Cybersecurity Incident Response Plan

Aaron Gehring

Fox Valley Technical College

Incident Response

Wendy Diem

December 13, 2021

Cybersecurity Incident Response Plan

Statement of Purpose

The Incident Response Plan is designed for FOXES Enterprise, LLC. with the purpose of outlining the steps to maintain a secure environment in the event of a security incident. The Incident Response Plan adopts the National Institute of Standards and Technology (NIST) Incident Response framework to ensure effective analysis, eradication, and recovery after an incident. The plan also serves as documentation of the contact details and roles of individuals and organizations important to FOXES' security.

Contact List

The contact list is present in Table 1.

On-Call Schedule

An on-call worker is an incident responsder that is available to work within 15 minutes of being called in, at any time. The organization has a rotating schedule of four on-call incident responders, with each on call for a week at a time. If on-call worker is unable to be on-call, on-call duties will be shared by previous on-call worker and the next-down worker of the on-call worker. Contact details are in Table 2.

Escalation Procedures

To efficiently allocate business resources, incidents should be handled by staff appropriate to an incident's location on the risk matrix. Low risk incidents should be handled by helpdesk. Medium risk incidents should be handled by IT incident staff. High risk incidents should be handled by the Cybersecurity Incident Response Team (CSIRT). Critical risk incidents should involve the organization's highest level incident response staff. Incidents may be escalated past their starting level if needed.

War Room

The CSIRT will have unobstructed access to an assigned large work room, designated as the war room. The war room will have at least 10 workstations available, with capability to support 20 additional laptops. The workstations will be organized with three or four to a table, oriented to encourage collaboration. There will also be 10 laptops marked for use by the CSIRT if needed. Additional tables in a similar configuration will be present which can either be used as general purpose tables or as dock stations for the laptops. These additional tables should be on locking casters so that tables can be moved or put together as needed. The war room will have at least one projector, and have at least two large whiteboards, one on wheels and one mounted on a wall. In addition to the projector, the war room will also have two TV screens the any HDMI device can display on.

Communication Tracking

A communication timeline shall be kept. The timeline will have a row for each event, and six columns. ex

1. Datetime: 2021-09-28T20:13:51Z
2. Event: A description of the event
3. Investigator: The relevant person or party
4. Receiving: The person entering this record
5. Category: An organizational note
6. Notes: Additional notes

Toolkit

Hardware

- Digital Forensics Workstations
- Investigative/Computational Laptops
- Note-taking and research/Lightweight laptops

- Spare server(s)
- Removable media for:
  - Backups
  - Removable and portable storage
  - Live operating systems
  - Recovery tools
- Portable printer

Additional Tools

- Pen and notebook or journal
- Printer paper
- Chain of custody forms
- Evidence collection bags
- Digital Cameras
- Voice recorders

Important Documents

Some additional documents that need to be built or collected for the CSIRT. Port lists, baselines and hash tables help confirm what has or has not been modified. Network diagrams and documentation help the CSIRT navigate the organization's systems.

Indicators of Compromise Monitoring

The organization will have a team of security staff that can identify precursors and indicators of compromise (IOC), with varying areas of strength. When an incident is identified, the incident response team will begin with categorizing the incident and the steps above.

IOC Monitoring

The organization will use security information and event management (SIEM) software such as Graylog to monitor the organization's systems. The SIEM will be set up to ingest from all sources, and to perform automatic analysis. The organization will also utilize antivirus software to protect users' workstations and antispam software to protect the email system. Antivirus and antispam lists are to be updated frequently. Critical files on servers will be monitored for unauthorized modification via automatic SHA256 checksum generation. Logs from devices in the organization (Windows Event log, Linux's syslog, and other device-specific logs) will be directed to the SIEM ingest and to a log archive.

Incident Analysis

Most indicators do not indicate an incident, so analysis is necessary to pick out the important indicators from the pile. The organization will have a team of security analysts that can perform such a task, while maintaining effective logs and archives of activities. The team should take benchmarks and make a profile of the organization's systems to understand baseline operation. Additionally, the team should understand the system and its normal behaviors, and its typical fluctuations. Logs should be retained for three months, and indicators should be retained for at least 1.5 years. Archives may be kept longer, given sufficient reason. The organization's systems must all have their system time set to UTC+6, and if possible, synchronize with a trusted or local NTP server (time.nist.gov as a backup). In the case of an ongoing incident, the team should use packet sniffers, like Wireshark, to gather additional data for analysis.

