Case 4

Cyber Security Assessment
Group 10

Participants

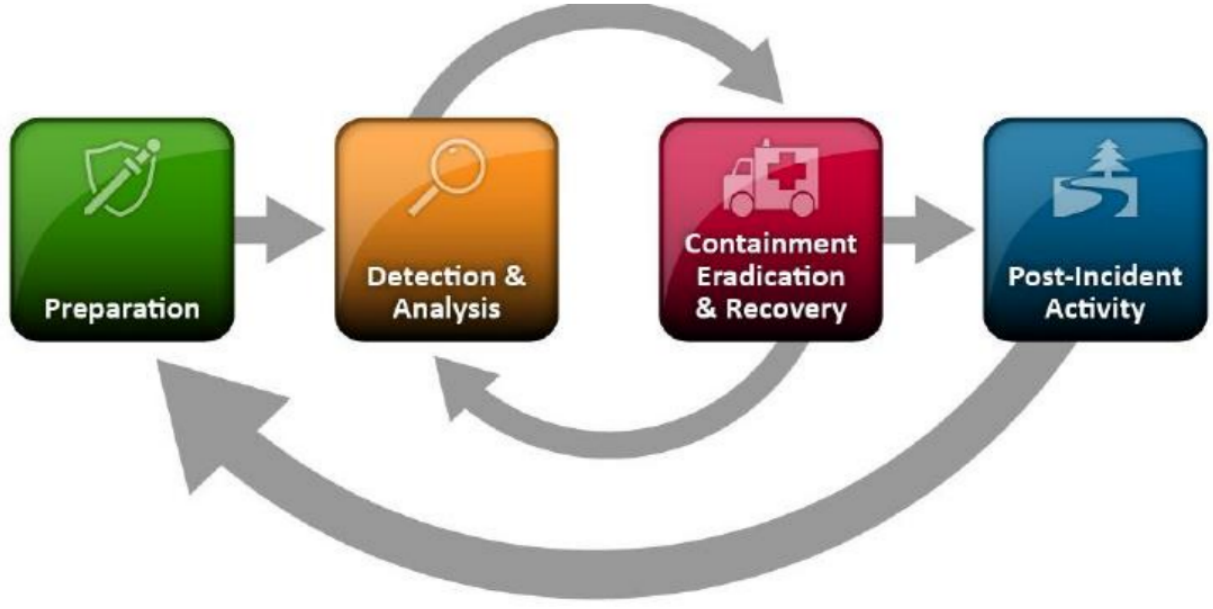
Athanasios Ntales (atnt3398)
Bilal Riaz (biri9477)
Chanchala Fernando (chfe1432)
Emad Abdulsamad (emab9908)
Lekhaz Adapa (lead3201)

Incident Classification:

It has been mentioned, the file transfer was done by an authorized account which supposedly belongs to an employee of the financial department. The event occured during an unusual time so it is considered a security incident caused by a deliberate intentional breach. This incident's cause is not yet fully discovered, since this might have been caused by an unauthorized person who had access to this account or a successful intrusion attempt exploiting a system vulnerability. Therefore, according to ENISA, the incident could be classified as such:

Incident class	**Incident type**
Intrusion attempt	**Exploiting vulnerability / Login attempts**
Intrusion	**Account compromise**

Incident Management Process:



1. **Preparation**

   Before any incident assessment can be completed, the incident response process must be prepared, which includes preventing future events like this. To begin, it should be ensured that the incident response team has access to the essential toolkits, information, journals, logs, and resources, as well as multiple communication and coordination platforms.

- Using a defined approach, categorize and classify a security occurrence or incident (such as NIST 800-61, or other appropriate Incident Handling Guides).
- Helping to build an information security database to share data, compare outcomes, improve alert information, and acquire a clear picture of information system threats and vulnerabilities.
- Guidance for determining whether elevation is required under a process, as well as who should be notified and what steps should be followed.

2. **Detection & Analysis**

   According to the system logs, the incident occured at the company's database, maybe from an employee at the financial department that has been granted remote access. The aforementioned assumption has been made because the incident took place during non-working hours. The incident was reported by the incident response team and more specifically by the incident response manager who received a notification. The compromised areas were the backend servers where a high usage of CPU was observed to one of the databases at 03.41(local time). The purpose of the possible attack was the attempt of intercepting records of registered accounts that belong to the company and that are only accessible by the financial department.

3. **Containment Eradication & Recovery**

   Containment:

- Remove/freeze access to the accounts of the concerned employee(s).
- Obtain all accessible evidence, including a physical computer and event logs.
- Examine logs from recent data extractions to ensure no previous events have been overlooked.

  Eradication:

- Determine where the files were transferred to and, if possible, erase the extracted data.
- Depending on the type of the transferred customer information, take the appropriate actions. If there is a financial liability associated with the accounts, for example, freeze withdrawals if appropriate verification techniques are not included in the affected data.

- Investigate whether the confiscated computer exhibits any signs of being contaminated with malware that could permit use of remote control on workstations. If any evidence of remote access is discovered, security vulnerabilities must be addressed immediately.

  Recovery:

- Document and notify legal authorities if an occurrence involving personal information is suspected.
- Begin an investigation to see if modifications to access control are needed to reduce the likelihood of future incidents.

4. Post-Incident Activity

The Information Technology Service Continuity Plan (ITSCP) is a collection of rules, standards, guidelines, and resources that organizations use to not only enhance their operations but also maintain them. Strengthening their resilience to substantial incidents, ensuring that essential systems and services do not fail or that breakdowns are recovered within acceptable process RTO constraints, as well as their capacity to respond when major system failures will occur.

Lessons learned:

After the immediate emergency has passed, the logs generated from the previously described file transfers, as well as the actions and discoveries made during the containment, eradication, and recovery phases, should be compiled into an incident report. A selected employee should be in charge of determining which lessons has been learnt by the incident using this report as a foundation. It should include how employees and management handled the situation, as well as whether or not documented processes were followed and correct. The nominated worker should also be in charge of determining how and to whom this information should be delivered, such as through training materials or main building meetings.

Post-incident actions:

a. Implementing a stronger primary defense by strengthening access controls and security policies to prevent unauthorized access to sensitive data and systems.

b. Conducting regular security audits and vulnerability assessments to identify and patch any possible security weaknesses.

c. Providing training and awareness tutoring sessions for employees to promote good security practices and incident reporting.

d. Reviewing and updating incident response plans and procedures to ensure that they are effective, up-to-date and with timing accuracy.

e. Engaging with external security experts or consultants to conduct independent security assessments and audits to ensure that all security protocols are effective and adequate.

f. Continuous monitoring and post sanctioned evaluation of the process simultaniously.