Internet Incident Response Table Top Exercise

ITU/APNIC/MICT IPv6 Security Workshop

8th – 12th May 2017

Bangkok

Introduction

The Plan

- Session 1:
  - 5 minutes - Introduction
  - 15 Minutes - Talk through Discussion 1 as a group
  - 10 Minutes - Groups develop presentation to address topics in Discussion 1
  - 15 Minutes - Talk through Discussion 2 as a group
  - 10 minutes - Groups develop presentation to address topics in Discussion 1
- Session 2:
  - 15 Minutes - Talk through Discussion 3 as a group
  - 10 Minutes - Groups develop presentation to address topics in Discussion 1
  - 15 Minutes - Talk through Discussion 4 as a group
  - 10 minutes - Groups develop presentation to address topics in Discussion 1
  - 5 Minutes – Wrapup
- Session 3: PRESENTATIONS

WHAT DO YOU NEED TO DO?

- Discuss issues within your team
- Use all the techniques you have learnt this week
- Produce a presentation showing your teams approach to the problems discussed
- Present this to the class

Terminology

- "hacker"
  - exploits software vulnerabilities to take control of computer systems, force the system to execute malicious code, or crash the system to deny its usage to a legitimate user.
- "Online Criminals"
  - can be one off individuals, but more often tend to be a group of hackers affiliated with organized crime who exploit software vulnerabilities for a monetary gain.

Terminology

- ‘zero day’ exploit or attack
  - takes advantage of a security vulnerability previously unknown to the general public. An attacker using a ‘zero day’ exploit is a severe threat as software developers and security companies are generally unaware of the vulnerability and have not issued patches or preventative measures to address the problem.

Exercise ground rules

- There are no right or wrong answers or ideas
- Maintain a no-fault, stress-free environment
- Use the scenario to provide context and spark creative ideas
- Do not limit discussion to official positions or policies
- Tap community resources and assets to aid/enhance brainstorming

How to work in your team

- Your team are employees of “Superpower Grid Inc”
- Some of you might be engineers, some might be managers
- You do not need to have the same role that you do in real life.
- You can change roles
- You shouldn’t be restricted with what you would do in your real job.

Module 1

InfoSec Criminal Threat Alert

APNIC
@apnic

Following

#Breaking: Hacker group @OBSCURA claim to have seized control of unidentified national electricity smart meters, threaten power shutdown

RETWEETS 1,567 FAVORITES 1,118

3:07 PM – 8 May 2017

Flag media

Discussion 1

Preventative Measures

Suggested questions to address

- How do variables in the threat information that we receive – such as timeframe, credibility, and specificity – impact our decision making and prevention efforts?
- Does this look like a casual hacker or a criminal organisation? Does this difference influence your decisions to take preventative actions?
- If the hacker were a part of a criminal organization, would that influence your actions? How you respond?
- What tools do we use to support infosec prevention? Are they sufficient?
- How do we share infosec threat information internally? What about externally, with groups like law enforcement entities?
- What are our expectations of the government? Do we coordinate with them? Should we?

Create a team presentation

- Take some time now to prepare a presentation
- This presentation should detail how you team would deal with **some** of the issues in the previous slide
- You do not have to address them all, but remember…

Points mean Prizes

Discussion 2

Planning & Policy

Suggested questions to address

- How well does our organization currently integrate infosec security into the life cycle system (i.e., design, procurement, installation, operation and disposal)?
- Are audits conducted on our infosec security systems? Are the systems compliant to our company's security plan requirements?
- Do we ensure that service providers (i.e., vendors) that have access to our systems are following appropriate personnel security procedures and/or practices?
- Discuss the decision making involved when determining internet access required for business versus restrictions that support infosec security.
- Does our organization have an asset inventory of all critical IT systems and a cohesive set of network/system architecture diagrams or other documentation (e.g. nodes, interfaces, and information flows)?
- Who are our infosec preparedness stakeholders (public, private, non-profit, other)? Why are they important?
- Do we have established infosec security risk-based performance standards?
- Where do we receive our infosec planning technical assistance?
- What are our policies and procedures upon being notified of a compromise/breach of security?
- Should legal representation be sought and at what point? What is the threshold?
- Should third party investigation help be sought and at what point? What is the threshold?

Extend your team presentation

- Take some time now extend your presentation
- Explain how your team would deal with **some** of the issues in the previous slides
- You do not have to address them all, but remember…

Points mean Prizes

Module 2

A Company Under Attack

APNIC

@apnic

Following

#Breaking, exclusive: Hacker group @OBSCURA hint that Superpower Grid Inc may be the victim of their #IOT Smart Meter hack

RETWEETS	FAVORITES
306	42

4:23 PM – 11 May 2017

Discussion 3

Detection & Response

Suggested questions to address

- What tools or assets do we have/do you have to assist us in detecting unauthorized activity?
- What type of detection hardware and/or software do we use? How successful or unsuccessful has this software/hardware been in detecting and/or preventing this activity?
- How would we/how would you conduct an assessment of this situation?
- What resources do we have or could we request for network forensics?
- Where do we receive our infosec response technical assistance?
- Do we have plans, procedures or policies in place to access this assistance?
- What are the needed resources and where would we get them?
- Do our current mutual aid agreements address infosec specific resources and staff?
- Do we have a InfoSec Incident Response Team? What is their composition/ skill set?
- Does our a InfoSec Incident Response Team have a systems administrator, business process mindset, and understanding of the IT architecture?

Extend your team presentation

- Take some time now extend your presentation
- Explain how your team would deal with **some** of the issues in the previous slides
- You do not have to address them all, but remember…

Points mean Prizes

Discussion 4

Notifications & Stakeholder Communications

Suggested questions to address

- What is our planned decision-making process for protective actions in a infosec incident? What options are available? Planned for? How are they activated?
- What about planned notifications? How do we do this internal to our organization? External to our organization?
- At what point would we – or should we – contact law enforcement?
- At what point would information be shared with vendors?
- Would knowledgeable experts be involved? Would your national Computer Emergency Readiness Team (CERT) be notified or involved?
- Would this situation trigger contact with regulators? Why or why not?
- How would we inform our other stakeholders, including customers?
- What are the business implications of the scenario? How would we determine them?
- What are the expectations or plans for information sharing among stakeholders and response partners?
- Are IT and business continuity functions coordinated with physical security? Would all three then be collaborating with public relations, human resources, and legal departments?
- What internal and external messages would need to be developed? How are they being distributed? Who leads the public information process?

Extend your team presentation

- Take some time now extend your presentation
- Explain how your team would deal with **some** of the issues in the previous slides
- You do not have to address them all, but remember…

Points mean Prizes

Acknowledgements

- National Level Exercise 2012: Cyber Capabilities Tabletop Exercise
  - https://www.fema.gov/media-library/assets/documents/26845
- Sean Mason - Table Top Exercises (TTX) for Incident Response
  - http://seanmason.com/2015/04/20/table-top-exercises-ttx/

Internet Incident Response Table Top Exercise

ITU/APNIC/MICT IPv6 Security Workshop

8th – 12th May 2017

Bangkok