Exercise planner

Package 1, exercise 1

'Social engineering'

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

This scenario involves a threat actor using social engineering to obtain access to the organisation in order to carry out targeted activities against the SAS network and industrial control systems.

2.1 Overview of the scenario

This guide outlines how a threat actor gains access to and compromises control systems on the facility through social engineering.
The following items describe the necessary steps to manage the targeted cyber-attack.

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 – system irregularities in SAS	x	x	x	x
2.3	Escalation			x	x
2.4	Extent of the damage			x	x
2.5	Damage limitation	x	x	x	x
2.6	System recovery			x	x

2.2 Initial events – irregularities in SAS

A minor irregularity is discovered in one of the control systems. This is reported to the personnel responsible for systems operation, who classify it as a random occurrence. Similar occurrences are identified, and after a while an error is detected in a critical unit. A decision is made to replace the unit in question. Shortly after the replacement, the irregularities resume.

2.2.1 Advisory questions

Personnel responsible for SAS/IACS

- How are irregularities in the control systems being managed?
- What are the procedures for incident reporting/notification?

Local operations managers

- What is considered normal irregularities in the control systems?

Personnel responsible for systems operation

- What is considered normal irregularities in the control systems?
- Who is responsible in such situations?

2.2.2 Dialogue with the system vendor

Communication with the vendor reveals that incidents with a similar pattern has been reported from facilities with weak barriers between the office- and industrial networks.

Personnel responsible for SAS/IACS

- Which weaknesses can occur in the barriers between the office- and industrial networks?
  - PCs with access to both networks?
  - Portable media?
  - Other factors?
- How do current procedures protect against social engineering via the exploitation of workplace PCs? (E.g. use of personal e-mail, attachment downloads, software installation, connection to external media, etc.)
  - Are the procedures adequately documented and followed up?
  - Were the procedures adhered to in the period prior to the occurrence of irregularities in the control systems?

Local operations managers

- How do current procedures protect against social engineering via the exploitation of workplace PCs? (E.g. use of personal e-mail, attachment downloads, software installation, connection to external media, etc.)
- Are the procedures adequately documented and followed up?

Personnel responsible for systems operation/ICT department

- What opportunities have there been for weakening the separation between the office- and industrial networks?
  - PCs with access to both networks?
  - Portable media?
- What system logs can be used to identify such factors?
- How do current procedures protect from social engineering via the exploitation of workplace PCs?

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

- How do we identify whether an irregularity is the result of malicious software (malware)?
- How can the organisation enhance its resilience in the face of social engineering?

2.3 Escalation

The ICT department carries out an analysis of the engineering station. Following reinstallation, the station is reconnected to the control network. However, the system continues to behave abnormally.

2.3.1 Advisory questions

Personnel responsible for systems operation/ICT department

- How do we reinstall the engineering station?
- How is it possible for the attack to continue after the engineering station has been reinstalled?
- Is it possible that the malware has spread to other machines?
    - Which resources will be deployed and how will these resources be utilised to identify this?
    - What type of support do we require from the suppliers?
- Who is responsible in such situations?
- Who must be notified?

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

- It appears that all the servers have the same password; only a single user is defined (shared account), and this has local administrator rights. As a result, the malware has spread to other machines in the same network.

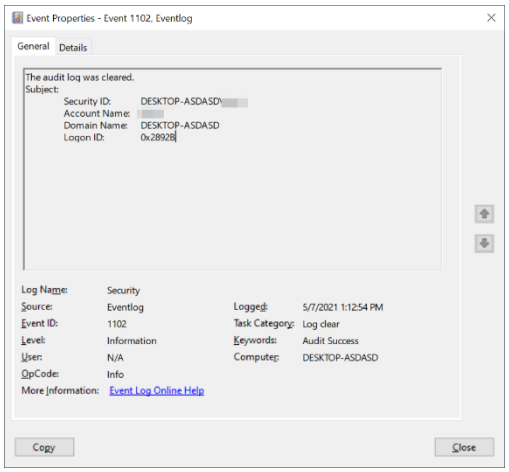
2.4 Extent of the damage

Since it now appears most likely that the malware has spread to several servers in the network, all of these must be analysed to assess what the malware is doing. The figure on the right is an illustration of a possible event log. The event log appears to be identical for other machines.

