OT Security Assessment

Scenario

This activity is meant to explore the possible consequences of a successful attack. This could be:

A compromised employee due to e.g. phishing and social manipulation

A malicious insider

A compromised remote access solution

The result of this intrusion is in all cases the same: a threat actor has obtained access to an internal OT environment, and tries to use this access to expand their foothold to enable further attacks that can disrupt production.

Preconditions

We recommend doing this scenario as a "white box" test, where the consultants have access to documentation and the possibility to review the environment with technical personnel. This gives us a broad view of vulnerabilities and potential weaknesses as effectively as possible, and reduces the chance of negatively affecting production systems.

Relevant documentation could include:	• Network and architecture diagrams • Inventory lists of systems, servers, equipment, etc. • Internal policy documents, operational procedures • System documentation

We require network level access to the environments. Our systems must be able to communicate with other machines in the environment to complete the assessment.

We also prefer being given user accounts with different privilege levels: regular employee level to test security features and administrative privileges for vulnerability and configuration assessments

In addition to the above, we need:	• Coordination with relevant third parties • Agreement on the time and duration of testing • Escalation procedures • Written approval to start testing

mnemonic's standard assignment confirmation form can be used to confirm specific details.

Test Execution

There are multiple differences between traditional IT/ICT systems and OT, which means that a somewhat different approach is needed.

In particular, OT solutions will often not have a dedicated test environment, and disruption to a production (or even test) OT environment caused by security testing may have severe impact, potentially including physical damage, or loss of life and health. Because of this, special care is needed when planning and carrying out such tests.

mnemonic suggests a dual approach to assess the security of OT systems:

- **Supporting infrastructure:**
  An OT system does rarely live in complete isolation - it necessarily has interfaces to communicate with traditional IT infrastructure, and also trust relationships with this supporting infrastructure. Furthermore, a cyberattack is more likely to originate from the outside of the OT environment, than within it. Because of this, reviewing the OT system architecture and assessing adjacent IT infrastructure such as network devices, firewalls, virtualization, Active Directory, and similar, will provide relevant and useful insight into the security posture of the OT system, by letting us explore potential attack paths in adjacent ICT infrastructure which could lead to a breach of the OT environment.

- **OT penetration testing:**
  Additional tests can be carried out **within** the OT system, subject to limitations ensuring the safety of the test. Specific test activities will need to be carefully planned and agreed based on the specific architecture and properties of the environment in question. Focus will generally be on careful information gathering rather than more disruptive tests.
  - If a test OT environment exists, it is *typically* possible to do a white box vulnerability assessment of selected OT infrastructure, followed by black-box penetration testing building on the knowledge from the white-box activity.
  - If testing in a live environment, the testing approach will be more limited, and focus on manual vulnerability assessment of selected OT infrastructure, in order to minimize the risks of adverse impacts.
  - As a general rule, we suggest that the OT environments that are being tested should be put in maintenance mode, and/or that they are not operational with critical availability requirements, during the test period.
  - Consultants for such assessments have relevant experience and training in how to conduct this type of testing in a safe way.

Result

The result of the activity will be validated findings and observations, as well as raw data from tools and other supporting materials.

High- and critical severity findings will be escalated directly according to agreed escalation procedures.

Findings will be linked to the various sub-activities and ranked based on mnemonic's assessment of impact.

[1] https://www.rapid7.com/db/modules/auxiliary/scanner/scada/modbus_findunitid
[2] https://www.rapid7.com/db/modules/auxiliary/scanner/scada/modbusdetect/
[3] https://www.rapid7.com/db/modules/auxiliary/scanner/scada/modbusclient/