Physical Security Recommendations for Hardware Devices

06/2022
TME12555

Deploy the equipment in a secure location

Custodians should secure equipment from unauthorized physical access.

- Access should be restricted to those who require access to maintain the equipment.
- Restricted areas should be clearly marked for authorized personnel only.
- Restricted areas should be secured by locked doors.
- Access to the restricted areas should produce a physical or electronic audit trail.

Secure access to the device front panel and console port

Deploy the device in a rack or cage that can be locked with a suitable key, or other physical methods. This will prevent access to the physical ports of the device.

Description of Risk

Attackers with physical access to covered equipment can access the device without authorization.

Recommendations

Physical security must be in place to control physical access to restricted areas and facilities containing devices. Devices should be locked behind cabinets or protected by physical restraints that prevent unauthorized access or removal from restricted areas. Access to areas containing covered equipment should only be granted to personnel who require access based on their job function.

Restricted areas should display signs that clearly indicate access is for authorized personnel only. Facilities containing covered devices should give minimum indication of their purpose, with no obvious signs identifying the presence of related functions.

Physical access control devices, such as key card readers, doors and cabinet locks, should be tested prior to use and on a periodic basis (e.g. annually). Resource custodians should produce physical or electronic audit trails to record all personnel's physical access to restricted areas for security incident investigation. Inventory of who has physical access to control devices should be regularly reviewed, and any inappropriate access identified during the review should be promptly removed.

Firmware Updates

Schneider Electric strongly recommends that, prior to deployment, customers ensure their devices have been updated with the latest firmware versions. Customers are also strongly advised to review security bulletins that relate to their Schneider Electric products.

For information on new and updated security bulletins, visit the **Schneider Electric Security Bulletins web page**.