2.4.1 Advisory questions

ICT department

- What is the malware doing?
- Is the malware operating automatically or is it creating a backdoor?
- Is it possible to obtain indicators from the network showing signs of mapping of services or spread?
- How can the servers be disinfected?
- What technical characteristics does the malware possess?
- Will disinfection/reinstallation of the servers remove all traces of the malware?
- Has the malware caused damage to the control systems?



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

- It appears that the malware is making modifications to the servers that run Windows and is issuing commands that lock functions in the control system.

2.5 Damage limitation

All servers that appear to have had the malware installed are isolated from the network. A temporary solution is being installed to see if the control systems will function normally in this situation.

2.5.1 Advisory questions

Personnel responsible for SAS/IACS

- How can we verify that the control systems are functioning normally?
- How can we verify the configuration of the control systems?
- How do we verify the integrity of the control systems?

Local operations managers

- How can we verify that the control systems are functioning normally?
- Are there any emergency response measures that should be implemented?

Personnel responsible for systems operation/ICT department

- Are there mitigation measures that should be implemented?

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

- The malware has been removed, but there are still irregularities in the control systems.
- Due to inadequate detection, mitigation measures have not accounted for all infected servers.
    - How do we identify the last servers?

2.6 System recovery

All infected servers were ultimately identified and located. The systems are being reinstalled from back-ups.

2.6.1 Advisory questions

Personnel responsible for systems operation onshore/ICT department

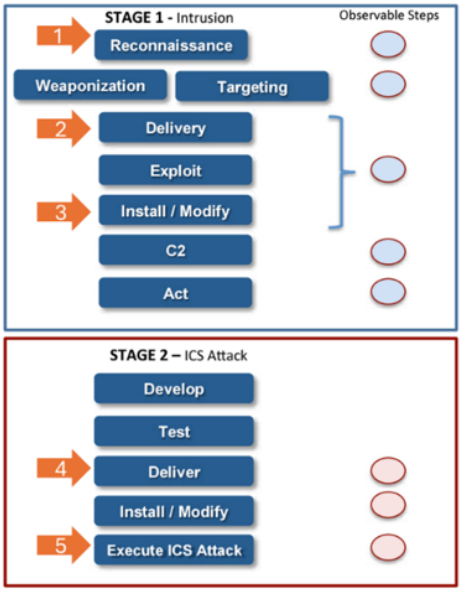
- Should any changes be made to the reinstallation procedures to prevent an identical situation to occur?
- When was the last back-up carried out?
- Are we able to restore the systems to their status prior to introduction of the malware?
- What significance will it have for us if information has been 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.



- Attack:
  - 1) The establishment of relation
  - 2) Attachment in social media
  - 3) Instalment of code
  - 4) Code established in OT environment
  - 5) Execution of attack
- Exercise points:
  - Diligence regarding information in social media
  - Diligence regarding private use of ICT equipment
  - Root cause for errors
  - Recovery

3.1 Introduction to the incident

John Smith is employed in a key position at his company, with access to its industrial ICT systems. His LinkedIn profile reflects his position and provides a summary of his education, the courses he has attended, and his experience. John Smith also has a Facebook profile for personal use where he has entered information that is publicly available, together with additional information available to his 'Facebook friends'. The threat actor in this scenario has conducted a targeted social media search for persons in key technical positions and has prepared a Facebook profile containing similar interests to those entered by John Smith.

