Approach for Handling Cyber Security Incidents in an Organisation

Nishant Mehta[#1], Dr.Sonali Patil[*2]

[#]*M-Tech Student &* [*]*Associate Professor*
K.J Somaiya College of Engineering, Vidyavihar, Mumbai – 400077, India

Abstract *— Criminals and nation states are increasingly attacking the technology assets of individuals, organisations and governments, stealing and selling valuable information, and in an alarming trend, paralysing critical infrastructure.*
So handling and responding to such computer security incidents has become an important part of information technology programs due to growth in digitalization of today's world.
To carry out incident response into any organisation requires substantial planning and resources. In this paper, the focus will be on handling variety of incidents which occur in an organisation.

Keywords— *Incident response, phishing, ransomware, malware,.*

I. INTRODUCTION

Incidents are the series of events that have a negative impact on the company. An incident could be somebody seeing that somebody stealing from the company, security administrator looking at audit trails and seeing there is a problem or getting to know there is some malicious activity in the trails. So for that, there should be a warning bell saying that there is a threat or a potential problem. For handling such incidents, there is an Incident Response Team who get in the moment the incident happens. This team is aware of what are their roles, procedure to follow, all their responsibilities, whom to communicate with.

The goal is to first contain the problem so it doesn't get any worse. And then to repair any damage that was caused by the incident. The skills that Incident Response (IR) team member should have will be as communication skills, training on company policy including their procedures as part of the response team for incident management, able to handle incident management and technical skills.

As part of the incident response plan one might halt activities to take pause and collect as much information as possible of the current state of the system. But in incident response team and incident response plan need to specifically address cyber-attacks. One of the important aspect of incident response is that the team need to be prepared to learn from the incidents that occurred in past.

Finding out the root cause of the incident is the most important task of incident response team. This might help to get to know how the incident was occurred; because of what reasons.

II. LITERATURE SURVEY

In the year 2016 following security incidents occurred around the globe as per the Symantec Internet Security Threat Report. Total 1209 breaches out of which 15 breaches with more than 10 million identity exposed. Total identity exposed 1.1B and average identity exposed per breach was 927 thousand. Organization faced email threats, malwares and bots attacks as follows: in year 2016 53% spam rate out of which 1 in 2596 phishing rate, 1 in 131 email malware rate, 357 new malware variant and 98.6M bots. Mobile devices attacked in year 2016 was with 3.6k new variant of malware. 76% of scanned website with vulnerabilities out of which 9% were critical and as per average number of attacks blocked per day is 229k. Number of detection of ransomware in year 2016 was 463,841 and average ransom amount demanded 1077$. Due to increase in the security incident day by day it is essential to handle in effective manner. This paper represent the day to day incidents faced by the organization and the methodology by which incident can be handled.

III. METHOD FOR HANDLING CYBER-SECURITY INCIDENT

It is important to have an incident response plan in place before handling the any cyber security incident.

Incident response plan must clearly specify the following points:

1. Identify what assets to be protected and the potential threats to the organization.
2. Identify, Categorized and Document organization vitals / essentials, potential threats and vulnerabilities.

Before handling any security incident it is important to know what type of incidents are there and what incident had occurred. It is also important to classify the incidents as well as what is the severity of the incident.

Different types of incident that may occur in an organization is as follows:

IT infrastructure (Hardware/Software), natural calamities, internal personnel, external personnel.

This paper will focus on the frequent and most common Information Security Incidents an organization face:

1. Malware
2. DDoS
3. Phishing Mail
4. Data exfiltration
5. Rogue Mobile Application

Handling Cyber-Security Incident

For handling information security incidents few steps need to consider which is mentioned below:

1. Information gathering
2. Identification of the Incident
3. Implementing control measures for the incident
4. Discover the origin of the incident
5. Patch the system from known vulnerabilities
6. Document and report to higher authority regarding the incident.

Following is the cyber security incident handling flow chart.

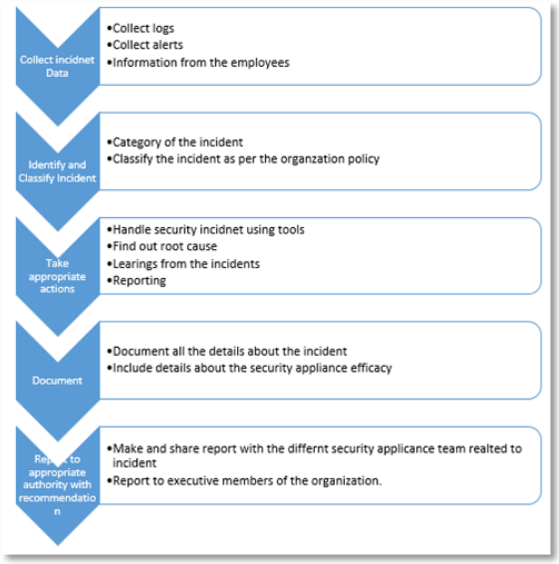

Figure A. Cyber-Security Incident flow chart

B. Steps taken for finding out Root Cause of Cyber-Security Incident

In handling any incident it is important to find out the root cause of the problem. For finding out root cause following steps shall be followed:

Figure B. Root Cause of Cyber-Security Incident

IV. Cyber-Security Incident Response Methodology

Incident response is a planned methodology for managing the consequences of a security breach in the organization. The aim is to handle the security incident which limit the damage and reduces recovery time and costs. Step by step process has to be mentioned for handling various security incident as a guideline for incident response team when the security incident occurs.

An incident response team should have all the details of various team members handy. And should be in coordination with other teams such as general IT staff, legal department member, human resource team, public relations department.

To handle information security incident, incident response team shall need to follow the following steps:

1. Detecting security incident.
2. Responding to particular security incident.
3. Containment of the problem.
4. Recovering from the security incident.

For the above steps following details need to get covered:

1. Finding out possible source of the attack.
2. Possible symptoms after the attack.
3. Classification of the incident based on severity.
4. Taking appropriate steps to handling the incident and minimizing the damage to system.
5. Contacting third party to take action against the incident as required.
6. Recovering the data with minimum cost.
7. Getting key notes for the incident.
8. Maintaining record of all the incident in the detail.

V. Different Security Incidents

A. Malware attacks

Attackers are targeting the organization by different methods but the most common method is spreading malware.

Following are the steps taken for handling cyber-security incident related to malware:

a) Detecting an Incident:

Possible source of attack include:

Banks employee downloading and installing / running portable tools from unauthorized website without permission.

- Installing of software with hidden malware on organization network, systems and infrastructure.
- Organization employee receiving mail with attachment containing malicious link / file.
- Attaching of infected and authorized device connected to Bank's network.
- Organization employee while browsing over the internet, unwanted popups to download and add-ons to browser get downloaded which try to download other malicious content from the internet.

- Attacker targets the organization employee by learning browsing history of the employee and infecting the website to which the employee visit on frequent basis.
- Networking devices like Bluetooth remaining on is vulnerable to malware attacks.

Possible symptoms include:

- Antivirus software raising an alert, unable to update its signature, shutting down or unable to run manual scan.
- Antivirus pop up messages of malware detected on frequent basis but unable to clean.
- Showing system space running out message when tried to install any new software or trying to save some file on the system.
- Unusual hard-disk activity: the hard drive makes huge operations at unexpected times.
- Unusual network activity: slow internet connection / poor network share performance at irregular intervals.
- System getting infected due open share available on the network.
- The System reboots unusually.
- Increase in "Blue screen of death" error.
- Application crashing unexpectedly.
- Pop ups windows appearing while browsing the web or in some cases without browsing.
- Unwanted ads shown while browsing and unwanted plugins and home page get set into the browser.
- Services like command prompt, task manager, and registry stop working.
- Desktop wallpaper showing unwanted messages.
- IP address (if static) is blacklisted on one or more Internet Black lists.
- People are complaining about receiving spam / random emails your organization.

b) Response

- Classify the incident based on its criticality / severity. If the criticality / severity is very high then contact external incident response agencies to provide assistance.
- In the infected systems check for the following:
- Check all running processes for unusual / unknown entries.
- Check for any unusual / unexpected network services installed and started.
- Check for any unusual programs launched at boot time.
- Check for any unusual big file on the storage support.
- Check for any unusual files added recently in system folders
- Check user's autostart directory
- Check for unusual and unknown accounts created especially in the Administrators group.
- Check for file shares.
- Use a sniffer and see if there are unusual attempts of connections to or from remote systems.
- Check for log files for unusual entries.
- Check firewall log files for suspicious activity.
- Volatile memory capture for analysis
- Try browsing sensitive websites and check if unusual network activity is triggered.
- Communicate to the end users, customers, partners, making them aware about the attack.
- Disconnect / disable wifi, Bluetooth like services.

