International Journal of Innovation in Computer Science and Information Technology
Vol.2, NO.2 , P: 25 - 30
Received : 08 April 2020
Accepted : 15 June 2020

Provide architecture for response to computer incident in framework NIST sp800-61 and ITIL

Mahdi Sadeghi Ghahareh
Master engineer computer, Department of computer, Faculty of Electrical and Computer Engineering, Islamic Azad University, Tehran north Branch, Tehran, Iran.
md.sadeghi.gh@gmail.com
Nasser Modiri
Assistant Professor, Department of Computer, Faculty of Electrical and Computer Engineering, Islamic Azad University, Zanjan Branch, Zanjan, Iran.
nassermodiri@yahoo.com

Abstract:
In this paper provided response architecture for incident. This architecture is made for computer emergency response team (CERT) to incident response. This helps to team just for response. In this architecture used parameters NIST sp800-61 and also this is in framework NIST standard and ITIL framework. This architecture activated after discover incident and gain information about incident. This is response incident after pass a process. This architecture in this process makes documentary, report and etc. for incident response. In addition, defensive center can certain some incident (now can say these are threat) if necessary and when happens these are, CERT impact defensive or offensive to the threat. In the end this architecture can response incident in the form of documentary, limiting system that have response, reports to the defensive center and manager system or organ, defensive or offensive against incident(or threat) and etc.

Key words: incident, response, defensive, offensive, ITIL, NIST, incident response.

Introduction:

Computer security incident response has become an important component of information technology (IT) programs [1]. When computer security incidents occur, it’s critical for organizations to have an effective way to identify that something has happened and conduct a response [2]. WITH the increasing number and diversity of cyberattacks, Computer Emergency Response Teams (CERTs) emerged as a solution that provides timely response and proactive protection against these threats [3].One of the works that computer security response teams(CERTs) are doing, is response to incident. Response to the incident is very important and effect because incident, the programs or systems. Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources [1]. Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented [1].Performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources [1]. In the following expressed frameworks of these work, ITIL incident management and NIST sp800-61.

ITIL Incident Manager:

ITIL is a collection of best practices for the management of IT services. ITIL helps organizations to become aware of the business value their IT services provide to internal and external stakeholders. The ITIL security management process describes the structured fitting of security in the management organization [4].The Information Technology Infrastructure Library (ITIL) is a framework of best practices that promote quality computing services in IT sector. ITIL was first developed by the British Central Computer & Telecommunications Agency merged [4]. Incident Management and Problem Management are two main activities of ITIL service operation framework which handles incidents and their root causes respectively [5]. ITIL have four parts [4]:

- Service strategy
- Service design
- Service operation
- Continual Service Improvement

The important part in the Continual Service Improvement is incident manager. Incident manager is a cycle that started at discover incident to close the incident file.in the other words, identification the incident management process begins with identification. 2). Incident logging this step is required for each type of incident, both large and small. 3). Incident categorization in making incident categories requires a special process between the IT manager and the organization management [16, 17]. It aims to generate incident categories and priority handling in line with the organization's business processes. 4). Incident priority the incident priority step is based on a pre-made categorization. 5). Initial diagnosis The initial diagnosis of an incident must be carried out by any person initially connected with the incident, whether it is a service desk, a technical staff, or an automated device such as event management. 6). Incident escalation Incident escalation is an act of raising the level of incident handling. 7). Investigation (investigation and diagnosis) Investigation measures are conducted to find the source of the problem from the incident. 8). Resolution (resolution and recovery) this step is an action taken to resolve an incident. 9). Closing (incident closure) the closing step is the steps undertaken by the service desk and associated technician staff to ascertain whether the incident has been properly addressed [6]. In this paper cycle response to the incident is in framework of ITIL incident manager.

Nist sp800-61:

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate security information for all agency operations and assets [7]. NIST have 3 categories in the field security Computer, Internet, Information. This provided as a guide and recommendation. NIST published standard such as SP800, SP1800, SP500, SP-800-94 and etc. Cyber security framework NIST in organized showed in figure2.

These steps include: [8]

1. Define goals
2. Prepare a detailed proposal
3. Assess the current situation
4. Analyze the difference between the results and identify the necessary measures Implement an operational plan.

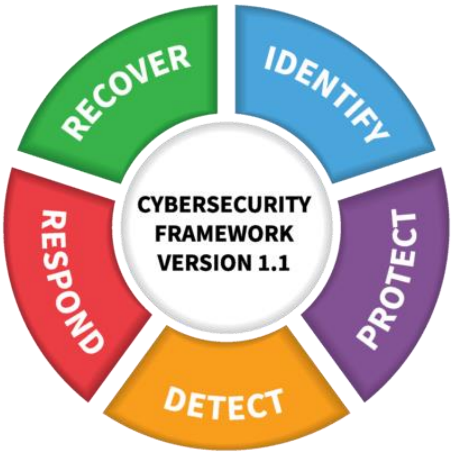


Figure1.cyber security framework [8]

NIST sp800-61 publication seeks to assist organizations in mitigating the risks from computer security incidents by providing practical guidelines on responding to incidents effectively and efficiently [1]. It includes guidelines on establishing an effective incident response program, but the primary focus of the document is detecting, analyzing, prioritizing, and handling incidents [1].