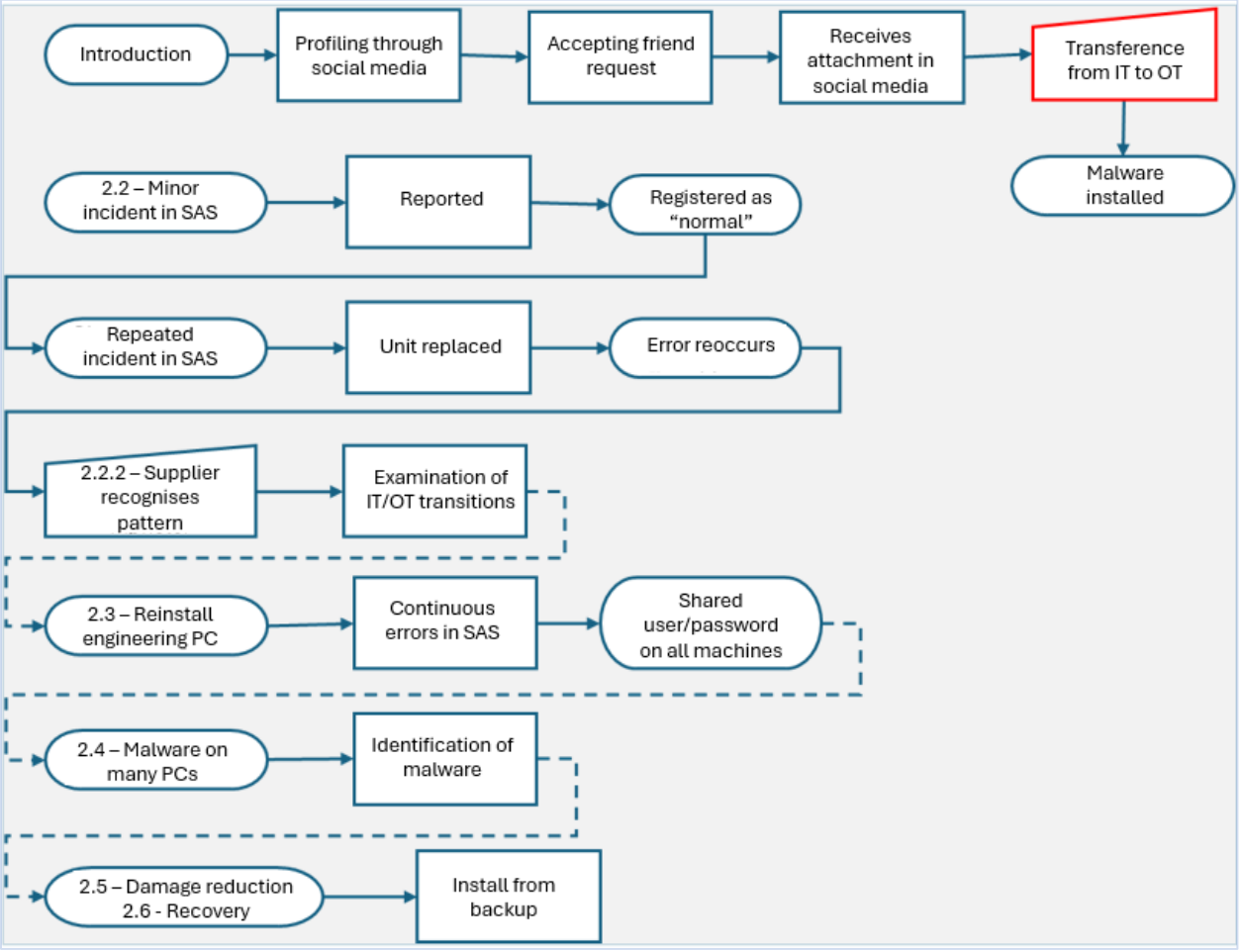
Some time ago, Smith received a friend request including an introductory remark to have met at a concert in Oslo the previous year. Smith accepted the request, and he and the threat actor maintained contact for an extended period during which they shared their interests. One day, while Smith is at work, he receives a Facebook message from the actor with a file attached; 'Concert tickets.pdf'. Smith opens the attachment on his workplace PC without noticing anything remarkable. But the threat actor now has gained access to the network.

3.2 The incident

A threat actor achieves access by means of social engineering, and by conducting a reconnaissance exercise using social media and job advertisements. The attack is initiated by exploiting an exposed employee using social engineering.

The threat actor establishes communication via a concealed channel in an undetected opening in the network. The actor then proceeds to carry out internal attacks on specific targets, combined with automatic spread of installed malware.

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



The sequence of events is initiated by a threat actor, operating on the black market and supplies services on a mercenary basis, often referred to as a 'hacker for hire'. Anonymised networks enable individuals to contact each other to commission cyber-attacks with specific aims against named targets.

The threat actor uses tried and tested attack techniques such as social engineering and the exploitation of known vulnerabilities. Such vulnerabilities are commonly identified using a variety of vulnerability scanners. Human targets are selected based on their social media

profiles, using parameters such as their employer and their positions. In relation to this threat actor, social engineering most often involves a set of targeted operations, which may take anything from days to many months to carry out.
Characteristics for this threat actor includes terrorism and sabotage of industrial control systems. Such actions can result in major negative impacts on commercial interests, health, the environment, and safety.

