REDGUARD
SECURING YOUR ASSETS

SMART METER & NETWORK EXTENSIVELY TESTED

In a comprehensive security audit followed by a penetration test, Vilters-Wangs' electricity plant had its network checked for vulnerabilities. This also included the Internet of Things component of the smart meters for remote reading of electricity consumption. The Vilters-Wangs electricity plant operates two networks: one for controlling the production plant and one for reading out the distributed electricity meters (smart meters)..

Technische Betriebe Vilters-Wangs
Elektrizität | Kommunikation | Wasser

As part of a security audit, Redguard tested how resistant these networks are to cyber-attacks.

Defining scope and main focus

In a first step, Vilters-Wangs and Redguard created an overview of the systems and networks together. Furthermore, the exact scope of the audit was defined. This clearly specified the main focus and ensured an efficient use of the available time. The municipality of Vilters-Wangs carried out an audit for the first time. "The cooperation worked well because Redguard's security testers explained all the matters, answered questions and responded to our individual needs," explains Patrik Schlegel, Vilters-Wangs' municipal council clerk.

Network architecture review

Within the defined scope, the Redguard security testers conducted an architecture review of the two networks. This audit is a useful addition to the technical penetration test: the architecture review provides a conceptual analysis of the current situation and sets the main focus for the penetration test.

The architecture review included:

- Weaknesses in the logical process
- Interaction of components
- Operational concepts
- System design
- Network zoning

IoT, Internet and physical access

The predefined target systems were checked by Redguard using penetration tests. Automated tests find weak points that are easy to discover, so-called "low hanging fruits". Through manual tests, the security testers cover more complex system environments and examine hidden attack paths. This allows both obvious, deep and complex vulnerabilities to be detected at an early stage.

Redguard's security testers tried to gain access to Vilters-Wangs' network in various ways:

- Via the Internet using VPN access
- Through access from the IT service provider's premises
- By means of direct connection to the server zone
- Through access to a productive smart meter system of a residential building

Among other things, Redguard managed to intercept the network traffic of the smart meters and analyze the network protocols used. Patrik Schlegel explains: "In the final report, the weak points were systematically identified, including prioritization in relation to our business. The review report serves as a basis for further processing and securing the vulnerabilities."

New zoning to seal off the IoT

Components of the Internet of Things (IoT) such as smart meters are often connected in an easily accessible network – therefore a correct network zoning is crucial. It is important that the IoT network is physically separated from networks containing critical control systems. Redguard examined if Wilters-Wangs' network configuration corresponds to a secure system architecture and checked on-site in the internal network whether the zoning was implemented correctly. This ensured that the smart meters were isolated from the community control system and other smart meters.

Our penetration tests

Benefit from the profound technical expertise of the Redguard security specialists. A penetration test is a technical security analysis that aims to identify vulnerabilities within a defined scope (network segments, servers, applications). This ensures that obvious and concealed system vulnerabilities are detected early on.

„The security review serves as a basis for improving our information security."

Patrik Schlegel, EW Vilters-Wangs

Once completed, the test report delivers clear indications of countermeasures that can be applied to rectify the vulnerabilities.

We offer our penetration tests in the following areas:

Web applications
We help you to identify and systematically address vulnerabilities that may impair your security. To do this, we perform active tests in the role of the attacker.

Networks
Data is constantly moving and is shared back and forth between a variety of systems. This form of sharing is only possible with a stable and secure network. We check whether exclusively your authorized persons have access to sensitive connections and data.

Mobile
We check the security of individual apps and their matching backends. Our tests include the OWASP Top 10 and other application-specific risks.

Docker security
We help you to use container technologies safely and review how they are implemented. We base all procedures on our Container Security Verification Standard.

IoT & hardware
We assist you in ensuring the security of IoT from the concept to the security verification of hardware components, from the update strategy to the JTAG interface.

System hardening
We review whether your operating system (Windows, MacOS, Linux) is adequately hardened and therefore consistent with the necessary security level.

Erstelldatum 10/2019, RG-C0