ICS/SCADA PENETRATION TEST

ICS/SCADA systems are used in a variety of industries, including transport management and public services, and belong to the most critical systems currently in use. A large proportion of these systems and their protocols was developed when the focus was more on functionality and availability than security.

These systems were not expected to be available from the public Internet, but rather would be isolated (Air Gap). The physical isolation of ICS/SCADA systems does not mean that an attacker cannot penetrate this network. Depending on the nature of the system, a security incident may have fatal consequences, such as life threats, sabotage, financial loss, and production outage. In the past, there were notorious attacks on power grids in Ukraine and STUXNET in Iran.

SERVICE OVERVIEW

The purpose of the penetration test is to identify security vulnerabilities and misconfigurations in ICS/SCADA systems to prevent real hacker attacks. The penetration test results in a report and customer consultation. The report does not contain any "false-positive" findings, but only verified vulnerabilities and recommendations on how to remove them.

The penetration test can be performed using the BLACK BOX (no information about the tested infrastructure), GRAY BOX (partial information about the tested infrastructure) or WHITE BOX (full information about the tested infrastructure, including configuration files of devices / settings) method.

The cost of the penetration test depends on the depth of the tests, and the size and complexity of the tested infrastructure. The price is determined after customer consultation, which determines the scope, type of test, and other requirements from the customer.

ICS/SCADA systems may partly be tested using the same methodologies as with the other provided services (infrastructure and web penetration test, VA, IoT, WiFi, reverse engineering, etc.), but there are some important differences. If the testing has side-effects (change of data, unavailability), then these effects are more serious and have more impact than in a typical corporate network, especially when tested in a production environment. ICS/SCADA testing requires more understanding of how the infrastructure works, precise planning, active collaboration, and a team of people with ICS/SCADA experience. It is therefore ideal to test in a backup/test environment that is identical to the production environment, or when the production environment is offline - for maintenance purposes.

Test phases:

- Conversation with the customer and determination of the test scope
- Test plan (Threat modeling) - identification of possible vulnerabilities in the infrastructure (potential attack vectors are identified in collaboration with the customer)
- Testing
- Test evaluation, report
- Presentation of results to the customer

Our ICS/SCADA infrastructure penetration tests usually include:

- Application test
- Infrastructure test
- Wireless network test
- Physical security assessment
- Social engineering
- Code and configuration check
- General safety assessment

Binary House recognizes the importance of expertise in ICS/SCADA testing. Therefore, we cooperate with a major South Korean company that has years of experience and expertise in industrial systems testing.

References:

kt

Singtel

ST Engineering

Other references are available on request.