company phones/PDAs disposed of? Are disposal policies applied? | Not relevant, no phones and PDAs. No disposal policies are applied. |
| Where are the backups stored? Are storage devices tracked? Are the backups tested? | On external hard drives, not tracked, not tested. |
| Are employees trained on cyber security policies? | Yes (use of password, incident response) |
| Are contractors screened for adequate security clearance? | Yes |
| Is external access allowed for sub-suppliers? How is it controlled? | Yes, through a jump (Engineer PC) |
| Is the remote maintenance performed adequately logged? | Yes |
| Are satellite and radio communications secured? | No relevant |
| If the system is intended to be kept behind locked doors, is the physical security and boundary defense implemented? | Yes |
| Is the system secured against theft, fire, and accidental damage? | Yes |

## 2.2.2 Identify threats and consequences

No data

## 2.2.3 Identify incident prevention barriers

Existing barriers:

* Firewall
* Physical security
* Network segregation
* User Access Management
* Training

## 2.2.4 Identify consequence reduction barriers

Existing barriers:

* Data Backup
* Redundant components (some)
* Incident response plan

## 2.2.5 Check barrier robustness and effectiveness

No data