NIST sp800-61 includes Organizing a Computer Security Incident Response Capability, Handling an Incident and Coordination and Information Sharing. This standard explain how manage organ and what do and how do when incident occur and make response incident.

In the following explain suggested architecture and matched to NIST sp800-61.

Method:

In this part explain suggested architecture for response to incident. This tip is important that incident was discovering last. The cycle of this architecture is including:

- Analysis incident for response
- Specify systems that have incident
- Alarms
- Division teams incident response
- Limited systems that have incident
- Determine a solution to the incident problem
- Send report for CERTs
- Do solution
- Controlling team confirm that Executive team does right solution
- CERTs Check and confirm solution
- Determine the appropriate defense to deal with a repulsed incident
- Defense test
- Elimination limitation
- Inspection for final approval
- Prepare a report for the management department
- Documentation of answers
- Evaluate the response
- Learning Training related to the parts that were or are related to the incident
- Close response to the incident

Analysis incident:

This is first step. This step is analyzing incident for understanding detail of incident. If report was from last phase, helps analyzing and find details of incident. In this step determine response team what do in next's steps.

Specify systems that have incident:

In this step, determine limited of system suffer incident. In this step chose all of the system that should do incident cycle in system.

Alarms:
In this step, response team should announcement all of the part of system that occur incident, or affected response.

Segmentation response team:
In this step, response team is divided. One team for controlling response and else team doing response. Response team could divided to the else team if necessary. In controlling team can get help of person work with incident system.

Limiting system incident:
This step is necessary. All of the relationship to the system's incident as much as possible disconnected. This work helps to the system that controlling incident. Furthermore a new system should do works this system's that have incident.

Determine a solution to the incident problem:
Now in this step should founded solution for incident. This solution helped to system do not repeated. This step is similar to problem manager, but have different with problem manager. The ends of this step, founded solution for don't let repeated this incident in this system. For example one system occur virus, installing antivirus and scanning system and cleaning that is a solution for computer virus.

Send a report for CERTs:
In this step, at first is made report by response team. Team send this report at limiting, solution and etc. to the computer emergency response team.

Do solution:
After send report, team does solution that specified in last step. According NIST eliminating an incident is essential.

Controlling Team confirm that Executive team does right solution:
In this step, control team, check solution and all of the activity executive team. Control team is checking and testing all of the activity.

CERTs Check and confirm solution:
Now, CERTs checked all of the activity response team. It's important all of the steps do right and effect good. In this step, analysis results of last steps and in case of successfully confirm this response.

Set suitable defensive for ward off incident:
In the response should set suitable defensive. It's important because defensive don't let repeat this incident. Defensive guarded the system. Defensive have different type.

1- Defense based on the linear
2- Defense based on the zoning
3- Defense based trust
4- Deep defense

Choosing defensive is responsible response team. Also, this choose must accept to the CERTs and manager organ.

Test defensive:
If choosing defensive accepted to the CERTs and manager organ and don't disruption for programming systems, testing defensive. This defensive test for understand that is this useful or not? This is done by team consisting manager organ, persons of CERTs, response team and person that work by system.

Limit restrictions:
After make defensive and test that and else steps, system could been unlimited.

Inspection for final approval:
In this step, a team organized manager organ, staff of systems had incident. They should analysis system understand incident ended or not. This team should analysis system according to her wishes.

Prepare a report for the management department:

According to the NIST sp800-61 response team should send a report to the manger organ. This report should consist of all of the detail response. This report should in a way that understanding works response team.

Documentation of report:

Documentation is difference with report. In the documentation, you show all of the steps in the form of animated, image, video and etc. This is based all of the steps and shows in the how response to the incident. With documentation, in the future response team will understand what do with response.

Evaluation response:

In this step, is evaluation of employee, management and all of the relation of incident system. This step don't need done in the way and can run in the future.

