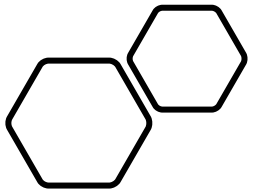

ROCHESTER SECURITY SUMMIT

Incident Response Tabletop Exercise

HARBORSHIELD CYBERSECURITY

Agenda

- Introductions
- Scenarios
  - Scenario #1
  - Scenario #2
  - Scenario #3
  - Scenario #4
  - Scenario #5 [if necessary]
- Wrap it up – Lessons Learned

HARBORSHIELD CYBERSECURITY

The Quick Fix Scenario

SCENARIO:

Antony, our network VP/administrator is overworked. His bags are packed, and he is ready for a trip around the world with his wife when he is tasked with deploying a critical patch.

In order to make his flight, Antony quickly builds an installation file for the patch and deploys it before leaving for his trip. Anu, the on-call service desk technician, begins receiving calls that nobody can log in. It turns out that no testing was done for the recently installed critical patch.

Employees are not able to access company data and a note has been received asking for a 3-million-dollar ransom. If payment is not received by EOD today the information to press outlets starting at 6pm.

- **What is your response?**

Discussion Questions

What is Anu’s response in this scenario?

Who should we get involved at this point?

When should legal be involved?

Who else should be on the CERT team?

Does your organization have a formal change control policy?

Are your employees trained on proper change control?

Does your organization have disciplinary procedures in place for when an employee fails to follow established policies?

Does your organization have the ability to “roll back” patches in the event of unanticipated negative impacts?

Synopsis

Processes tested: Patch Management

Threat actor: Insider

Asset impacted: Internal Network

Applicable CIS Controls™: CIS Control 2: Inventory and Control of Software Assets, CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers, CIS Control 6: Maintenance, Monitoring, and Analysis of Audit Logs

Scenario #1 Recap

What went right?

What went wrong?

A Malware Infection Scenario

Exercise 2

SCENARIO:

Thomas used the Law School's digital camera for Marketing purposes (picture for the website). In the course of doing so, he took a perfect photograph that he then loaded onto her personal computer by inserting the SD card. The SD card was infected with malware while connected to the employee's personal computer. When re-inserted into a company machine, it infected the organization's system with the same malware.

Your employees are not able to access company data.

What is your response?

Discussion Questions

Who within your organization would you need to notify?

How would your organization identify and respond to malware infecting our system through this vector?

What is the process for identifying the infection vector?

What other devices could present similar threats?

What should we do as management?

Should legal be involved?

How can we prevent this from occurring again?

Do you have training and policies in place to prevent this?

Synopsis

Processes tested: Detection ability/User awareness

Threat actor: Accidental insider

Asset impacted: Network integrity

Applicable CIS Controls: CIS Control 8: Malware Defenses, CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services, CIS Control 12: Boundary Defense

Scenario #2 Recap

What went right?

What went wrong?

HARBORSHIELD CYBERSECURITY

The Unplanned Attack Scenario

Exercise 3

SCENARIO:

A hacktivist group threatens to target your organization following an incident involving an allegation of the misuse of consumer data. You do not know the nature of the attack they are planning.

How can we improve our posture to best protect your organization?

What is your response?

Discussion Questions

Should you contact legal or the authorities?

What are the potential threat vectors?

Have you considered which attack vectors have been most common over the past several months?

Are there other methods you can use to prioritize threats?

Have you checked your patch management status?

Can you increase monitoring of your IDS and IPS?

If you don't have the resources to do so, is there another organization that could be called upon to assist?

What organizations or companies could assist you with analyzing any malware that is identified?

How do you alert our help desk?

Do you have a way of notifying the entire organization of the current threat?

Does your Incident Response Plan account for these types of situations?

synopsis

Processes tested: Preparation

Threat actor: Hacktivist

Asset impacted: Unknown

Applicable CIS Controls: CIS Control 8: Malware Defenses, CIS Control 12: Boundary Defense, CIS Control 17: Implement a Security Awareness and Training Program, CIS Control 19: Incident Response and Management

Scenario #3 Recap

What went right?

What went wrong?

The Cloud Compromise Scenario

Exercise 4

SCENARIO:

Your engineering departments frequently uses outside cloud storage to store large amounts of data. We have recently learned that the cloud storage provider that is being used has been publicly compromised and large amounts of data have been exposed. All user passwords and data stored in the cloud provider's infrastructure may have been compromised.

What is your response?

Group Discussion

Does our organization have current polices that consider 3rd party cloud storage?

Should our organization still be held accountable for the data breach?

What actions and procedures would be different if this was a data breach on our own local area network?

What should management do?

What, if anything, do you tell your clients?

* How/when would you notify them?

Synopsis

Processes tested: Incident response

Threat actor: External threat

Asset impacted: Cloud

Applicable CIS Controls: CIS Control 10: Data Recovery Capabilities, CIS Control 13: Data Protection, CIS Control 19: Incident Response and Management

Scenario #4 Recap

What went right?

What went wrong?

HARBORSHIELD CYBERSECURITY

Financial Break-in Scenario

Exercise 5

SCENARIO:

A routine financial audit reveals that several people receiving paychecks are not, and have never been, on payroll. A system review indicates they were added to the payroll approximately one month prior, at the same time, via a computer in the financial department

What do we do?

INJECT: We confirm the computer in the payroll department was used to make the additions.

Approximately two weeks prior to the addition of the new personnel, there was a physical break-in to the finance department in which several laptops without sensitive data were taken.

OPTIONAL INJECT: Further review indicates that all employees are paying a new "fee" of $20 each paycheck and that money is being siphoned to an off-shore bank account. Having this additional information, how do you proceed?

Group Discussion

What actions could we take after the initial break in?

- Do we have the capability to audit our physical security system?
- Who would/should be notified?
- Would we able to assess the damages associated from the break in?
- Would we be able to find out what credentials may have been stored on the laptop?
- How would we notify your employees of the incident?
- How do we contain the incident?
    - Optional Inject question: How do you compensate the employees?

Synopsis

- **Processes tested:** Incident Response
- **Threat actor:** External Threat
- **Asset impacted**: HR/Financial data
- **Applicable CIS Controls:** CIS Control 4: Controlled Use of Administrative Privileges, CIS

Scenario #5 Recap

What went right?

What went wrong?

HARBORSHIELD CYBERSECURITY