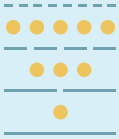
advenica

10 measures for SCADA security

In this guide, we compile the various security measures with which you commonly need to work!

1. Malware protection

Infected websites, suspicious e-mail links or e-mail attachments are common attack vectors that can lead to malicious code sneaking into your system. The best protection against malware is found in antivirus software with features such as automatic updating, malware removal, browser security and detection of all types of infection.



2. Segmentation

Segmentation means that the systems are divided into different security zones. It can be done since all systems do not need the same level of protection. Giving all information the highest level of protection is neither practical nor economically sustainable. Properly executed segmentation results in a deep defence that can effectively withstand a sophisticated attacker. The process means that all information flows between the systems are supervised and monitored, i.e. that information is checked before it is allowed to enter a zone (to protect the integrity of the zone), and checked before it is allowed to leave the zone (to protect the confidentiality of the zone). A security/information policy governs which the permitted information flows are.

3. Monitoring and logging

Operational monitoring supervises the business's IT systems, primarily in terms of availability. From a security point of view, it is most important that you monitor the security functions you have installed.

Logging means that information about events in the system is recorded and stored with the time and the involved resources. A logging system can, for example, monitor operating systems, database managers and application servers or applications. By using logging, you can follow up on the deviations. To have intrusive detection/protection, access control, etc. without having logging with "incident response" is much like having a burglar alarm but not caring or doing anything when the alarm is triggered.

4. Identity and access control

Inappropriate permissions and old user accounts entail an increased risk of fraud and unauthorised access to sensitive information. Proper management of permissions reduces these risks, improves the user experience (shorter lead times for permissions orders) and reduces costs (for instance for licenses, helpdesks and administration).

An important measure is that accounts must be personal and there should also be few administrator accounts. Logouts should be done automatically as far as possible (always in the case of administrator accounts). In SCADA environments, machine accounts are at least as common as accounts linked to a person. This type of account must also be per machine or service.

Another important thing is password management. It is e.g. not good to have the same password on different accounts. In some cases, not only passwords are sufficient for authentication, but multifactor authentication must be introduced.

5. Intrusion detection

Intrusion detection identifies illegal activity in networks and systems. The system analyses information from various sources to identify possible security breaches. Do not forget to monitor the systems and act on the alarms generated (see logging).

6. Encryption

Encryption makes information impossible to read for anybody who is not approved. Decryption is required to make the information readable. The information is completely protected against unauthorised eavesdropping. Encryption should be used when information is transported over any media or communication link over which you have no complete control. Note that encryption is sometimes unnecessary and may actually be counterproductive from a security perspective. For example, traffic that is transferred between zones must be monitored and controlled and encryption makes this more difficult.

7. Hardening

Hardening a computer ensures that only the user permissions that need to be on a given computer are there; others are removed. You delete or deactivate functions in the computer that are not needed with the purpose of minimising the number of potential attack vectors. You also ensure that the system is updated/patched. The local firewall is configured to allow only what is necessary. E.g. the old and vulnerable SMBv1 protocol is still often turned on when installing Windows-based systems.

8. Software updates

Make sure to do the periodical security updates on computers and other equipment. This ensures the best possible protection and removes any unnecessary security holes.

9. Secure remote access

Many organisations depend on remote access via RDP, for example for suppliers to be able to perform maintenance, or for operating personnel to be able to monitor a facility. Remote access means that there are risks of both misconfiguration and implementation bugs. Use RDP and protect the jump server with an explicit security solution for secure remote access.

10. Physical security

IT security and physical security go "hand-in-hand". It does not matter if you protect your IT system "logically" with access control, segmentation, hardening etc., if you allow free physical access to the systems or the process that the systems are intended to control.

advenica

At Advenica, we have extensive experience with both general security analyses (risk and security analyses) as well as security protection analyses. We can advise you on how to get started with mapping processes and routines from a security perspective. We also provide expertise and unique, technologically advanced, sustainable and future-proof cybersecurity solutions with high assurance for critical data-in-motion up to Top Secret classification. Contact us at advenica.com/en/contact-us

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED