Exercise planner

Package 2, exercise 1

'Threat actor has access to the network'

Version 1.0

Table of contents

1 Introduction

1.1 Background and scope

Facilities and installations in the petroleum sector are required to have preparedness plans in place for managing serious incidents. The industry is subject to various scenarios involving ICT incidents, but the Norwegian Ocean Industry Authority (Havtil) has, through audits, noted that little or no training is carried out related ICT security in the industrial control and security systems. Considering this, Havtil has commissioned a set of training and exercise scenarios. These exercises have been prepared by Proactima together with Netsecurity and was adapted by Havtil.

The Activity regulation § 23 stipulates that: «necessary training and necessary drills are conducted, to ensure that the personnel are always able to handle operational disturbances, hazard, and accident situations in an effective manner». The Technical and Operational regulation stipulates the same in § 52. This means that the requirements for training and exercise are the same for onshore and offshore facilities.

Training enhances personal skills and knowledge, while exercises test collaboration and response capabilities during an emergency. In addition, exercises can reveal organisational and structural strengths and weaknesses and prepare management for dealing with various crises.

1.2 Structure of this guide

The exercise planner contains several scenarios. Each scenario includes suggestions on which functions are relevant to the exercise. The scenarios can be used for training, tabletop exercises, or incident response simulation exercises.

Part 3 of the guide contains additional information to aid in preparation and implementation. This includes:

- a possible sequence of events prior to exercise start-up
- a sequential incident flow chart
- relevant technical material

2 Scenario

The scenario described in this guide involves the control room operators loosing certain operational rights in the industrial control systems.

2.1 Overview of the scenario

This scenario starts when a control room operator detects that is it no longer possible to change the set point on certain regulators. The responsible personnel for SAS/IACS reset the access rights for the control room operators, but three weeks later, the control room operators again lose their ability to change the set points.

If required, the scenario can be split up according to the time available. Table 1 indicates which functions/departments may be appropriate to include in the different stages of the scenario. To scale down the scope of the exercise, it may be appropriate to play out the roles that are not related to ICT.

Table 1. Summary of roles/functions that can be trained using the various modules.

Task	Stage	Personnel responsible for SAS/IACS	Local operations managers	Personnel responsible for systems operation	ICT department
2.2	Initial events – loss of write access	x	x	x	x
2.3	Escalation – use of dormant firewall rule	x	x	x	x
2.4	Analysis	x		x	x
2.5	System Recovery			x	x

2.2 Initial events – Control room operator loses write access to some set points

The threat actor changes the access rights for the control room operator, and the operators can no longer change certain set points. The responsible personnel for SAS/IACS reset the access rights for the control room operators, but a few days later, the control room operators lose their ability to change set points once again.

2.2.1 Advisory questions

Personnel responsible for SAS/IACS

- How can we uncover what has happened?
  - Why have the control room operators lost write access?
  - How can the system supplier be utilised?
- Who should be notified?
- How can we get an overview of the scope of the situation?
  - Which systems are affected?
  - Which set points are affected?
- How can this situation escalate?
- Can we continue production considering the irregularities that has been identified?
- What measures must be implemented to secure the installation?

Local operations managers

- How will the operation management be notified of the incident?
- How can we get an overview of the scope of the situation?
  - Which systems are affected?
  - Which set points are affected?
- How can this situation escalate?
- Can we continue production with the irregularities that has been identified?
- How will we notify about this incident?
- Will the crisis management team be mobilised?

Personnel responsible for systems operation / ICT department

- How can the personnel responsible for system operations support in this situation?
- How does one proceed to uncover what has happened?
  - Why have the control room operators lost write access?
  - How can the system supplier be utilised?
- How can we get an overview of the scope of the situation?
  - Which systems are affected?
  - Which set points are affected?
- How can this situation escalate?
- Who must be notified?

2.3 Escalation – activities on dormant rule in OT firewall

An inspection is carried out on the firewall log for the industrial networks. Activities on a dormant rule is uncovered.

2.3.1 Advisory questions

Personnel responsible for systems operation / ICT department

- When was the rules last reviewed and how was the review quality assured?
- How do we find out what this rule entails?
  - Could there be a connection between the rule change and the loss of write access?
  - What can be uncovered from the logs?
- How can we get an overview of the scope of the situation?
  - Which systems are affected?
- How do we issue notifications about the incident?
  - Management?
  - Organisation?
  - CERT/SRM?