Notify organization executive and legal teams about the attack on: Nature of attack, Impact, Timelines

c) Containment:

- Quarantine the machine to prevent more infection on the network and to stop any action being done from endpoints.
- Analysis of suspicious binaries and learn about malware nature.
- If network is infected, switch to alternate sites.

d) Recovery:

- If possible reinstall the OS and the application restore user's data from clean, trusted backups.
- If possible try to remove the malware infection from the system using end point security tools and try to recover the infected files using recovery software.

In case the computer has not been reinstalled completely:

- Restore files which could have been corrupted by the malware, especially system files.
- Reboot the machine after all the suspicious files have been removed, and confirm that the workstation is not exhibiting any unusual behavior. A full, up-to-date AV scan of the hard-drive and memory should be performed.

B. DoS / DDoS attacks:

Organizations are receiving threat mail from the attacker for paying ransom it avoid the DoS / DDoS attacks. In case of any DoS / DDoS attack following things need to be considered:

a) Detection

Possible source of attack:

Internal / External network, Botnets, Cloud based attack, and End User.

Possible symptoms of attack:

- Services responding slowly or non-availability of services. For example a page takes several minutes to render.
- Server crashes. For example, server returning a 503 "service unavailable'" error

- DDoS mitigation services indicating unexpected services on a legitimate port
- Suspicious Bandwidth congestion
- Alerts from implanted security devices such firewall and IDS
- Notification from ISP, and third party

b) Response

- Classify the incident based on its criticality / severity. If the criticality / severity is very high then contact external incident response agencies to provide assistance
- Understand the logical flow of the DoS / DDoS attack and identify the infrastructure components affected
- Identify and differentiate the traffic generated due to DDoS
- Connect with ISP to understand if the DoS / DDoS attacks is their end. Also communicate with ISP for assistance in controlling the traffic specific to network blocks involved, source IP addresses and protocols
- Notify the organization officials about the DDOS attack with details like nature of attack, impact and timelines

c) Containment

- Use tools which provide DoS / DDoS protection at layer 3, layer 4 and layer 7
- Organization need to temporarily disable the application features, if the application is affected
- Attempt to throttle or block DDoS traffic as close to the network's "cloud" as possible via a router, firewall, load balancer, specialized device etc
- Terminate unwanted connections or processes on servers and routers and tune their TCP/IP settings
- Switching to alternate network till the incident get properly handled
- If required, route traffic through a traffic-scrubbing service or product via DNS or routing changes
- Connect / Work with ISP to understand if the issue at their end is being resolved or not

d) Recovery

- Ensure that the impact services are restored and available again
- Ensure that your infrastructure performance matches the required baseline performance standard

Roll back of mitigation measures:

- Switch back traffic to your original network
- Ensure secure configurations and restart stopped services
- Ensure that the recovery-related actions are decided in accordance with the network teams. Bringing up services could have unexpected side effects.

C. Phishing:

Due to lack of understanding of the security, the employees of the organization are targeted with phishing mails which indirectly affect the organization. Following is the process to handle phishing incidents:

a) Detection:

Possible source of Attack:

- Use of subdomains and misspelled URLs
- URLs created using different logical characters to read exactly like a trusted domain
- Intelligently crafted email
- Public sources / Social media sites

Possible symptoms of attack:

- Employee opening crafted malicious email can infect the system which can spread across the network affecting the network and system performance
- Unwanted popups in the system without user intervention
- URL redirecting to malicious domain, changing browser settings

b) Response:

- Classify the incident based on its criticality / severity. If the criticality / severity is very high then contact external incident response agencies to provide assistance
- Communicate the employee regarding URL of the phishing website to prevent the employee from accessing it
- Communicate to end users, customers, partners via e-mail making them aware about the phishing attack
- Notify organization executive and legal team about the attack. Which includes details like nature of attack, impact and timelines of the attack

c) Containment:

- Check the source code of the website to know how the data is exported, either by sending an email to fraudster or by another script
- In case of phishing page hosted on a compromised website, contact the owner of the website to remove the fraudulent content
- Contact the hosting organization of the website to take down the website as soon as possible
- Contact the email hosting organization to shut down the fraudulent e-mail account

d) Recovery:

Ensure that the fraudulent pages and / or e-mail address are down.

