User Note:
Secure configuration of Weidmüller Industrial Security Router

Measurements to protect networks and network devices against unauthorized access.

1. Introduction

To use communicative devices in your application you should take technical and organizational measures to ensure a secure operation. In particular to protect components, networks and systems against unauthorized access of third parties.
This user note shall support you to configure your devices enabling them to provide a certain level of security.
More information can be found at following websites[1]:

- ICS Security Compendium
- Remote maintenance in industrial environments
- ICS-CERT recommended practices

2. Recommended measures

2.1. Avoid exposing devices to public networks directly

- In case the Router is connected directly to a public network (e.g. via 4G) activate NAT masquerading on the interfaces to hide local IP addresses.

2.2. Change default Password

- Change the default password during initial configuration of the device.
- Recommended is a password strength of **at least** 8 signs including small and capital letters, numbers and special characters.
- Change the password regularly.
- Don’t use one password for several applications.

2.3. Update Firmware regularly

- Weidmüller provides regularly firmware updates for the products. You can find them at the website or in the catalog.
- We recommend updating the devices as soon as there is new firmware available. You can see in the update log if there are critical security fixes or function upgrades.
- Via u-link Remote Access Service there can be mass-updates performed remotely.

2.4. Change the Firewall (Packet Filter) settings

- Weidmüller Industrial Security Routers have a performant whitelisting firewall. That means all communication that does not match to a rule top-bottom principle will be dropped. The routers contain one firewall rule by factory default: “Allow All”.

[1] Last visited on November 19th, 2018

- To improve security, make a list of communication which flows via the router. Then add these communication parameters to the Firewall setting for a whitelisting. When all required traffic is whitelisted delete the rule “Allow All” to ensure that other traffic will be blocked.
- The SecureNow! function can assist you finding fitting firewall rules for your application.

2.5. Perform access restrictions

- The device offers the possibility to create various user profiles which can obtain rights on a granular level.
- Only grant access to the persons who need access with only those rights that are needed for their tasks.

2.6. Deactivate unsecure communications

- Deactivate HTTP access of the router on all interfaces.
- Deactivate HTTPS access of the router on interfaces that are exposed to a public network.
- SNMP is deactivated by default. If you use it, please make sure to use SNMP v3 and choose a strong password instead of default.

2.7. Secure remote access

- For accessing your local network remotely, a Virtual Private Network (VPN) is recommended.
- This can be done using an open technology as OpenVPN or IPsec or the Weidmüller solution u-link Remote Access Service.

2.8. Secure physical access

- Secure physical access to the device by locking the cabinet and use a lockable service interface such as FrontCom®.
- With the Port Lock function of Weidmüller Switches, service interfaces can be configured to only allow specific MAC or IP addresses.

2.9. Defense-in-depth

- Secure configuration of a router is a first step in securing networks behind the router. Still components in this network should be used and configured in a secure manner as well to avoid a security breach on the lower network level.

2.10. Regular thread analysis

- Performing a thread analysis on a regular basis lowers the risk of vulnerabilities caused by new technologies and changes in the surrounding networks

2.11. Security during Service

- Use up-to-date security software on the service PC’s accessing the network to prevent malicious software to enter the network from the inner side

2.12. Report vulnerabilities

- Weidmüller has a Security Advisory Board dealing with vulnerabilities. Please report these to us on this webpage so we can improve our firmware and close the potential thread.