Date | Version: 10.04.2025 | 1.0 |
Responsible: T. Weber

CyberDanube:
Process Control System Pentesting

In-Depth Technical Security Assessments of Process Control Systems

Process Control Systems (PCS) are widely used across different industries like pharmaceutical, chemical, manufacturing and critical infrastructure. Those critical industries have a significant impact to our daily life and can lead to shortage in various fields, if such control systems are compromised.

Preparation

- Kick-off Appointment
- Maintenance window / precise scope definition
- On-site pentesting

The preparation phase of a technical PCS pentest includes a sharp scope definition during a kick-off appointment. We know that this is crucial to ensure the operation during the pentest as many parts of the PCS are often replications. Therefore, if some parts of the PCS are tested, the results often apply to other parts of the system. Frame conditions like maintenance windows and restrictions or exclusions must be also clarified during such a meeting. A comprehensive technical process control pentest contains network separation and cell testing as well as security testing of the proprietary used (fat) client/server software, if available.

Technical Assessment

Testing On-site

- Network structure testing (cell structure, PURDUE/PERA)
- Proprietary industrial protocol testing
- Sub-system testing (PLCs, RTUs)
- SCADA server/client software testing
- Optional: OT device/product pentesting

During the technical assessment of a Process Control System (PCS), we test the full stack from PLCs, RTUs and other components up to the network structure and SCADA client/server software. Architectural issues of misconfigurations can be detected very efficient this way. Proprietary protocols are also tested if they are defined in the scope of the pentest. An optional part, that we always offer, is dedicated testing of OT devices in our CyberDanube lab in Vienna. The firmware and/or the hardware of such OT devices can be tested in detail without having an impact on the PCS itself. Moreover, there is an increasing number of Process Conctrol Systems (PCS) with connections to the Cloud. Such attack vectors are also covered by the tests if needed by the customer.

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

Typical Challenges

The biggest challenge we are always facing when testing Process Control Systems (PCS) is to have no impact to the live operation. This requires to talk to the responsible technicians before doing crucial tasks for testing the system. Other challenges are mappings of partial scans of the PCS to other parts that are not 100% equal to the scanned part. Ensuring that nothing in the PCS was modified during the test is often the last step after the pentest itself. A lot of challenges are usually gone if testing in a maintenance window.

Remember. Each Process Control System (PCS) is different, even if it is the same vendor, the same product and the same version!

Typical Findings

- Insufficient network separation
- Outdated firmware/software/OS versions
- Dangerous services and features activated in devices and proprietary protocols
- 0-day vulnerabilities in OT devices
- Additional internet connections like GSM routers (often installed by 3rd parties)

A huge amount of the typical findings are also widely known problems in traditional IT infrastructure, but testing of Process Control Systems (PCS) is a different discipline in our experience. The key-abilities of such a pentest is communication with personnel on-site and the precision of the IT Security Specialist, who executes the pentest. This ensures the availability of your system and provides you the best view from an active security testing perspective on your OT systems.

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 Pentest of a OT Infrastructure or an (I)IoT/Embedded Device,

Contact us via : ✉ office@cyberdanube.com

This Whitepaper has been inspired by real word projects.