KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

General product security recommendations

Below you will find the measures recommended by KRONES for the cyber security of KRONES products and services.

Please observe and implement these measures as an operator to ensure a consistently high level of cyber security for your production networks.

Product security

- KRONES establishes a foundation for protection against cyber security threats in production networks through secure initial setup of hardware and software components during the development and construction of machines.
- KRONES monitors the software components used for vulnerabilities, based on risk and until the end of security support. If necessary, KRONES provides security advisories with solutions such as security updates or workarounds for customers to appropriately address vulnerabilities.
- If previously unknown vulnerabilities in KRONES products and services become known, they can be reported to KRONES in accordance with the KRONES Vulnerability Disclosure Policy (https://www.krones.com/media/downloads/krones-vulnerability-disclosure-policy.pdf).
- For questions regarding the cyber security of KRONES products and services, you can contact the KRONES Serviceline and your known KRONES contacts.

General note

The following measures are generic in nature and should be adapted by the operator to the specific deployment environment, risk profile, and operational requirements of the KRONES product or service.

General cyber security measures

- The operator should establish and maintain an Information Security Management System (ISMS). The ISMS should include comprehensive, regularly maintained controls to ensure the security of industrial products and components, based on current best practices and security recommendations provided by suppliers.
- The operator should establish and maintain appropriate organizational policies and technical controls to detect and protect against malware, particularly malware that may be introduced through removable devices and media such as maintenance laptops, smartphones, and USB flash drives. These measures may include maintaining an inventory of approved devices and media, permitting such media only when no alternative is available, disabling or blocking physical ports, and scanning devices and media for malware before use.
- The operator should establish and maintain physical access controls to restrict access to authorized personnel only, using locking systems and other appropriate protective measures.

Personnel training

- The operator should provide regular cyber security training to personnel and ensure they are aware of current threats to production networks and the corresponding countermeasures.
- The operator should ensure that personnel who interact with industrial products and components receive adequate training on cyber security practices with such products and components.
- The operator should train all personnel on the secure handling of authentication credentials, such as transponders used for user login on KRONES HMIs. In particular, transponders should not be attached to machines and should remain in the possession of authorized, trained personnel.

KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

Network security

- The operator should isolate and segment networks by implementing appropriate organizational and technical controls. This includes the use of managed switches with unused ports disabled, firewalls configured with strict filtering rules, and VPN solutions. Internet connectivity should only be enabled when required for the intended use of industrial products and components.
- The operator should monitor and assess network traffic between different networks, particularly between industrial networks, office networks, and the internet. Monitoring should be performed using industrial anomaly detection solutions.
- The operator should implement redundancy for critical network components and communication links where appropriate.

Secure operation

- The operator should manage security vulnerabilities in a timely and effective manner. This includes evaluating newly identified or updated security advisories and implementing appropriate mitigation or remediation measures when necessary. KRONES Security Advisories are available at https://www.krones.com/de/security-advisories.php.
- The operator should manage authentication information appropriately. This includes passwords, cryptographic certificates, cryptographic keys, and access tokens such as transponders used for login on KRONES HMIs.
- The operator should regularly back up critical data, including project files and configuration files, and perform recovery testing to verify backup integrity and restore capability. Backups should be protected through appropriate security measures.

Cloud security

- The operator should establish agreements with cloud service providers to ensure an adequate level of security, such as through Service Level Agreements (SLAs).
- The operator should use only trustworthy and/or certified providers for cloud-based components and services.
- The operator should implement cryptographic protections and access controls for cloud components