IT Forensics – Week 6

Incidence Response

Overview

- Types of Crimes
- Incident Response

Types of Crimes

- When does digital evidence come into play during digital investigations?
- Digital evidence is present in most types of crimes.
- The types of crimes can fall into the following categories:
  - Cybercrime
  - Cyber aided crime
  - Crimes with digital evidence

Cybercrime

- Definition of cybercrime
  - Sophisticated attacks, or high-tech crimes
  - https://www.interpol.int/content/download/5267/file/Cybercrime.pdf
- A computer is used to perform a crime against another computer or system
- For example, hacking, malware attacks, DDOS extortion
- These types of crimes are usually performed by knowledgeable persons.

Cybercrime

- For this category of crime:
  - The means and opportunity would involve specialized use of tools and knowledge of IT / Systems / Programming etc.
  - This can be important in an investigation when trying to identify suspects and the skills needed to perform a transgression should match the suspects profile.

Cyber Aided Crime

- Also known as Cyber Enabled Crime
- Definition:
  - ‘Traditional’ crimes which are facilitated by technology
  - Examples: For example, theft, fraud, even terrorism
  - https://www.interpol.int/content/download/5267/file/Cybercrime.pdf
- Crimes / Offences have been around a long time.
  - Criminals do not have to be computer experts to use the tools etc
- They use the computer/tools to commit a transgression

Crimes with Digital Evidence

- A forensic Investigator can look for and expect to find digital evidence
- Example (Drugs Trade)
- Past – two people meet on a street corner and exchange money/product. What evidence of the transgression is left? Very little.
- Present – If this was online via a social media platform or email what evidence do we have? Even more if the payment is digital.
- In our modern society it is difficult not to leave a digital footprint.

Incidence Response

- Managing incidents in an IT environment
- This process is not particular to digital forensics but it is important to follow process and procedure.

Example 1 - Stuxnet

- Good example of a cyber warfare case.
- Stuxnet was malware that targeted specific controllers (Siemens) that were used in an Iranian uranium enrichment plant.
- It was spread via USB keys
- It infected local networks and contained a very specific payload to manipulate the controllers
- The code lay dormant for a long period of time, it was triggered when specific conditions occurred
- This was clearly targeted and premediated

Example 2 - WannaCry

- Example of Ransomware (2017)
- Infected approx. 200k machines
- Encrypted data on the computer
- Demanded payment to get data back

- Is this an example of specific targeting?

Incidence Response

Establishing Capabilities

- When an incident occurs for an organization it can be a very stressful situation to find the cause and offer a solution to remedy the problem.

Example - MAERSK

- Organisation
- Hit with Not Petya ransomware (2017)
- Forced to reinstall approx. 9k computers
- Large financial loss for downtime
- For a situation like this it is very important to have careful preparation \ consideration in formulating a solution.
- Need to be fast and effective in resolving the issues

Dealing with Incidents

- Need to create a Computer Incident Response Team (CIRT)
- Need to develop policies and procedures
- The goal of CIRT is to know exactly what to do when it is required.

Creating a CIRT

- Identify all roles and competencies needed
  - Technical staff
  - Legal expertise
  - Public affairs / media relations
  - HR
  - Management
  - Etc…
- These roles can be key in managing an incident

Creating a CIRT

- Developing policy / procedure may contain several steps
- These will give the CIRT team a roadmap to better manage the situation
- The document should outline how to react to an incident.

Content for a CIRT Document

- **Define the incident**
  - What has transpired and what type of event requires the activation of the CIRT
  - (Some incidents are general and can be handled by the IT Dept)
  - A DoS attack may warrant the activation of CIRT
- **List the members of CIRT**
  - The document needs the names and contact information for each person.
  - The role each person will perform should also be documented.
  - Some people will need to provide ICE info (eg work mobiles)

Content for a CIRT Document

- **Business continuity plan**
  - Determine a priority of incidents and functions
  - Need to describe what the most important IT assets are
    - This will help create a list of priorities when dealing with an incident
  - The plan is trying to identify what can be sacrificed to protect certain IT assets (priority)
  - What needs to be performed for certain types of incident (eg cut network connection)

Content for a CIRT Document

- **Communication Plan**
- Who to contact and when
  - IT Team members
  - Law enforcement
  - MD / Board of directors
  - Media
  - Specialist Services
- Example:
  - https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Incident Handling

- When something happens, it must be dealt with in a structured way
  - Identify
  - Contain, eradicate and recover
  - Post incident tasks

Identify

- Collect information
- Identify the nature of the incident (if any)
  - Looking at log/error entries
  - Analysing computers/devices
- Evaluate and determine if CIRT activation is needed
- Gather information from users who experienced the incident
  - How it happened, what the user did next
- Information gathered in this phase may be evidence if this goes legal.

Contain, eradicate and recover

- Incident management
- The goal is to try minimize the effect of the incident
- Try to resume standard operation asap
- For containment
  - Try to contain infected devices
- Eradication and recovery are the steps to try recover from the incident
- Example: Restore machines disconnected from the network and reintroduce to the network in a controlled/monitored manner

Post Incident

- Document the incident
- Secure all evidence gathered from the Identify Phase
- Write a report
- Determine what further IT intervention is needed for this case
- Determine if legal action is needed
- Consider the GDPR compliance wrt breech (contact data commissioner?)
- Forensic examination of the material gathered in the Identify Phase.

What role does Digital Forensics play in this?

- Offering specific domain knowledge
- Digital forensic knowledge (process to follow)
- Computer security and knowledge of attacks and exploits
- Triage of incident
- Recommend course of action (ie CIRT activation)
- Conduction a post incident forensic investigation
- Preparing reports etc.

Sources

- The 2017 MAERSK Cyber Incident
- https://techforce.co.uk/blog/2019/maersk-ransomware-attack

- NIST Computer Security Incident Handling Guide
- https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

- Interpol - Cybercrime
- https://www.interpol.int/content/download/5267/file/Cybercrime.pdf

- Kävrestad, J., 2020. Fundamentals of Digital Forensics. Springer International Publishing.

Questions