D. Data Exfiltration:

Organization are spending huge amount in security but then also organization data is send outside the

organization. In case of data exfiltration incident following steps need to be consider.

a) Detection:

Possible data exfiltration source include:

- Internal and external network.
- Loss of storage media.
- End Users.
- Malware

Possible Symptoms include:

- Data being sent from organization's network to external and unauthorized destinations using FTP, Instant Messenger etc.
- Suspicious logs of uploading of organization's data via forms on websites
- Printing of organization's confidential and private data via unauthorized reprographic devices
- Logs generated by DLP solutions / tools
- Decrease in network performance due to huge data sent across / outside the network
- Malicious / unauthorized system having multiple hits on proxy from the organization to the external network trying to upload the data

b) Response

- Classify the incident based on its criticality / severity. If the criticality / severity is very high then contact external incident response agencies to provide assistance.
- Isolate the system/device form where the data has been compromised from the organization's network and guard it as evidence using the Evidence Handling Guidelines of the organization.
- Check the browsing history of the system from where the data has leaked. Ensure that all browsers are scanned for history as users use more than one browser.
- Check for end point protection logs which include AV, DLP, HIPS, and others endpoint security tool.
- Communicate to end users, customers, partners via e-mail making them aware about the phishing attack.
- Notify organization executive and legal team about the attack. Which includes details like nature of attack, impact and timelines of the attack.

c) Containment:

- Ensure that appropriate Information Security training is imparted to the organization's employees.
- Conduct periodic reviews of the logs generated by the DLP Solution/tool. The DLP solution/tool should cater to data rest and in motion.
- Ensure that all data transfer ports such as the following but not limited to USB, Bluetooth, Infrared, SD card slot are blocked and monitored to prevent loss of data.
- Ensure that all unwanted printed documents are fed to the shredder and disposed securely.
- Ensure that data important and confidential to the bank is stored in a secure location and standardized encryption methodologies are applied.

d) Recovery:

- Perform data leakage tests before restoring the compromised system to the last stable state.
- Change the password and authorization credentials of the compromised systems.

E. Rogue Mobil Application:

Due to digitalization every organization has their own mobile application available to make the work handy. Employees unaware about the security threats that is caused by installing third party made rogue mobile application understanding that the application is from the organization. Also the other application specifying the details of the organization without organization permission. Such kind of incidents related to application can be handled as follows:

a) Detection:

Possible source of attack:

- Unauthorized Application developed by 3rd party using organization name.
- Rogue application found on internet using organization's name and not available on the legitimate mobile application website.

b) Response:

- Check for the services accessed by the application.
- Check for the network activity when application is use and also when application in not in use.
- Check for any file drop by application in the mobile device.
- Check for the source code of the application for any malicious code.
- Check for the information stored in the application and network activity of the application for information sent over the network.

c) Containment:

- With the help of third party take down the malicious application from the internet
- Communicate to end users, customers, partners via e-mail making them aware about the malicious / rogue application available on the internet

d) Recovery:

Ensure that application is taken down from the internet and no links for that application is available.

VI. CONCLUSION

Experience and study has shown that handling incident response is a straightforward but continuous process. The aim of the paper is to address the common attacks faced by the organization and the way to handle it. As this paper specifies few of the common attacks that all the organization faces but there are other category of attacks emerging in day todays digital world. In this paper we specify the common steps taken to handle the information security incidents mentioning the different ways to handle the incident. Paper also specifies the steps taken to finding out root cause of the information security incident with appropriate action to be taken. Future scope of the paper include the incidents like web defacement, vishing, identity theft, etc.

References

[1] I. G. Jason Creasey, "Cyber Security Incident Response Guide," 11 2014. [Online]. Available: https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf.

[2] T. M. T. G. K. S. Paul Cichonski, "Computer Security Incident Handling Guide," [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

[3] C. Terrill, "How To Plan For Security Incident Response," 31 May 2017. [Online]. Available: https://www.forbes.com/sites/christieterrill/2017/05/31/how-to-plan-for-security-incident-response/#47c07e695bc8.

[4] M. Rouse, "Incident response plan," [Online]. Available: http://searchsecurity.techtarget.com/definition/incident-response-plan-IRP.

[5] J. B. Tucker Bailey, "Ten Steps to Planning an Effective Cyber-Incident Response," 1 July 2013. [Online]. Available: https://hbr.org/2013/07/ten-steps-to-planning-an-effect.

[6] "Types of Cyber Security Breaches – What are the Most Common?," City business solution, 23 September 2016. [Online]. Available: http://www.cbsit.co.uk/2016/09/types-cyber-security-breaches-common/.

[7] T. Campbell, "An Introduction to the Computer Security Incident Response Team (CSIRT)," 2003. [Online]. Available: https://cyber-defense.sans.org/resources/papers/gsec/introduction-computer-security-incident-response-106281.

[8] Symentec, "Internet Security Threat Report," April 2016. [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

[9] Cyber Security Coalition, "Cyber Security Incident Management Guide," October 2014. [Online]. Available: https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf.