Assignment 1:  
Part 2: Incident Response Plan

*Kyle, Jacob, Riley*

*Pod #5*

*ISEC2700*

*09/11/2024*

Table of Contents

[**Before Incident:** 3](#_Toc177462680)

[Preparation: 3](#_Toc177462681)

[Preparation (cont.): 4](#_Toc177462682)

[Identification: 5](#_Toc177462683)

[**During Incident:** 6](#_Toc177462684)

[Containment: 6](#_Toc177462685)

[Eradication: 6](#_Toc177462686)

[Recovery: 6](#_Toc177462687)

[**After Incident:** 7](#_Toc177462688)

[Lessons Learned: 7](#_Toc177462689)

[Update Plan: 7](#_Toc177462690)

[Bibliography 7](#_Toc177462691)

# **Before Incident:**

## Preparation:

Security policies will be put in place to prevent an attack before one happens. Such as implementing Multi-Factor Authentication for all devices on the work network. It can be seen as inconvenient; however it is much safer than not using it. Using a software to track keys presses to keep track of what employee’s/staff are using the network for, whether it be browsing or work related. Make sure this policy is explained in detail to all employees, as well as have these practices listed on the company website along with the in the company rules/handbook that every employee will be required to read through with information on security practices. In the process of creating these security policies, things that may not have been up to standards could come to your attention. These can be altered to allow for more secure practices going forward.​ (Kost, 2024)

Implement training for all employees on how to avoid allowing attackers into the network. Not visiting websites that don’t have a trusted connection, not downloading things from random websites onto company devices. Make it clear that all network activity is being tracked and logged. If anything sets off a flag such as an inappropriate website or random content being downloaded or allowing outside access into the company network to outside users and is traced to an employee’s computer, it can result in heavy consequences. Examples of punishment include immediate discontinuation of employment, or heavily restricted access and permissions, including being monitored heavily when using technology on the network.

Determine ways of communicating with any shareholders or staff, as well as appropriate law enforcement should it be required. Included should be all forms of communication with security personnel on staff with a way to contact them in an emergency should other methods not be sufficient. Ensure these communication methods are encrypted to allow for fast response without worry of being monitored by the attacker(s).

Ensure security practices are being run as well as backups are being created for all critical hardware/software being run in the company. All communications between hardware and software should be encrypted to not allow for easy monitoring of information. As for backups, these are the methods

## Preparation (cont.):

1. Domain Controller – Replication, have a second domain controller which can automatically be designated as the primary domain controller should the initial primary domain controller go down for any reason
2. DHCP Server – Create a backup of the server configuration, which is update every 60 minutes, and store this backup configuration on a network share to the Systems Manager (Myra Dante). This will allow it to be accessed even if the entire server goes down. A backup can also be stored on the server itself to have multiple backups in case something goes wrong.
3. NAS – Replication, have a second NAS with a backup of the main NAS on it, this can be an incremental backup and be done repeatedly once a certain amount of time has passed.
4. File Server – Offsite backup on a separate storage server
5. WSUS Server – Perform a database backup, can be done in the graphical way using SSMS (SQL Server Management Studio), or through the command line.[[1]](#footnote-1)
6. WDS Server – Complete a System Image Backup of the WDS Server hard drive as a backup.
7. Print Server – Backup configuration settings for the print server and share through a network share to the Systems Manager (Myra Dante)
8. Hyper-V Host Servers – Create regular snapshots of configuration files, as well as store a copy of the backup on a NAS device, as a secondary backup.
9. Cisco Switch – create a backup of the config file using a TFTP server which can be used to restore the settings.
10. Cisco Firewall – create a backup of the config file using a TFTP server[[2]](#footnote-2)

## Identification:

During the identification phase it is important to have a basic understanding of who the person was that found/flagged the potential attack. Any employee has a duty to report any potential threats, not just security personnel. Take note of what kind of device and what section of your network the attack/incident if focused on. This can allow for a quicker containment phase. How the attack or incident was discovered will be reported as well.

Computer viruses can range in terms of what they effect and how harmful they are, some common kinds that have been identified are:

1. Boot Sector Virus

* Attacks the master boot record, which contain the instructions for booting the system. These are difficult to get rid of. Typically require reformatting the computer. These are usually spread through things like emails or USB. These have been happening less frequently due to improvement in BIOS structure

Risk: Extremely Dangerous

1. Polymorphic Virus

* Stealthy viruses that can hide from antivirus programs, these viruses will replicate themselves but change their binary code when they do, resulting in the antivirus not being able to identify the virus itself.

Risk: Hard to Detect

1. Multipartite Virus

* A multi-prong virus that can behave differently based on what OS it is on, this virus can infect both the master boot record and executable files, which can cause problems for the system.

Risk: More Dangerous

1. Direct Action Virus

* This is an infector, it attaches itself to certain types of files in the computer, such as executable files. When this file is run, it will spread to similar file types on the system. This type of virus can be identified and removed with regular antivirus

Risk: Significant Risk

1. Overwrite Virus

* This type of virus will delete any content it infects, though it is not overly harmful to the system itself. Deleting the infected content can remove the virus. They are spread through emails making them quite difficult to detect for the average user.

Risk: Moderate[[3]](#footnote-3)

# **During Incident:**

## Containment:

Depending on the nature of the attack, the targeted system should be quarantined and disabled accordingly. For any web-based attacks, such as email-borne malware infections, any mail servers should be shut down and separated from the network. For something network related, such as a DDoS strike, any hardware on the network edge such as a router, DNS servers, etc. should be disabled and removed from the network as well. If individual employee accounts are targeted, be sure to suspend employee access to detect and stop further intrusions. (Dutka)

Be sure to keep a recorded log of all evidence for legal reasons. This includes any identifying information from the attacked points, such as location, serial number, model number, hostname, MAC address and IP addresses.

## Eradication:

For certain attacks, eradication may not be necessary or could be completed during the recovery phase. If possible, incident handlers and/or administrators should work to restore systems to normal functionality through restoring systems from *clean* backups, installing patches, changing passwords and tightening network security. (National Institute of Standards and Technology)

## Recovery:

Eradication and recovery often go hand in hand. A phased approach, starting small and working towards the more intensive methods, is the best practice to ensure data is recoverable. An attack that strikes once will often try to strike the same vulnerability again, so ensuring the overall security of the system is increased should be prioritized. Next, the actual infrastructure should be analyzed and updated, such as new firewalls or increased security.

After security has been patched and during the infrastructure updates, backups and recoveries should be applied to all affected systems. Depending on the severity of the attack or infection, a full clean restore should be applied to the systems alongside any snapshot recoveries for virtual servers and systems.

# **After Incident:**

## Lessons Learned:

After the threat has been identified and eradicated, staff should gather to discuss the things they discovered during the process. Gathering which information would have prevented the attack to begin with and which corrective actions could be used to prevent similar incidents in the future should be the focal points.

Creation of a follow-up report for each incident should be considered as a reference for similar attacks that may occur in the future. This should be as detailed as possible to assist in documentation, including time-stamped information like log data, for expeditious containment later, as well as legality reasons to provide as evidence. This report can also be useful for determining the success of the incident response team and to determine if more funding is required.

## Update Plan:

Using the follow-up report and lessons learned meeting, identify which vulnerabilities the system had and work to ensure the incident does not happen again. This could include upgrading the physical hardware itself to something more modern and secure or simply implementing new security practices within the organization, like two factor authentication for all employees or additional steps to avoid social engineering attempts.

# **Testing:**

In this scenario, a DNS hijacker would have affected and spread over the course of multiple days throughout the network. First, a DNS hijacker will redirect DNS queries to another, malicious DNS server to send users to fake websites designed to steal information or inject more malicious software.

After hearing the report from Bruce, the first step would be to identify the threat. In this instance, trying to access the same resources that Bruce did not have access to compared to other users and systems would be the best place to start. Once it is established that the network itself is compromised and not just Bruce’s workstation, the containment phase will begin.

Using this Incident Response Plan, the first step would be to notify the appropriate team members to make sure the attack was known ASAP. This includes Myra Dante, System Manager and all System Operators. Due to the nature of the attack, a notification should be sent to users as well, as the network may experience delays or outages to quarantine the threat.

During containment, as this attack is aimed at our network, the DNS configuration of the DC should be changed immediately to a secure, reliable DNS server like Google (8.8.8.8, 8.8.4.4). This should keep users online while preventing any further damage. If the DNS settings of the DC cannot be changed or even appear *unchanged*, a switch to the replicated server, not attached to the network previously as per the Preparation plan, should restore network functionality to keep the network online while eradication can begin. This depends on the severity of the infection. Security scans and updates should be run on both DC’s to be sure. The DHCP server portion could also send out malicious DNS settings to clients, so this portion should be restored from backup/snapshot via Myra Dante.

Assuming the network resources Bruce was trying to access were saved locally on our network, there is a good chance the File Server and NAS could be infected as well. Both the File Server and NAS are backed up regularly, so loss of data should be minimal during backup.

If the other servers and systems are functioning correctly, they may not require a full backup, but the DNS settings on each server and piece of hardware should be checked for tampering and restored from backup whenever necessary.

After eradication and recovery, the team should gather for a follow-up report to log the incident for legal and future reference. Careful study into how Bruce acquired this trojan should be done in order to point out the vulnerabilities in our network and update our systems accordingly.

# Bibliography

Admin. (2020, 06 22). *Wonderful Engineering*. Retrieved from https://wonderfulengineering.com/7-most-common-types-of-computer-viruses/

Dutka, M. (n.d.). *Incident Reponse Plan (PowerPoint).*

Kost, E. (2024, 09 09). *How to Create an Incident Reponse Plan (Detail Guide)*. Retrieved from UpGuard: https://www.upguard.com/blog/creating-a-cyber-security-incident-response-plan

Marshall, A. j. (2024, 09 03). *AJTek*. Retrieved from AJTek: https://www.ajtek.ca/wsus/how-to-backup-windows-server-update-services/

National Institute of Standards and Technology. (n.d.). *Computer Security Incident Handling Guide.* Retrieved from https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

1. (Marshall, 2024) [↑](#footnote-ref-1)
2. (Kost, 2024) [↑](#footnote-ref-2)
3. (Admin, 2020) [↑](#footnote-ref-3)