Personnel responsible for SAS/IACS / Local operations managers

- How will the operations management be informed about the escalation?
- What evaluations are performed in regard to whether the production can continue?
  - Could there be a connection between the rule change and the loss of write access?
  - What can be uncovered from the logs?
- How can we get an overview of the scope of the situation?
  - Which systems are affected?
- How do we issue notifications about the incident?
  - Management?
  - Organisation?
  - CERT/SRM?

2.3.2 Additional action points (dependent of the outcome of discussions/decisions)

- How can we utilise external competency in the investigation of the situation?
- Should we remove the rule or monitor it?
  - What are the evaluations that must be made?

2.4 Analysis

The investigation of the firewall routing rules uncovers that a threat actor has had access to OT, and the logs show that there has been traffic in several servers on the network. The rule is removed and this access to OT is blocked.

2.4.1 Advisory questions

Local operations managers / ICT department

- Who should be responsible in such situations?
- What measures should be implemented on the servers on the networks?
  - Is malware installed?
  - How can the servers be controlled and checked out?
- Is it possible that units in the control network are affected?
- How to inform?
  - Management?
  - Organisation?

Personnel responsible for SAS/IACS

- How can personnel responsible for SAS/IACS support the investigation?
- How to inform local operations managers?
  - How can the reliability of the systems be checked?

2.5 System recovery

The analysis has uncovered that one of the servers may have been modified.

2.5.1 Advisory questions

Local operations managers / ICT department

- When was the last back-up performed?
  - How do we restore the correct configuration?
  - Do we have the ability to restore the system to the state it was before the threat actor gained access?
- What will it entail if information is lost between the last back-up and the time of restoration (log history, etc.)?
  - If information is lost, which types of information is lost?
  - Which consequences can this information loss have?

2.5.2 Additional action points (dependent of the outcome of discussions/decisions)

- It is uncovered that there is an error in the back-up routine. How can we remediate this?

2.6 System recovery

All infected servers were ultimately identified and located. The systems are being reinstalled with the aid of back-ups.

2.6.1 Advisory questions

Personnel responsible for systems operation onshore/ICT department

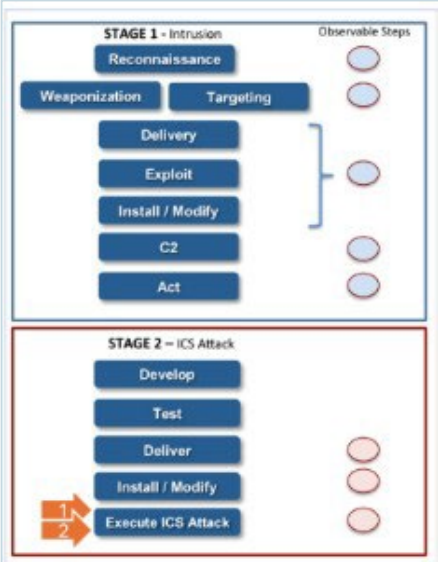
- Should any changes be made to the reinstallation procedures to prevent an identical situation to occur?
- When was the last back-up carried out?
- Are we able to restore the systems to their status prior to introduction of the malware?
- What significance will it have for us if information has been lost in the period between the last back-up and system restoration (technical and operational)?
    - If information has been lost, what types of information is lost?
    - What does this mean for the secure operation and use of the system?

2.6.2 Additional action points (dependent of the outcome of discussions/decisions)

- It appears that there is an error in the routine being used to reinstall the servers. How do we remedy this error?
- How do we involve our suppliers?
- Should we consider a retrospective security test to see if there are other vulnerabilities that can be exploited by threat actors?
- Has a list of indicators been prepared for managing similar incidents?
- How do we ensure that lessons learned from this incident will be applied throughout the organisation?
- How can our company policy regarding information in social media be clarified/emphasised?

3 Additional information for preparation and implementation

This chapter contains background information about targeted cyber-attacks against industrial ICT systems. Digital attacks often adhere to fixed patterns, often referred to as 'kill chains'. The diagram on the right illustrates the various stages making up this exercise, as well as the exercise items incorporated into the guide.



