School of

Engineering and Computer Science

Te Kura Mātai Pūkaha, Pūrorohiko

CYBR 171 T1 2023

Ngā whakapūtanga o Te Haumaru rorohiko

Cybersecurity Fundamentals

Week 11 - Incident response

Material based upon Chapter 1, *Incident Response, Digital Forensics and Incident Response*, Gerard Johansen, Pakt Publishing (2017)

One employee double clicks on a link

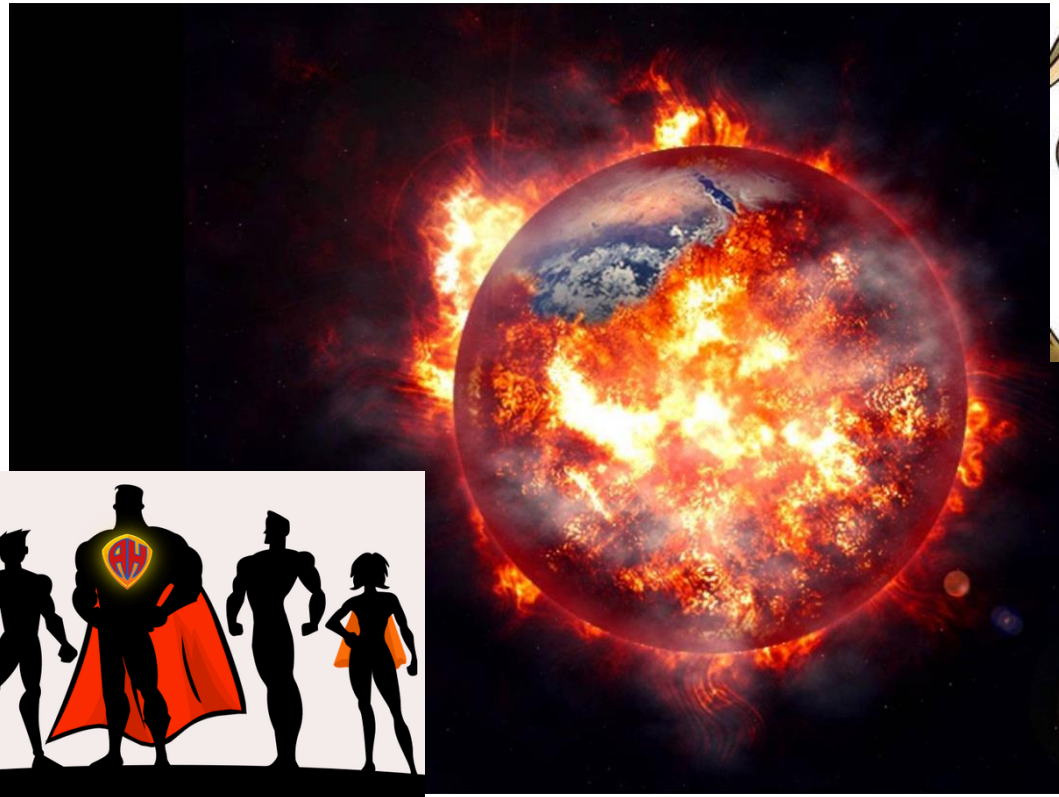
Corporate fileserver is affected

Every user contacts the helpdesk

Business halted - unhappy managers

Technical staff struggle to deal with spreading attack

This is your world



INCIDENT RESPONSE

Incident response

Organisations have security policies and procedures developed during as part of applying operations security.

Need also to have a plan for dealing with security incidents such as a cyber attack.

No time during a cyber attack to respond because of difficulty determining what's happening and how to respond while dealing with users and managers.

Incident response (cont.)

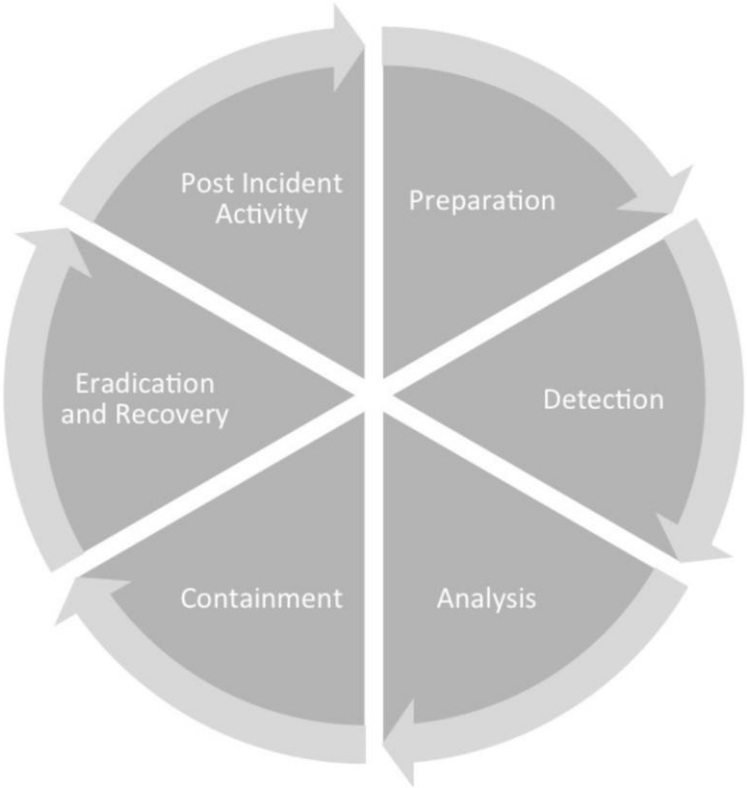
- Incident response capability allows orderly response:
  - Limit damage of attack
  - Recover from potential damages
- Key components:
  - Knowledge of incident response process (nontechnical)
  - Incident response team
  - Plan and processes for handling incidents
  - Keep these plans and processes current and effective