Incident Documentation

All activities involving the incident response team should be recordable, and indeed, recorded. This includes both actions taken by the incident response team, as well as

activity observed by the team. An issue tracking system will be used to organize incidents, and the data that goes with them. All activity logs should, at a very minimum, contain a datetime, personnel information, and a description of the activity. However, every log should aim to document more information.

Incident Prioritization Matrix

When the incident response team has more incidents to respond to than available labor, certain incidents must be prioritized. This will be achieved through a three-dimensional matrix, like a risk matrix. The three factors are:

- Functional Impact
- Information Impact
- Recoverability

As an example, an incident where an attacker destroys hardware, steals trade secrets, and deletes swaths of data would be of utmost priority, with critical marks in each of the three factors. An incident where an attacker performs a distributed denial-of-service (DDoS) attack against our system for an hour may gain some marks in functional impact, however, would ultimately be low priority, with zero marks in information impact or recoverability.

Choosing a Containment Strategy

All containment strategies should be taken only after the nature of the incident is known. This way, containment strategies can be selected strategically, avoiding alerting the attacker to our efforts against them.

To choose the appropriate containment strategies, several aspects must be identified about the incident:

- What known threats/vulnerabilities/incidents does this incident match? If none, is this a zero-day or a variation of an existing attack?

- Will this incident cause further damage if firewall-ed?
- What systems and devices have been affected?
- What user accounts have been affected?
- Was any data stolen?
- How? What systems are involved with that?
- Has the incident affected any containment strategies already?
- What resources does the organization have available to contain the incident
- Is sandboxing feasible?

Evidence Gathering and Handling

Documentation of evidence gathering and handling must be created and maintained. This documentation must be accurate and thorough enough to hold up in a court. Read the *Federal Rules of Evidence* for a guide on evidence best practices, available at https://www.law.cornell.edu/rules/fre.

A chain of custody form must be generated for every item of evidence. This chain of custody form will track who has had access to each item of evidence and when, among other things.

- Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of a computer)
- Name, title, and phone number of each individual that collected or handled the evidence during the investigation
- Time and date (including time zone) of each occurrence of evidence handling
- Locations where the evidence was stored.

  (Cichonski et al., 2012)
- How the evidence was collected (Bagged/tagged, pulled from a desktop, etc.)
- When it was collected (e.g. Date, Time)
- How you transported it (e.g. in sealed static-free bag, placed in a secure storage

container)

- How it was tracked (as an example, I use a form and also track the forms used with an Excel spreadsheet. Provide a sequence number, too, as this serves as a key field for the evidence tracking reports that you may generate)
- How it was stored (for example, in secure storage at your facility)
- Who has access to the evidence (e.g. this is the check-in/check-out process that you will need to develop. It is essential that we know who had access to each acquired piece of evidence. You will be asked to demonstrate this, if this is a court case.)

(McFarland, 2018)

Identifying the Attacking Hosts

Identifying the attackers is important, especially for denying future attacks, but optional. Most malicious incidents will have some communication with an external host, be that a C2 server, exfil drop or botnet. The most common addresses to look for are going to be IP addresses and email addresses. Keep in mind that these can be spoofed, and even a packet going to an external address may not be an accurate final destination if the attacker is using a proxy or botnet.

Eradication and Recovery

At this point, all information needed to act should be identified.

- The users that have been compromised have been given new credentials. Also given training, if necessary.
- The systems that have been affected have either been cleaned of attack remnants or restored to a previous backup.
- Attack surfaces have been closed or otherwise secured.

Now, the organization can move forward with recovery. Systems have been affected by the incident can be restored to full function. Again, backups can be used to restore the

state of things before the incident occurred. Take a profile of the system and compare to the most recent baseline from before the incident to ensure that the organization's functions are recovered fully.

Post Incident Analysis Report

All incidents with a greater than low risk must have a Post Incident Analysis Report made before closing the incident. The template for the Post Incident Analysis Report is in Table 3.

Lessons Learned

The last activity to take place before closing the incident will be a lessons learned meeting and review. This meeting will involve the full incident response team, involved management and stakeholders. The lessons learned meeting should answer questions from these prompts, as a starting point:

- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

(U.S. Department of Housing and Urban Development, 2020)

The lessons learned meeting should produce a “Lessons Learned Report” that answer these questions and can be used to improve FOXES future security.