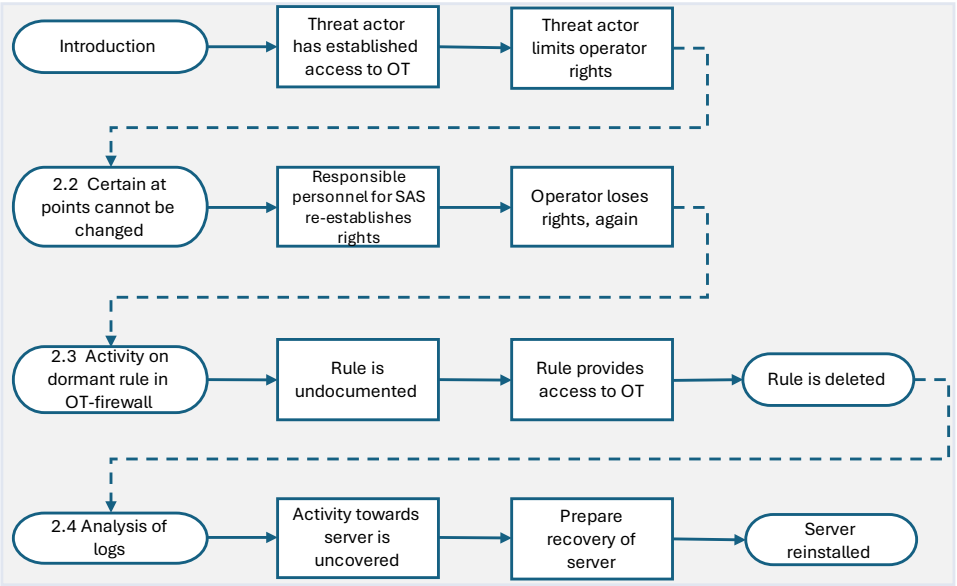
- Threat actor has breached the barriers for stage 1 and 2
- Attack:
  1) Modifications on user access in the operator interface
  2) Repeats modifications
- Exercise points:
  - Root cause for error situations
  - Control of firewall rules
  - Investigation/forensic
  - Recovery

3.1 Introduction to the incident

A threat actor has gained access to the control network by utilising a project-established VPN-connection with adhering firewall rule.

3.2 The incident

Our preparation of the exercise package has been based on the sequence of events illustrated in the diagram below.



3.3 Lessons learned

Review of procedures, improvement of systems to prevent new attacks, etc.

3.3.1 Advisory questions

Discussion leader

- How are the participants involved to provide feedback to the final report from the exercise?

Personnel responsible for SAS/IACS

- Are roles and areas of responsibility adequately described?
- Did the existing procedures support this type of incident?
- Were the procedures adhered to?
- How do we ensure learning across all shifts?

Local operations managers

- Are roles and areas of responsibility adequately described?
- Did the existing procedures support this type of incident?
- Were the procedures adhered to?
- Was any need for enhancing skills to manage similar incidents in the future identified?
- How do we ensure learning across all shifts?

Personnel responsible for systems operation/ICT department

- Are roles and areas of responsibility adequately described?
    - Is the division of responsibility and tasks between the personnel responsible for systems operation and ICT department clear?
- Did the existing procedures support this type of incident?
- Were the procedures adhered to?
- How do we ensure that lessons learned from this exercise is implemented in the organisation?

3.4 Relevant reference material

The sequence of events described in this guide is inspired by the cyberattacks against the power grid in Ukraine in 2015 and 2016. During the incident in December 2015, the operators experienced that they were locked out from the HMI and that someone was overriding manual functions, thus shutting down parts of the distribution network for electricity.

During the incident in 2016, they experienced that switches in the distribution network were opened and the power supply was shut down. When the operators reset the switches, they were almost immediately reopened.

Several of the previous exercises refer to the report *"Analysis of the Cyber Attack on the Ukrainian Power Grid"*[1]. This report describes how a threat actor gained access to the control system networks. The incident in December 2016 uncovered the use of malware that actively override equipment in the industrial control networks. The malware utilises the same protocols as the control system and is therefore difficult to block using firewall rules. This malware is commonly referred to as both Industroyer and Crashoverride. The malware is modular in design and utilises several protocols for communication with field equipment. The blogpost *"VAnalysis: Industroyer/CroashOverride Malware Attack"*[2] from virsec provides a short overview of the incident and the report *"CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations"*[3] from Dragos provides a more in-depth technical description.

[1] nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf
[2] https://www.virsec.com/resources/blog/virsec-hack-analysis-deep-dive-into-industroyer-aka-crash-override
[3] CrashOverride_revised091118