INCIDENT RESPONSE PROCESS

This is not an appropriate process

https://video.link/w/SZDd

Incident response process



#1 Preparation

- Lack of preparation:
  - Hard to respond effectively
  - Might make things worse (e.g. Morris worm)

- Main components:
  - Create a plan.
  - Find staff.
  - Train them.
  - Obtain forensics hardware and software.
  - Run regular exercises (e.g. Tabletop exercises)

#2 Detection

- Events:
  - Observable occurrence in system or network
  - You didn't see it? Didn't happen
  - Examples: connect to server, sending email, firewall blocking a connection event

- Computer security incident:
  - Violation or imminent threat of violation of computer security policies
  - Example: denial of service, phishing, ransomware etc.
- Role of firewalls, access logs, self reporting by users and intrusion detection systems

#3 Analysis

- Collect evidence:
  - Running memory
  - Log files
  - Network connections
  - Running software processes

  Can take hours to days.
- Use tools to examine the evidence:
  - Wireshark
  - Encase (commercial tool)
- Apply root cause analysis:
  - What is the root cause of the incident
  - What were the actions of threat actor
  - Cover time from initial compromise to detection

#4 Containment

- Stop it getting worse!
- Threat actors seek to:
  - Spread laterally to other machines
  - Communicate with **command-and-control** servers
  - Exfiltrate confidential data
- Aim is to block these actions:
  - Use firewall to block IP addresses and ports
  - Disconnect network cable
- Don’t want to make it **worse** though:
  - Shutting down systems unnecessarily
  - Stopping communication

#5 Eradication and recovery

- **Remove** the *threat actor*
  - anti-malware solution (malware).
  - reinstall the operating system (malware).
  - Remove accounts/change passwords (compromised account).
- **Recover** data from *backups* (similar to a disaster plan)
- **Remove** *vulnerabilities*
  - apply patches to operating systems.
  - remove unnecessary user and admin accounts.
- Carry out due diligence
  - audit permissions on accounts.
  - scan for vulnerabilities.

#6 Post-incident

- **Review** what happened (post mortem) with stakeholders.
  - what happened
  - what worked
  - what didn't work
  - what can be improved

- Stakeholders are **not just technical staff** because need to understand the wider impact on business.

- Update incident response process using what was learnt.

INCIDENT RESPONSE TEAM

Establishing a CSIRT

Computer Security Incident Response Team (CSIRT)

While there are a good deal of titles for incident response teams, the term **Computer Emergency Response Team** *(***CERT***) is often associated with CERT NZ*

For our purposes, we will use the more generic CSIRT.

Who is in a CSIRT?

Established with clear guidelines as to what can and cannot do – might be entirely internal or parts of it contracted out.

- **Core**:
  - **Incident response coordinator** – manages the CSIRT activities
  - **CSIRT senior analyst**(s) – trained in incident response
  - **Security operations analyst** – **SOC** is a security operations centre monitoring IDS etc.
  - **IT security engineer** – deploys tools and fixes
- Additionally, draw upon three other main groups:
  - Technical support personnel
  - Organisational support personnel
  - External resources

Who is in a CSIRT? (cont.)

