KNX Secure Hardening Checklist

Click or tap here to enter text.

Based on the content of the KNX Cybersecurity Hardening Guide, here is a structured checklist.

General Security Principles

- [ ] Use KNX Secure (IP Secure and Data Secure) wherever possible.
- [ ] Apply layered security: combine KNX Secure with IT security measures.
- [ ] Segment the system into distinct segments.
- [ ] Restrict physical access to authorized personnel only.

Device Installation

- [ ] Devices are securely mounted with anti-theft protection where required.
- [ ] Distribution boards are locked or in secure rooms.
- [ ] External devices are mounted to prevent unauthorized access.
- [ ] Switches in public use binary inputs or push-button interfaces.
- [ ] Touch panels are password-protected.

Twisted Pair (TP) Security

- [ ] Cabling is protected from unauthorized access.
- [ ] KNX cabling is not accessible when routed through public or unsecured areas.
- [ ] Use conventional sensors in exposed areas, connected to secure KNX input modules.

KNX Network Segmentation / Coupler and Router Configuration

- [ ] Filter tables are enabled online couplers and IP routers.
- [ ] Broadcast and individually addressed telegrams are blocked.
- [ ] Filtering is enabled, also when using a visualization system.

KNXnet/IP and OT Network Security

- [ ] KNX IP devices are placed on a dedicated OT network or VLAN.
- [ ] VLANs are configured to isolate building systems.
- [ ] Firewalls and managed IT switches are in place to restrict access.
- [ ] Network Access Control (NAC) is implemented (e.g., MAC filtering).

- [ ] Monitoring tools (e.g., SNMP, Syslog) are active.
- [ ] Vulnerability scans are conducted regularly.

MAC Address Filtering & IGMP

- [ ] MAC filtering is configured
- [ ] IGMP Snooping is configured and verified to work correctly with KNX Routing (e.g., multicast address 224.0.23.12).

Secure Remote Access

- [ ] VPN or encrypted channels are used for remote access.
- [ ] Strong authentication and role-based access are enforced.
- [ ] Remote access is logged and monitored.

Project Handover & Documentation

- [ ] ETS Security and Certificate Reports are generated and shared with the customer.
- [ ] Customers are informed of system security features and limitations.
- [ ] Password management policies are defined and documented.
- [ ] Device certificates are recorded and transferred securely.
- [ ] A list of individuals with ETS access is maintained.