CYBER Security Spring 2022

Case IV

Cyber Security Incident Response

1 Introduction

In order to challenge, exercise, and elaborate on the knowledge that you have obtained during the lectures and literature studies of this course, you are now asked to apply this knowledge in practise by describing a cyber security incident management situation. The scenario in this exercise is presented in the next chapter. The scenario is fictive, though it is based on events and experience from the industry. The (scientific) base that you are required to have by now is not only based on the lectures and course literature, but also on your own research material and information that you have found on the net (or elsewhere).

The purpose of this exercise is for you to learn to be able to manage a cyber security incident from a given scenario. The expected learning outcomes are the following: You should be able from a given scenario:

- Mange the incident management (in accordance with the incident management process that you have learnt during the lectures)
- Explain how you respond to and resolve the incident (step-by-step)
- Propose improvement actions

The work with the case are structured as follows.

- The case is published in iLearn Wednesday 27th April 08.00.
- The group spends 2 hours working on the case, any time before Friday 29 April 13.00.
- The group members are allowed to meet via on-line communication.
- On Friday at 13.00 the group submits its work in iLearn to the fora called Case 4 Hand-in and it is important that the subject of the message is 'Case 4 Incident Response Group X', where X is replaced by your own group number.
- At 13.00 on Friday the schedule for peer-review is published in iLearn.
- 13.05 the group starts going through the documentation of the group they will peer-review according to the schedule presented in iLearn.
- At 14.45 the group sends their comments and at least four questions to the other group by replying to the original message of their peer-review group, in the fora Case 4 Hand-in in iLearn.
- In this way their documentation, your comments and questions, and then their reply will be in the same message thread in iLearn.
- Now the group reads the answer sent in by the group that has done a peer-review of your group, and this message should be found as a reply to your own original message, with the hand-in of your documentation.
- At 14.45-15.45 the group discuss the feedback from their peer-review group and sends their answers and comments by replying to the correct message in iLearn.
- At 15.45 the group can read the answers of your comments and questions from the group you have peer-reviewed.
- A few days later the groups will get some feedback from the teacher on their documentation.

2 Scenario

Disclaimer: This scenario is meant for educational purposes only. Any resemblance to similar existing names is for realistic and dramatic effect to the case description in question. Casino 10-4 is an online casino with over 12000 regular players every day, and a total of 220 000 registered accounts. The company that owns Casino 10-4 is called Entainence and has 120 employees and circa 10 different departments of which are three IT departments: one for operational IT, one for IT development, and one for IT security.

The company targets Sweden (among other countries), but the operations and head quarter are based in Malta. Since Casino 10-4 is an online service, reliability and stability is of the essence when it comes to IT infrastructure. The company has a primary data centre located on Malta, provided by a third party - specialised in data centre operations.

There is also a secondary data centre located outside the city centre, which works as a backup for the primary data centre site if the primary would go down. Both data centres are of industry standard including backup power supplies with diesel engines, and other relevant and necessary equipment.

The infrastructure is heavily "virtualised" - i.e. composed out of several virtual machines hosted on a VMWare platform cluster. There are 20 Redhat Enterprise Linux servers running the backend of the casino, e.g. bank transactions, web site functionality, databases, even some of the game engines for the simpler games are run on virtual servers. An additional 6 non-virtual Red Hat Linux servers run the backend game engines for the more performance requiring games. There are 7 Windows Servers (Server 2019) that manage user profiles and authentication of staff computers, DNS controllers, internal accounting programs, licence management, and more. Two Solaris (11.4) machines manage the internal storage and backend databases of the company. Each employee has a laptop that runs Windows 10, with an anti-malware software provided by a third party. Updates on these laptop computers are managed by the IT operations department in collaboration with the IT security department and are pushed out once every two weeks.

At the headquarters in Malta, all employees' laptops are connected to the internal network and the internet with ethernet cables. There is also a wireless guest network protected by WPA-2 Enterprise encryption. Some employees (like on-call accountants, the CEO, the head of IT and so on) have access to the internal network over VPN. All network traffic is monitored, logged, and saved for three months. All network routing is handled by Cisco routers, firewalls and switches.

2.1 Incident Description

At 03.41 hours (local time), the incident response manager of Casino 10-4, receives a notification that a possible incident has been identified and registered. The following has been observed: high usage of CPU power on one of the database backend servers. Database backend servers reside on a Solaris machine and the processes that are consuming the CPU power are multiple instances of /bin/scp - a file transfer program, similar to the Unix command cp, that uses the SSH protocol to transfer files[1].

2.2 Task Description

During assessment, the incident response team found out the following from the logs:

- File transferred were initiated from an authorised account.
- The employee has access to the records of all registered accounts.
- File transfers of several instances were started during non-working hours.

[1] https://en.wikipedia.org/wiki/Secure_Shell

When investigating the authenticated account that authorised for the transfers, it appears that it belongs to one of the employees at the financial department that has access to the records of all registered accounts. I would appear to be an unusual time of authentication to start a file transfers of several instances, so you decide to call this an incident and start an investigation.

1. How would you classify the incident? Define in a few sentences.
2. How would you assess and resolve the incident? Describe the steps (in accordance with the incident management process presented in the lecture) and actions taken.
3. Identify and propose post-incident actions.

2.3 Requirements

There is no template for this seminar assignment - you are free to present the result in any way you find most sufficient and appropriate. The following requirements must be fulfilled in order to pass the seminar:

Group size should be 3-4 people

Groups must be registered in iLearn

All group members should be active in the group work

Files should be submitted to iLearn before the deadline

The submission file must include group number

If you have any questions regarding the case, you can use supervision in iLearn. Since the groups can work with the case any time between Wednesday and Friday the teachers may not read the Supervision fora immediately after you have sent the question, so there could be some time before you get the answer. Remember: Internet search engines could provide you with the most detailed and adequate answers for some of the questions that you may have, but if there are questions about the scenario you should post a question to iLearn.