- **Technical support personnel:**
  - Network and server admins
  - Application support for internal applications
  - Desktop support for anti-virus, desktop maintenance
  - Help desk
- **Organisational support personnel:**
  - Legal for managing impact of things like data breaches
  - Human resources to cover if investigating staff
  - Marketing/communications to manage public perception
  - Facilities for after hours access, meeting spaces, resources
  - Corporate security for **physical security** aspects
- **External resources:**
  - High tech crimes NZ Police
  - NZ CERT
  - InternetNZ
  - NZITF (New Zealand Internet Task Force)

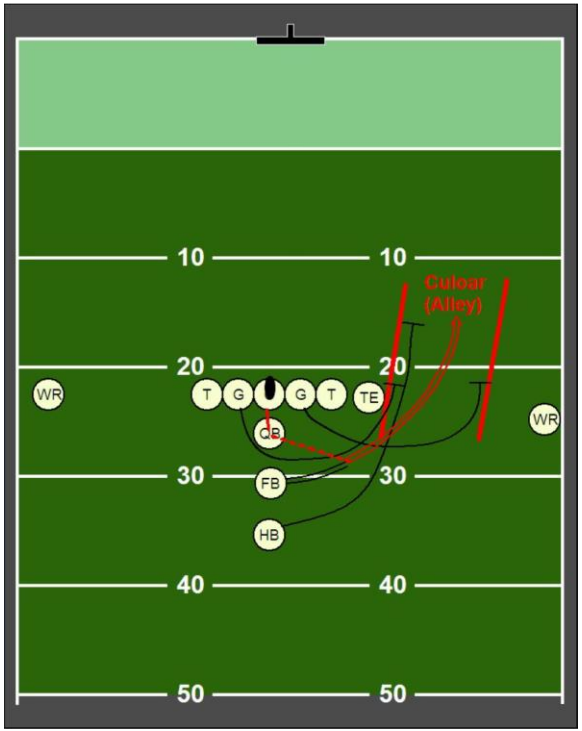
PLANS AND PROCESSES

Incident response plan

- Outlines high-level structure of **response capability**.
- Incident response charter – the "**mission statement**"
- Detailed list of services offered – so can easily say **"we do this, we don't do this"**
- Roles and responsibilities of each CSIRT team member – so can **avoid turf wars under pressure**
- Contact list – need to be able to **respond 24/7**
- Internal communications – **how do you communicate** if the hacker is in your system?
- Incident classification – define what incidents pose the worst threat to an organisation and **classify them**

Playbooks for incident handling

- Plays that a player or team may run in games of American football or basketball.
- **Incident response playbook** is a set of **instructions** and **actions** to be performed at <u>every step</u> in the incident response process.
- Aim is to simplify responses when under pressure.



Playbooks for incident handling (cont.)

EXAMPLE SOCIAL ENGINEERING

- **Preparation**: In this section, the organization will highlight the preparation that is undertaken. In the case of phishing, this can include employee awareness to identify potential phishing email or the use of an email appliance that scans attachments for malware.
- **Detection**: For phishing attacks, organizations are often alerted by aware employees or through email security controls. Organizations should also plan on receiving alerts via malware prevention or **Host Intrusion Prevention System** (**HIPS**) controls.
- **Analysis**: If an event is detected, analyzing any evidence available will be critical to classifying and appropriately responding to an incident. In this case, analysis may include examining the compromised host's memory, examining event logs for suspicious entries, and reviewing any network traffic going to and from the host.
- **Containment**: If a host has been identified as compromised, it should be isolated from the network.
- **Eradication**: In the event that malware has been identified, it should be removed. If not, the playbook should have an alternative such as reimaging with a known good image.
- **Recovery**: The recovery stage includes scanning the host for potential vulnerabilities and monitoring the system for any anomalous traffic.
- **Post-incident activity**: The playbook should also give guidance on what actions should take place after an incident. Many of these actions will be the same across the catalog of playbooks, but are important to include, ensuring that they are completed in full.

How and when to escalate

Sending staff to investigate many false positives will **burn the team out leading to poor performance**.

- Escalation procedure
  - who is responsible for flagging events as incidents
  - who to contact to minimise chance of burnout
- Example:
  - Help desk might be starting point.
  - Cannot apply simple procedure to fix so escalate.
  - Contact CSIRT member on call.
  - May escalates to CSIRT coordinator to make call who to involve.

Clearly defined responsibilities and authority.

Don't want paralysis because don't know who to contact.

MAINTAINING CAPABILITY

Maintaining capability

- Run a **tabletop exercise** once plan and playbooks developed.
- Simulated real-world situation.
- Led by facilitator.
- Done in classroom setting.
- Allows you to test the plan and playbooks.
- Identify gaps in the plans or playbooks.
- **“No fault” answers** – the purpose is to see if things break when it doesn’t matter, not to point blame.

Maintaining capability (cont.)

- **Socialise** the CSIRT
  - We are not the secret police.
  - Not focussing on employee misconduct.
  - Make mission statement available to everyone.
  - Share reports on incidents handled.
- Regular **training**
  - Courses
  - Tabletop exercises
- **Annual review**
  - Update the incident plan (no use if it isn't up to date)

Summary

- This is the idea of incident response planning.
- It isn't the most exciting aspect of computer security, **but it is hugely important**.
- Explored the basics:
  - Forming a team
  - What goes into the plan.
  - Playbooks.
  - Maintaining capability.