International Journal on Emerging Technologies (Special Issue on ICRIET-2016) **7**(2): 41-47(2016)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

A Survey of Computer Security Incident Handling and Its Issues

M.D. Bhagwat*, Dr. P.H. Patil** & Dr. T. S. Vishawanath***
**Ph. D. Scholar, VTU Belgaum, Maharashta, India,*
***Professor, SKN SITS Lonavala, Maharashta, India,*
****Professor & HOD, BKIT Bhalki, Karnataka, India,*

(Corresponding author: M.D. Bhagwat)
(Received 16 September, 2016 Accepted 19 October, 2016)
(Published by Research Trend, Website: www.researchtrend.net*)*

ABSTRACT: When masquerader tries to cheat online user by applying a mixture of tricks for luring user to share personal information, it results into phishing attack. Phishing is very serious kind of attack which usually happens through social sites or usually visited websites by the user. Incident or event handling is similar to emergency medicine. The caregiver tends to be under pressure, and mistakes can be very costly. After the occurrence of incidence, users have to face other information robberies. Secure Incident Handling is the need of tomorrow's cyber wireless world. This chapter elaborates different cyber security aspects for Incident Handling and phishing.

Keywords: CERT, CSIRC, SOPs, *ISIRT*

I. INTRODUCTION

Nowadays, the Internet has become one of the most useful and widely available communication mediums on earth, and our life very much depends on it. Governments, banks, schools and corporations conduct their day-to-day business over the Internet. With such wide use, the data that resides on and flows across the network varies from banking and securities transactions to proprietary data, medical records, and personal correspondence. The Internet is cheap and easy to access, but the systems attached to it lack a corresponding ease of administration. As a result, many Internet systems are not secure. Additionally the underlying network protocols that support Internet communication are not secure to use, and few applications make use of the limited security protections that are currently available. The database available on the network make Internet systems vulnerable attack targets. It is common to see articles in the media referring to Internet intruder activities. But, however exploitation of security problems on the Internet is not a new phenomenon. In 1988 the "Internet Worm" incident occurred and resulted in a large percentage of the systems on the network at that time being compromised and temporarily placed out of service. Shortly after the incident, a meeting was held to identify how to improve response to computer security incidents on the Internet. The recommendations resulting from the meeting included a call for a single point of contact to be established for Internet security problems that would act as a trusted clearing house for security information. In response to the recommendations, the computer emergency response team coordination center (CERT/CC) was formed to provide response to computer security incidents on the Internet. The CERT/CC was one of the first organizations of this type. A computer security incident response team (CSIRT) was formed in 2001 to provide computer security incident response services to any user, company, government agency or organization [1][2][7].

Incident or event handling needs patience and courage. Hurriedly taken steps may result into mistakes which can be very costly. A simple approach is the best. The good experienced experts follow well defined and systematic steps for responding to security-related incidents. They follow six stages such as preparation, detection, containment, eradication, recovery, and follow-up.

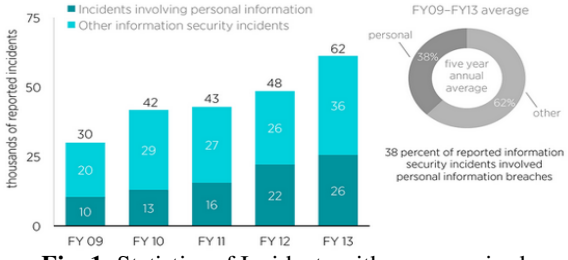

Fig. 1: Statistics of Incidents with compromised personal information and other.
(Source: Congressional Research Service, "Cyber-security Issues and Challenges: In Brief", December 16, 2014).

They call on others for help [3]. With other incidents, the personal information compromise incidents have larger statistics as shown in Fig. 1. It shows around 38% security incidents are the personal information breaches.

II. SECURE INCIDENT HANDLING

Organizing an effective computer security incident response capability (CSIRC) consist several major decisions and actions. The first considerations should be to form an organization. The organization should decide what type of services the team should provide, consider which team structures can provide those services, and select and implement one or more incident response teams. Incident response plan, policy and procedure creation are very important part of establishing a team, so that incident response is performed efficiently and effectively. The plan, policies and procedures should reflect the team's actions with other teams within the same organization similarly with outside parties, such as media, and other incident response organizations [1, 2].

A. Events and Incidents

It is defined as any observable occurrence in a system or network is called event. Events include a user connecting to a file share, a server receiving a request for a Web page, a user sending email and a firewall blocking a connection attempt. Adverse events are events like a negative consequence, such as network packet floods, system crashes, unauthorized use of system, unauthorized access to sensitive or important data and execution of malicious code that destroys data [2].

B. Incident Definition and Examples

Malicious code that is covertly inserted into another program to destroy data, run destructive programs or otherwise compromise the security, integrity and availability of the victim's data, applications or the whole system. These codes are designed to perform nefarious functions without the system's user knowledge. Malware consist attacker tools such as rootkits, backdoors and keystroke loggers, and tracking cookies [8].

A incident may involve any or all of the following:

Unauthorized computer access, Compromise of information integrity, A denial of service condition, Loss of information confidentiality, Loss of information availability, Misuse of systems or information, Physical damage to systems etc.

Risk. In general, hurdles are likely to come our way during the completion of project which effects on its progress. Risk is the "effect of uncertainty on objectives". A Risk is potential problem "it may happen or may not" While the internet is revolutionizing the way we do business, the risk the internet introduces can be fatal to a business. The Figure 2 depicts different risks during the process in execution [4].

Fig. 2. Different types of Risk.

Virus. A self-replicating code or program that spreads by inserting copies of it into other programs is called virus. Viruses insert themselves into host programs and propagate when the infected program is executed, generally by opening a file, running a program, clicking on a file attachment. Viruses are designed to play annoying tricks, whereas others have destructive intent [4].

Worm. A worm is nothing but type of virus that can spread automatically via e-mail, Internet relay chat or other network transport mechanisms. Worms are completely self-contained. They do not require a host program to infect a victim. They can create fully functional copies. They are self-propagating; unlike viruses. Worms take advantage unsecured Windows shares. Although some worms are intended mainly to waste network resources and system, many worms damage systems by performing some malicious acts [4].

C. Need for Incident Response

Incident response has become very important task because attacks frequently cause the loss of personal and business data. Incidents involving viruses, spyware, worms and other malicious code have damaged millions of networks and systems around the world. The advantages of having an incident response capability: Responding to incidents systematically so that the appropriate and quick actions are taken. Minimizing loss of information and disruption of services. To provide stronger protection for systems and data. Appropriate dealing with legal policies and issues that you may face during incidents [1, 2].

D. Incident Response Policy, Plan, and Procedure Creation

This section explain policies, plans and procedures related to incident handling and response, with an emphasis on interactions with outside parties, like law enforcement agencies, media and incident handling or incident reporting organizations.

Policy governing incident response is strongly individualized to the organization; most policies include the same key elements, regardless of whether the organization's incident response capability is indigenous or outsourced.

It is very important for the organizations to have a formal, coordinated and focused approach in responding incidents. To effectively implement such a capability, an organization must have strong incident response plan. The plan provides the organization with a roadmap for implementing its incident response capability. The plan should provide a strong approach for how incident response capability can support to the overall organization. Each organization needs a plan that meets its unique requirements, which should correlate to the organization's size, mission, functions, and structure. The plan needs management support to effectively maintain and mature an incident response capability. The organization's strategies, mission and goals for incident response should help in determining the structure of its incident response capability.

Procedures should be based on the incident response plan and policy. Standard operating procedures (SOPs) are a delineation of the checklists, techniques, specific technical processes, and forms, which are used by the incident response team. SOPs should be comprehensive. In addition, following standardized responses should minimize errors, particularly those that might be caused by incident handling tempo and stress. SOPs should be tested to validate their usefulness and accuracy. It should be distributed to all team members. The organization should communicate with outside parties regarding an incident [1].

E. Incident Response Team Structure

An incident response team should be available for contact at emergency situation by anyone who discovers that an incident involving the organization has occurred. One or more team members, depending on the seriousness of the incident and availability of manpower, will then handle the incident. The incident handlers first do the analysis like the incident data and then determine the impact of the incident and gives response appropriately to limit the damage to the organization and restore normal services. Even if the team may have very few members, the team's success depends on the participation, motivation and cooperation of individuals throughout the organization. The incident response team structure identifies such individuals, discusses incident response team models. It provides advice on selecting an appropriate model [2].

Central Incident Response Team. An incident response team handles incidents throughout the organization. This model is effective for both small organizations as well as for large organizations with minimum number of computing resources.

Distributed Incident Response Teams. The organization has many incident response teams, each responsible for handling incidents for a particular segment of the organization. This model is effective and efficient for large organizations and for the organizations with large number of computing resources at distant locations. The incident response teams should be part of a single centralized entity because the response process is consistent across the organization and information is shared among many people. This is very important because multiple teams may handle similar incidents. Good communication between teams and consistent feedback or review makes incident handling more effective and efficient [1, 2].

Coordinating Team. An incident response team provides suggestion to other teams without having authority like a department wide team may assist individual agencies' teams.

III. HANDLING AN INCIDENT

Information security management is a continuous process and iterative cycle. It has several phases, from initial preparation through post-incident analysis. The initial phase involves formation of team and basic training, and collection of the necessary tools and resources. During preparation, the organization also attempts to limit the number of incidents that can occur by selecting and implementing a set of controls based on the results of risk assessments. The use of proper security protection and safeguard reduces the risk of attacks. Secure incident handling is a continuous process which performs the activities before, during and after some incident occurs. The major phases of the incident response process are preparation, detection and analysis, containment, eradication, recovery and post-incident activity [2]. Figure 3 shows different steps in incident response life cycle.

When you are not prepared and security incident occurs then follow these basic steps first:

i. Remain calm.
ii. Notify the right people, choose them and get help.
iii. Tell the details of the incident to the minimum number of people possible for preserving privacy.
iv. Do not use email, chat, talk or news to send some information, instead use phone and fax.
v. Remove computer system from the network.
vi. Prepare a backup of the affected system by using unused medium.
vii. Get back in business by restoring your system from backups to determine whether it can resume its tasks.
viii. Learn from the experience, so you may remain prepared for the next time an incident occurs [7].

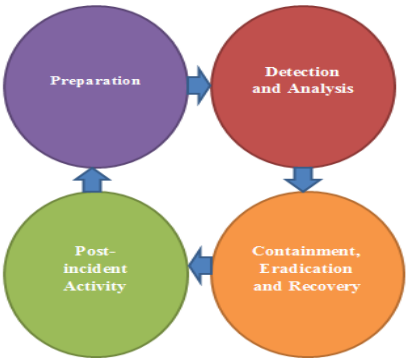

Fig. 3: Incident Response Life Cycle

A. Preparation

Incident response methods typically emphasize preparation so that the organization is ready to respond to incidents. Also it prevents incidents by ensuring that systems and networks are secure. Although the team is not responsible for incident prevention, it is now considered as a basic component of incident response programs. The incident response team's expertise should be valuable in establishing recommendations for securing systems [1, 2].

Table 1: Planning and preparation Activities.

Sr. No.	Activities in planning and preparation
1.	Incident Handling Plan
2.	Reporting Procedure
3.	Escalation Procedure
4.	Security Incident Response Procedure
5.	Training
6.	Monitoring Measure

B. Detection and Analysis

Incidents can occur in number of ways, so it is very difficult to develop a right procedure for handling every incident. So it is important for any organization to be prepared generally to handle common incident types.

Table 2: Detection and Analysis Activities.

Sr. No.	Activities in Detection and Analysis
1.	The Description of the incident.
2.	The Damage or impact made
3.	Indication if the attacker is still active in the system
4.	Information of the system like system name, version. functions, host name, IP address, operating system etc.
5.	Supporting information like screen capture and system messages

The incident categories listed below are neither comprehensive nor intended to provide definitive classification for incidents; rather, they simply give a basis for providing advice on how to handle incidents based on their primary category [1].

C. Containment, Eradication, and Recovery

When an incident is detected, it is very important to contain it before the damage increases. Most incidents require containment, so it is very important to handle each incident. An essential part of containment is decision-making like disconnect it from a network, shut down a system, disconnect its modem cable and disable certain functions. Such decisions are easy to make if strategies and procedures for containing the incident have been predetermined. Organizations should define acceptable risks in dealing with incidents and develop strategies accordingly.

Containment strategies are based on the type of incident. It is strongly recommended that organizations create separate containment strategies for each type of incident separately, to facilitate quick and effective decision-making.

In some cases, some organization delays the containment of an incident so in that case the incident response team should discuss delayed containment to determine if it is feasible. If an organization knows that a system allows the compromise to continue, it may be liable if the attacker uses the same system to attack any other systems. The delayed containment strategy is very dangerous because an attacker could escalate unauthorized access or compromise other systems within a fraction of second. Only a highly experienced incident response team should monitor all of the attacker's actions and disconnect the attacker to attempt this strategy.

Table 3: Containment Activities.

Sr. No.	Activities in Containment
1.	Conducting impact assessment of the incident on system data
2.	Confirmation if the data or service had already been damaged.
3.	Protection of sensitive or critical information and system.
4.	Decision on the operation status of the compromised system.
5.	Building an image of the compromised system as evidence for subsequent follow up action.
6.	Keeping a record of all actions taken during this stage.
7.	Checking any systems associated with the compromised system through any relationship.

Eradication. The next task after containment is eradication. Eradicating an incident is to remove the cause of the incident from the system, such as removing a virus from the infected data or system. Possible Actions for Incident Eradication are follows.

Recovery. The purpose of this stage is to restore the system to its original state. The recovery stage include following tasks or activity.

Table 3: Eradication Activities.

Sr. No.	Activities in Eradication
1.	Kill all active processes of hacker.
2.	Delete all fake or image files created by the hacker.
3.	Eliminate all malicious programs installed by the hacker.
4.	Apply patches and test the system thoroughly before restore it to.
5.	Correct improper settings in the system.
6.	In case of a computer virus incident or malicious code, follow the advices of anti-virus tool.
7.	In some case make a use of security scanning tools.
8.	Update all the passwords of all login accounts.
9.	Keep a record of all actions performed.

Table 4: Recovery Activities.

	Activities in Recovery
1.	Perform damage assessment.
2.	Re-install the deleted or damaged files. Sometimes the whole system.
3.	Verify that the system is back to its normal operation means the restoring operation was successful or not.
4.	Prior notification to all related parties like operators, administrators and senior management
5.	Disable unnecessary services.
6.	Keep a record of all actions performed.

D. Post-Incident Activity

Post incident activity is one of the most important parts of incident response since it is also the most learning and improving thing. Each team should reflect or discus new threats, lessons learned and improved technology. Many organizations have found that holding a meeting with all involved parties after a major incident is extremely helpful in improving the incident handling process itself. This meeting provides a chance to learn by reviewing what occurred, how well intervention worked and what was done to intervene. The meeting should be held at the end of the incident [8].

IV. INFORMATION SECURITY INCIDENT RESPONSE TEAM (ISIRT)

An ISIRT shall be established in each bureau/department (B/D). ISIRT is the central body responsible for communication, coordination. It takes security incident handling actions in the B/D. The size and scale of ISIRT varies according to the relative sensitivity of the systems, the scale and scope of the systems in different B/Ds, and potential impact of security incidents on them [8].

A. Functions of the ISIRT

The major functions of the ISIRT are: Overall supervision and coordination of security incident handling within the B/D. Necessary follow up actions, report to police and further assistance. Dissemination of security alerts on impending within the B/D.

iv. Information sharing within the B/D on security incident handling [8].

B. ISIRT Formation

The ISIRT is coordinating all IT security incidents within the respective B/D. Head of B/D should designate an officer from the senior management team to be the commander of ISIRT. The commander should have the authority to appoint core team members for the ISIRT. In the formation of ISIRT, the advice and support from the Defense Information Technology Services Organization (DITSO) is required to assist the ISIRT commander to develop system specific security policy and incident handling plan to establish the related logistical arrangements. The DITSO also needs to ensure that the departmental IT security policy is observed and enforced in all the information systems of the respective B/D.

There are a number of roles that the ISIRT has to play like ISIRT Commander, Incident Response Manager, and Information Coordinator. These roles can be performed by a single officer or may be different officers [8].

C. Roles of the ISIRT

ISIRT roles vary depending on different system entities.

Commander. The responsibilities of the commander are as follows.

Making decisions on critical matters like system recovery, the extent of involvement and the engagement

of external parties and service resumption logistics after recovery etc. Depending on the impact of the incident on the business operation of the B/D, triggering the departmental disaster recovery procedure where appropriate. Providing management on the provision of resources for the handling process. Providing endorsement in respect of the line-to-take for publicity. Coordinating with the Government Information Security Incident Response Office (GIRO) on incident reporting and necessary follow up actions [8].

Incident Response Manager. The role of Incident Response Manager is to monitor all security incidents handling process within the B/D and support for the handling process and seeking management resources. The responsibilities include: Overall management and supervision of security incident handling within the B/D. Alerting the ISIRT Commander upon receipt of report. Reporting the status of the security incident handling process to the Commander. Coordination with various external parties, such as service contractors, to support vendors, Police, and security consultants etc. in handling the incident [8].

Information Coordinator. The role of Information Coordinator is to handle public inquiries regarding the security incident of the B/D. The Information Coordinator is responsible for the overall control and supervision of information dissemination to the public, including the media [8].

Information System Manager. The information system manager will oversee the whole security incident handling process. The responsibilities include: Developing as well as implementing the system specific security incident response procedures. Observing and following response procedures for reporting incident to the ISIRT of the B/D. Coordination with all the concerned parties like service providers, contractors, and product support vendors etc. It takes rectification actions against the incident. Reporting the security incident and requesting for external assistance, such as Police and evidence collection. Providing technical support, evidence collection, system backup and recovery etc.[8].

V. TYPES OF INCIDENTS

There are numerous types of incidents like denial of service, malicious code, unauthorized access, intellectual property threats, etc. Table 6 depicts the incident types and respective actions to be taken.

Table 5: Types of Incident

Type of Incident	Description	Action
Unauthorized access	An individual physical access without permission to system, network, application, data, or other resource.	Examine firewall router protections. Examine access services regularly.
Denial of service	An attack that prevents normal authorized functionality of a system, network, or application by exhausting resources.	Employ backups for core services.
Malicious code	Successful installation of malicious software like virus, worm, or other code-based malicious entity.	Use virus checkers. Report suspicious activity. Monitor outgoing traffic. Protect the software load process. Use alternative sources.
Scans, probes, attempted access	Any task that seeks to access or identify a open ports, protocols, service. This activity does not directly result in denial of service.	Report probes to incident response team. Assess the damage.
Intellectual property	It includes the creative ideas and expressions of the human mind.	Inventory your intellectual property. Prioritize your intellectual property. Assign financial value. Implement misuse detection methodologies. Stay with the laws.
Investigation	Unconfirmed incident which is potentially malicious.	Collect maximum data. Target analysis [6][7][9].

The most important thing is dealing with phishing attack before it actually happens. Phishing attacks come in all shapes and sizes. Victims are both organization as well as single user.

VI. CONCLUSION

Today's world many people or many organization facing increasing cyber incident, it is necessary for them to monitor these entire incident effectively and carefully. Also management for incident handling is also very important. It is necessary to take care before the incident occur because many practical solution for such problems exists, but not a single comprehensive solution available to till date. Some solutions may be excellent but useful for particular incident only.

REFERENCES

[1] Karen Scarfone, Tim Grance, Kelly Masone, "Computer Security Incident Handling Guide" National Institute of Standards and Technology, March 2008.

[2] Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, Mark Zajicek, "Handbook for Computer Security Incident Response Teams (CSIRTs)" April 2003

[3] Maria B. Line, Eirik Albrechtsen, Stig Ole Johnsen, Odd Helge Longva, and Stefanie Hillen, "Monitoring of Incident Response Management Performance", SINTEF ICT, S P Andersensvei 15B, N-7465 Trondheim

[4] Alteren, B.," Implementation and evaluation of the Safety Element Method at four mining sites", *In Safety Science,* Volume **3**, pp.231-264, 1999.

[5] British Columbia Institute of Technology (BCIT): Industrial Security Incident Database Reporting Form. (2005)

[6] U.S. Department of Justice, "Incident Response Procedures For Data Breaches", U.S. Department of Justice Instruction 0900.00.01, August 6, 2013.

[7] Stephen Northcutt, "Computer Security Incident Handling- An Action Plan for Dealing with Intrusions, Cyber-Theft, and Other Security-Related Events", Version 2.3.1, March 2003.

[8] The Government of the Hong Kong Special Administrative Region, "Information Security Incident Handling Guidelines", Version: 5.0, September 2012.

[9] United States Government Accountability Office, "Information Security-Agencies Need to improve Cyber Incident Response Practices", Report to Congressional Requesters, April 2014.