3.2.1 Properties of the malware

- «Polymorphic» worm that has the same characteristics as a time bomb.
- Establishes foothold in the system in which the malware operates, unpack their attack code, and delete the installation file.
- Creates a backdoor to the infected system which the threat actor can utilise to perform tasks such as the manual exploitation of, and local attacks against, available networks.
- Spreads across networks by reusing passwords two days following its installation.
- Exploits both known and unknown vulnerabilities to attack various control systems.
- Carries out destructive functions, such as modifications to settings (after 29 days). These include data encryption, firmware deletion, and the resetting of system configurations, etc.

3.3 Lessons learned

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

- 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?
- How do existing procedures support incident management?
- Were the procedures adhered to? What modifications should be made?
- How do we ensure learning across all shifts?
- What needs for increased skills have been revealed?

Local operations managers

- Are roles and areas of responsibility adequately described?
- How do existing procedures support incident management?
- Were the procedures adhered to? What modifications should be made?
- How do we ensure learning across all shifts?

Personnel responsible for systems operation/ICT department

- Are roles and areas of responsibility adequately described?
- How do existing procedures support incident management?
- Were the procedures adhered to? What modifications should be made?

3.4 Relevant reference material

Telenor has prepared a booklet addressing cyber threats.[1] It also includes a discussion about how social engineering is carried out. It is commonly men over 50 who allow themselves to be taken in by these techniques, especially e-mail fraud. Fictive social media profiles with many contacts and shared interests can be perceived as trustworthy.

It may be the case that the threat actor includes some of your Facebook friends on his/her list of contacts. When you receive an invitation, such apparent acquaintances offer security, tempting you to accept simply because you share friends with the threat actor.

In December 2015, the hacker group Sandworm carried out an attack on the electricity supply infrastructure in parts of Ukraine. This attack has been discussed in many contexts, including an article from which the abstract on the right is taken.[2]

Analysis of Ukraine power grid cyber-attack 2015

Abstract

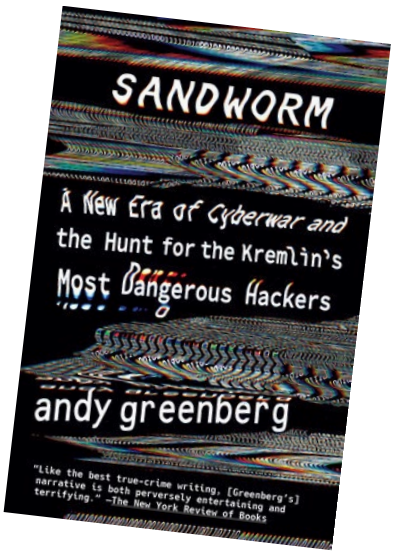
In December 2015, a regional electricity distribution company in Ukraine reported service outages to its customers. The outages were due to a cyber-attack on the company's computers systems and SCADA systems. Seven 110 kV and 23,335 kV substations were disconnected for many hours. Later reports suggested that additional portions of the electricity distribution grid were impacted and forced the operators to switch to manual mode.

The Ukraine power grid attack of 2015 is perhaps one of the most notable cyberattacks in the ICS industry. Over a period of six months, the attackers were successfully able to launch a series of sophisticated attacks that completely disabled the power system of Ukrainian power companies. The paper discusses the sequence of attacks that led to the final failure of the Ukraine power grid. Further it will highlight the details of each attack steps taken by the attacker. This attack vector can serve as the footprint of the potential threats an organisation might face in the event of a similar attack to the organisation.

The report 'Analysis of the Cyber Attack on the Ukrainian Power Grid', published by the security awareness agency SANS in 2016, contains more information about this incident.[3]

[1] https://www.telenor.no/binaries/bedrift/blogg/sikkerhet/sosial-manipulasjon/CTA%20cybertrusler.jpg
[2] https://doi.org/10.30574/wjaets.2024.11.1.0024
[3] SANS-and-Electricity-Information-Sharing-and.pdf (gwu.edu)

The journalist Andy Greenberg has written a book about how Sandworm operates.[4] The Financial Times gave the book the following review: *The true story of the most devastating act of cyberwarfare in history and the desperate hunt to identify and track the elite Russian agents behind it: "[A] chilling account of a Kremlin-led cyberattack, a new front in global conflict".*



[4] ISBN 9780525564638