Final Items

In additional to the process of closing tickets and sending final notices, the process of closing out an incident includes collating all reports and documentation related to the incident. The reports and documentation are archived and kept for three years. The reports and documentation may be kept for longer if needed, such as in the case of a criminal case.

References

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August). *Computer security incident handling guide : Recommendations of the national institute of standards and technology* (NIST SP 800-61r2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Federal rules of evidence [LII / legal information institute]. (2020, December 1). Retrieved November 28, 2021, from https://www.law.cornell.edu/rules/fre

Incident Response Consortium. (n.d.). *Playbook - data theft* [Incident response consortium]. Retrieved November 28, 2021, from https://www.incidentresponse.com/playbooks/data-theft

Jason Dion. (n.d.). *Preparation*. Retrieved September 28, 2021, from https://www.linkedin.com/learning/incident-response-planning/preparation

Johansen, G. (2017). *Digital forensics and incident response*. Packt Publishing. Retrieved September 28, 2021, from https://login.applibproxy.fvtc.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1562684&site=eds-live

McFarland, R. (2018, January 30). *Digital forensics – the essential chain of custody* [The cyber security place]. Retrieved November 28, 2021, from https://thecybersecurityplace.com/digital-forensics-the-essential-chain-of-custody/

U.S. Department of Housing and Urban Development. (2020, July 15). Cybersecurity incident response plan. Retrieved September 28, 2021, from https://www.hud.gov/sites/dfiles/OCHCO/documents/CybersecurityIncidentResponsePlan2.0.pdf

Table 1

Contact List

Name	Role	Org	Email	Phone 1	Phone 2
Scott Borley	CIO	FOXES	x@x.x	(xxx) xxx-xxxx	(xxx) xxx-xxxx
Victoria Lindqvist	Executive Assistant	FOXES	x@x.x	(xxx) xxx-xxxx	(xxx) xxx-xxxx
Steve Ebben	VP Network/Computer Support	FOXES	x@x.x	(xxx) xxx-xxxx	(xxx) xxx-xxxx
Joe Wetzel	VP Software Development/WEB	FOXES	x@x.x	(xxx) xxx-xxxx	(xxx) xxx-xxxx
X	Helpdesk	X	x@x.x	(xxx) xxx-xxxx	(xxx) xxx-xxxx
X	Helpdesk	X	x@x.x	(xxx) xxx-xxxx	(xxx) xxx-xxxx
X	Legal	X	x@x.x	(xxx) xxx-xxxx	(xxx) xxx-xxxx
X	Intrusion Detection monitoring	X	x@x.x	(xxx) xxx-xxxx	(xxx) xxx-xxxx
X	SysAdmin	X	x@x.x	(xxx) xxx-xxxx	(xxx) xxx-xxxx
X	Firewall Administrator	X	x@x.x	(xxx) xxx-xxxx	(xxx) xxx-xxxx
X	Business Partner?	X	x@x.x	(xxx) xxx-xxxx	(xxx) xxx-xxxx
X	Hardware Vendor	X	x@x.x	(xxx) xxx-xxxx	(xxx) xxx-xxxx
X	Software Vendor	X	x@x.x	(xxx) xxx-xxxx	(xxx) xxx-xxxx
X	IT Security Lead	X	x@x.x	(xxx) xxx-xxxx	(xxx) xxx-xxxx
X	CISO	X	x@x.x	(xxx) xxx-xxxx	(xxx) xxx-xxxx
X	Third Party	X	x@x.x	(xxx) xxx-xxxx	(xxx) xxx-xxxx

Table 2

On-Call Contact List

Name	Week	Email	Phone 1	Phone 2
X	First & Last Week	x@x.x	(xxx) xxx-xxxx	(xxx) xxx-xxxx
X	Second Week	x@x.x	(xxx) xxx-xxxx	(xxx) xxx-xxxx
X	Third Week	x@x.x	(xxx) xxx-xxxx	(xxx) xxx-xxxx
X	Fourth Week	x@x.x	(xxx) xxx-xxxx	(xxx) xxx-xxxx

Table 3

Post Incident Analysis Report Template

Category	**Required Information**
Incident Info	Unique ID, Affected Department/System, Date & Time of Incident + Ticket
Severity	Records of Impact & Severity Assessment
Cause	Attack Vector, Root Cause, Specific Action
Threat Information	Threat Attributes, Threat Name (if applicable), Related Incidents, Notes
Recovery Steps	Containment, Eradication, Recovery