Confidence in the Connected World

CIS Center for Internet Security®

Tabletop Exercises

Six Scenarios to Help Prepare Your Cybersecurity Team

October 18, 2018

Contents

Introduction

At CIS® (Center for Internet Security, Inc.®), we believe everyone deserves a secure online experience. We recognize that security is a shared responsibility between users, administrators, and technical professionals. We developed this white paper about tabletop exercises to help cybersecurity teams develop tactical strategies for securing their systems.

This guide is organized so that the exercises and discussion questions become more challenging and difficult as the white paper moves forward. However, you can easily jump to the section or exercise that most interests you. For more information about cybersecurity best practices, visit our website: https://www.cisecurity.org/.

Getting started

How to use these tabletop exercises

Tabletop exercises are meant to help organizations consider different risk scenarios and prepare for potential cyber threats. All of the exercises featured in this white paper can be completed in as little as 15 minutes, making them a convenient tool for putting your team in the cybersecurity mindset. In addition, each scenario will list the processes that are tested, threat actors that are identified, and the assets that are impacted.

Tips and tricks

- Designate a single individual to facilitate the exercise.
- Break the scenario into meaningful learning points.
- Read the scenario aloud to the group and ensure their understanding.
- Facilitate a conversation about how your organization would handle the scenario, focusing on key learning points as you discuss.
- Include applicable members of other business units.
- Be sure to follow up on any gaps identified during the exercise.

Exercise 1

The Quick Fix

SCENARIO: Joe, your network administrator, is overworked and underpaid. His bags are packed and ready for a family vacation to Disney World when he is tasked with deploying a critical patch. In order to make his flight, Joe quickly builds an installation file for the patch and deploys it before leaving for his trip. Next, Sue, 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.

What is your response?

Discussion questions

- What is Sue's response in this scenario?
  - Does your on-call technician have the expertise to handle this incident? If not, are there defined escalation processes?
- 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?

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

Exercise 2

A Malware Infection

SCENARIO: An employee within your organization used the company's digital camera for business purposes. In the course of doing so, they took a scenic photograph that they then loaded onto their 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.

What is your response?

Discussion questions

- Who within the organization would you need to notify?
- How would your organization identify and respond to malware infecting your system through this vector?
  - What is the process for identifying the infection vector?
- What other devices could present similar threats?
- What should management do?
- How can you prevent this from occurring again?
  - Does your organization have training and policies in place to prevent this?
  - Do policies apply to all storage devices?

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

Exercise 3

The Unplanned Attack

SCENARIO: A hacktivist group threatens to target your organization following an incident involving an allegation of use of excessive force by law enforcement. You do not know the nature of the attack they are planning. How can you improve your posture to best protect your organization?

What is your response?

Discussion questions

- What are the potential threat vectors?
- Have you considered which attack vectors have been most common over the past month?
  - 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 your help desk?
- Do you have a way of notifying the entire organization of the current threat (bulletin board, etc.)?
- Does your Incident Response Plan account for these types of situations?

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

Exercise 4

The Cloud Compromise

SCENARIO: One of your organization's internal departments frequently uses outside cloud storage to store large amounts of data, some of which may be considered sensitive. You 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?

Discussion questions

- Does your organization have current polices that consider 3rd party cloud storage?
- Should your organization still be held accountable for the data breach?
- What actions and procedures would be different if this was a data breach on your own local area network?
- What should management do?
- What, if anything, do you tell your constituents?
    - How/when would you notify them?

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

Exercise 5

Financial Break-in

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 is your response?

INJECT: You 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?

Discussion questions

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

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 Control 16: Account Monitoring and Control, CIS Control 19: Incident Response and Management

Exercise 6

The Flood Zone

SCENARIO: Your organization is located within a flood zone. Winter weather combined with warming temperatures has caused flooding throughout the area. Local authorities have declared a state of emergency. In the midst of managing the flooding, a ransomware attack occurs on your facility, making computer systems inoperable.

What is your response?

Discussion questions

- Do you have a COOP (Continuity of Operations Plan) or DRP (Disaster Recovery Plan)?
    - If so, do you carry out an annual simulation to ensure the COOP or DRP is sufficient and running smoothly?
- Do you have an Incident Response Plan (IRP) that specifically details ransomware steps?
    - What steps will you take if restoring from backup is not an option?
    - Does your IRP only take into account the financial implications of a cybersecurity incident, or does it consider the severity of the situation as well?
    - Do you have a plan in place for how to acquire bitcoin?
    - Have you considered that a targeted ransomware attack may require more bitcoin than is easily accessible on the market?
- Do you have a backup for completing Emergency Operations Center (EOC) processes without a computer system?
    - Can you route emergency communications/processes through a neighboring entity?
- Who do you need to notify, and how will you do so?
    - Consider that increased phone traffic may be congesting the lines.

Processes tested: Emergency response

Threat actor: External threat

Asset impacted: Emergency Operations Center Processes

Applicable CIS Controls: CIS Control 7: Email and Web Browser Protections, CIS Control 19: Incident Response and Management

Additional Information

Interested in cybersecurity best practices? CIS is here to help! Check out the resources below to take the next step towards security and compliance:

Resources - Free

CIS Benchmarks: https://www.cisecurity.org/cis-benchmarks/

CIS Controls: https://www.cisecurity.org/controls/

CIS-CAT Lite: https://learn.cisecurity.org/cis-cat-landing-page

Sample Remediation Kit: https://learn.cisecurity.org/remediation-kits

Webinar: CIS-CAT Pro Demo: https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-webinar/

Resources - Free for U.S. State, Local, Tribal, and Territorial (SLTT) Government Entities

MS-ISAC Membership (for U.S. SLTTs): https://learn.cisecurity.org/ms-isac-registration
EI-ISAC Membership (for U.S. SLTTs supporting elections): https://www.cisecurity.org/ei-isac/

Resources - Paid

CIS SecureSuite Membership: https://www.cisecurity.org/cis-securesuite/

CIS Hardened Images: https://www.cisecurity.org/services/hardened-virtual-images/

About CIS

CIS® (Center for Internet Security, Inc.) is a forward-thinking, non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats. The CIS Controls™ and CIS Benchmarks™ are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks. These proven guidelines are continuously refined and verified by a volunteer, global community of experienced IT professionals. Our CIS Hardened Images are virtual machine emulations preconfigured to provide secure, on-demand, and scalable computing environments in the cloud. CIS is home to both the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the go-to resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center™ (EI-ISAC™), which supports the cybersecurity needs of U.S. State, Local and Territorial elections offices.

Contact Information

CIS
31 Tech Valley Drive
East Greenbush, NY 12061

518.266.3460

learn@cisecurity.org