CyberDanube:
Industrial and Critical Infrastructure Pentesting

In-Depth Technical Security Assessments of Industrial/Critical Infrastructure Devices

Programmable Logic Controls (PLCs) are used in all modern Operational Technology (OT) infrastructure. They act as key component between physical processes and have direct impact to their environment like manufacturing and/or energy distribution. OT infrastructure and its components are potential targets for attackers from cyberspace, which emphases the importance for deep technical security checks in Industry 4.0.

CyberDanube supports critical infrastructure providers to prevent black-out situations for themselves, and their customers.

Preparation

- Kick-off Appointment
- (If applicable) Fat-client
- Typically three hardware devices (PLCs)
- Presentation and mitigation discussion

The preparation phase of a technical security assessment of a PLC includes a scope definition during a kick-off appointment. Frame conditions like the number of available PLCs, available spare parts and client software (incl. license) are clarified during such a meeting. A comprehensive technical PLC test contains hardware and firmware security testing as well as security testing of exposed interfaces like Ethernet.

Technical Assessment

Testing in the Security Lab in Vienna

- Secure Boot
- General Hardware Pentesting (Debug interfaces, Microcontroller Glitching, Data extraction)
- Testing for memory encryption
- SBOM (Software Bill of Materials)
- Testing for known CVEs (Common Vulnerabilities and Exposures)
- Testing for unknown vulnerabilities (Zero Days)
- Fuzzing

During the technical assessment of an PLC, the full stack from electronic components up to the services exposed to the interfaces is tested. This includes testing of secure boot, exposed debug interfaces, fuzzing, known CVEs, unknown vulnerabilities, reveres engineering of firmware and testing of real-time operating systems like proprietary systems or FreeRTOS.

CyberDanube's outstanding service, namely building a digital twin, has also been leveraged multiple times when testing devices like industrial PLC. This way, much deeper hidden vulnerabilities can be uncovered in such devices in contrast to testing only on the real hardware.

Typical Challenges

Building up a test setup for PLCs requires more than just the controller in a lot of cases. Modular PLCs often require special power modules. Special proprietary software is also regularly needed for test setups. The deep analysis steps are done with hardware tools, software debuggers (analyzing various CPU architecture's assembly code), static and dynamic analysis, which requires broad knowledge. Such issues do not pose a problem for CyberDanube experts in the hardware lab in Vienna.

Typical Findings

- Secure Boot Bypass
- Authentication Bypass in Proprietary protocols
- Vulnerable web-interfaces
- Hardcoded backdoor credentials

A lot of application-level vulnerabilities in this type of devices have been found in the past by CyberDanube experts. Such vulnerabilities can often be identified with the combination of static and dynamic methods in firmware, with final verification on digital twins. Identified hardware vulnerabilities (e.g. unprotected JTAG), in contrast to OS specific issues, remain the same – no matter which firmware was deployed on the device. Therefore it is always worth to test devices in Industry 4.0 & critical infrastructure. A lot of vulnerabilities in PLCs, industrial switches and routers have been published by CyberDanube security experts in the past. They can be found at *https://cyberdanube.com/en/blogs/.*

Experts Contact

Thomas Weber

Founder &
Technical Director

About CyberDanube

CyberDanube is a specialized cyber security company, offering OT, (I)IoT & Embedded Security testing services. CyberDanube provides a unique security toolset & technical consulting, e.g. penetration testing capability with a dedicated hardware lab for in-depth product analysis. With a proven track record in pentesting, research and published advisories including zero-day vulnerabilities, CyberDanube is a trusted authority (CNA) which operates independently from manufactures & investors as trustworthy partner in the security industry.

If you need a Cyber Security Pentest in Industry 4.0 for an Industrial Device,

Contact us via : office@cyberdanube.com

This Whitepaper has been inspired by real word projects.