KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

General security recommendations

Krones provides the basis for protection against threats in OT networks by setting up hardware and software components securely. Furthermore, Krones continuously monitors supported components for security vulnerabilities, and issues security advisories.

To permanently ensure a high level of security, Krones recommends implementing the following supplementary measures. Please also observe additional security recommendations listed in Krones Security Advisories at https://www.krones.com/en/security-advisories.php.

Overall information security

- Set up and operate an Information Security Management System (ISMS). This includes creating and revising a holistic concept for industrial security and continuous risk management.
- Before connecting external devices (e.g., notebooks of service technicians, removable media, network components) to your networks, scan each device for malware and document the scans and usage.
- Limit the physical access to your OT networks and machines to authorized individuals only.

OT networks

- Do not directly connect OT networks (or isolated networks) with other networks. If connections are required, set up an industrial firewall between the networks and enforce strict rules to control the network traffic.
- Deploy industrial anomaly detection to detect anomalous network traffic (e.g., originating from malware) at network level.
- Limit the administrative access to network components to authorized and trained individuals only.
- Use managed network switches for your OT networks. Disable any unused Ethernet ports in the configuration.
- Duplicate critical components of your OT network (e.g., firewall) to ensure high availability.

Machines

- Issue access transponders to authorized and trained staff only. Do not attach access transponders to machines.
- Have spare parts for machines available (including industrial PCs (IPCs) and removable media).

Staff

- Regularly train all individuals that access machines and OT networks (security awareness training).

Secure operation

- Regularly backup removable media and configuration files. Test these backups.
- Only use software from trustworthy sources.

Security at Krones

We at Krones give the security of our IT infrastructure as well as the security of our machine components and control systems top priority. Krones is ISO/IEC 27001:2013 certified and applies technical and organizational measures to ensure a secure and safe IT environment. This includes up-to-date operating systems, malware protection, and regular information security awareness trainings. Krones has established the Product Security Incident Response Team (PSIRT) to address any security vulnerability that could affect our products/services. In addition to this, the Information Security Incident Response Team (ISIRT) handles all internal security incidents. Both teams meet on a regular basis and in case of urgent need for action.