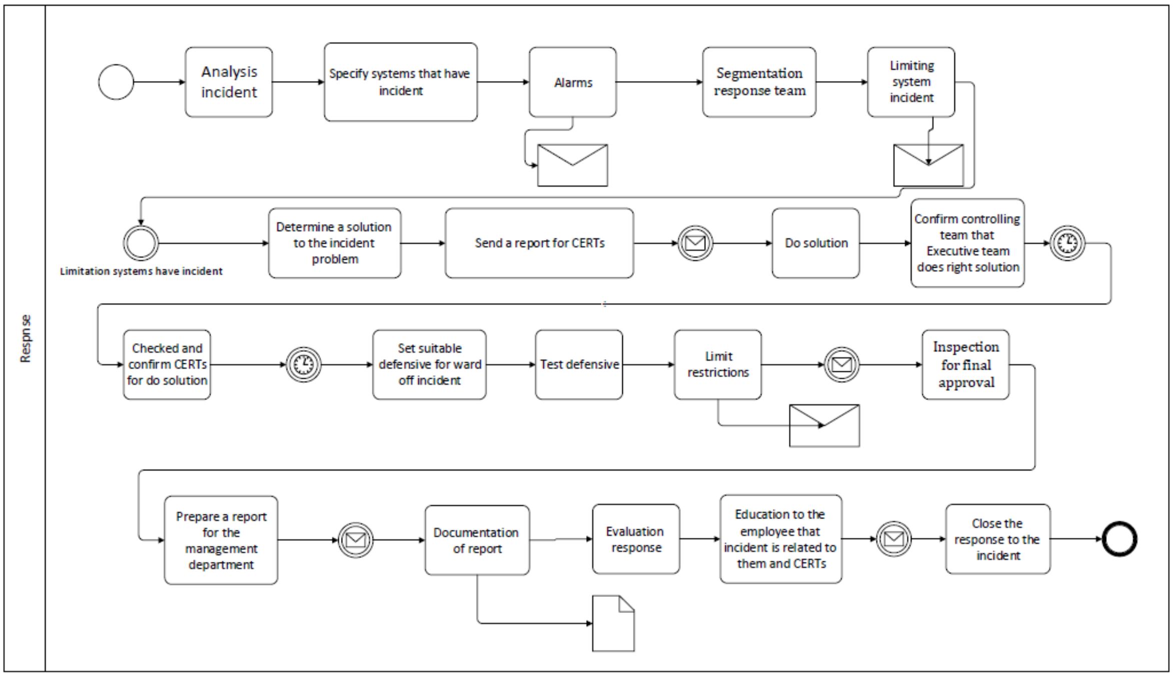
Education to the employee that incident is related to them and CERTs:

In this step response team should education employee that works with system have incident. After that is educated to CERTs that if repeat this incident or similar this, team response that.

Close the response to the incident:

At end response to the incident is closed.

In the BPMN process of response is including one lane. This lane is member of incident management pool. Graph 1 shows BPMN response incident.



Respnse
Analysis incident
Specify systems that have incident
Alarms
Segmentation response team
Limiting system incident
Limitation systems have incident
Determine a solution to the incident problem
Send a report for CERTs
Do solution
Confirm controlling team that Executive team does right solution
Checked and confirm CERTs for do solution
Set suitable defensive for ward off incident
Test defensive
Limit restrictions
Inspection for final approval
Prepare a report for the management department
Documentation of report
Evaluation response
Education to the employee that incident is related to them and CERTs
Close the response to the incident

Graph1. BPMN response incident

Conclusion:

This paper provided architecture in the cycle for response to the incident. This architecture is ability for send report, make documentary, make defensive for this incident especially and educated to the employee and etc. this architecture is in framework of NIST sp800-61. According this standard, response team should make process for incident limiting, make documentary and report and etc. Also, this is according incident management ITIL framework, and build a process of classification team, send report, announcement incident and etc. This architecture focused on response to incident and no else thing. This response architecture can use to defensive center for defensive at especial incident (threat). This can make reports good for CERTs and management of organ.

Reference:

1- Cinchonski, P & millar, T & Grance, T & scarfone.(2012). Computer security Incident handling guide. National Institue of standards and technology(NIST).

2- Ruefl e, R & Dorofee , A and etc. (2014). Computer Security Incident Response Team Development and Evolution. Copublished by the IEEE Computer and Reliability Societies.

3- Krsti, M & abarkapa, M & Jevremovi, A. (2019). Machine Learning Applications in Computer Emergency Response Team Operations. 27th Telecommunications forum TELFOR 2019.

4- Sheikhpour, R & Modiri, N (2012), A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management. Indian Journal of Science and Technology.

5- Refahi farjadi, A & Zoheir Mustafa, F. A CBR-based Approach to ITIL-based Service Desk.(2011, October). Journsl of emerging Trends in computingan d Information Science

6- V R Palilingan & J R Batmetan.(2017,October).Incident management in Academic Information System using ITIL Framework. IOP Conference Series: Materials Science and Engineering.

7- Fong ,J & Tong , J & Mao,J & Bohn, L & Leaf , D.(2011). Recommendation of the national Institude of standards and Technologe. National Institude of standards and technology

8- https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework