International Journal of Innovation in Computer Science and Information Technology
Vol.3, NO.3 , P: 50 - 55
Received : 22 July 2021
Accepted : 24 August 2021

Provided new architecture for discover and diagnose computer incident according NIST sp 800-61 and ITIL

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

Abstract

This paper provided new architecture for discover incident and make report of incident. This architecture is according standard NIST and ITIL framework. In this architecture at first recognize incident with controlling input and output system, monitoring all of the system in the regular time cycle. After that finding the reality incident and in the next step made accurate reports for next teams and manger organ. Also, in the architecture is made a database for controlling incident in future.

Keywords: incident, NIST, ITIL, offensive, incident computer, discovery incident, incident manager, diagnose incident, identification and classify incident, registration incident.

Introduction:

Todays, security in system computers is one of the important issues of societies. Many of the problems that arise in academic information systems come from incidents that are not properly handled [5]. Therefore, the security of information needs to be managed and controlled properly [7]. Incident management is very important in order to ensure the continuity of a system [5]. Therefore, different structure for prevent of computer incidents or events are made. Incident management requires organizations to establish processes for detecting, analyzing, responding to, and learning from incidents that threaten the con dentiality, availability, and integrity of critical systems and data [4]. Discovery of incident is first and important step. The most important part of the incident handling process is to determine whether the reported event is a security incident or not [6]. This paper was provided architecture for discovery incident and gain information of incident. Therefor, in first defined incident: Any event which is not part of standard operation of a service and which causes, or may cause, an interruption to, or a reduction in the quality of a service [2]. This tip is very important that incident and event have different. Event is part of incident. An event is any observable occurrence in a system or network. 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 [3].

In the following at first, explained frameworks ITIL and NIST and after that explain attack vectors and parameter about incident. In the last, said about proposed architecture and conclusion.

ITIL[1]:

ITIL is a collection of best practices for the management of IT services [1]. The ITIL security management process describes the structured fitting of security in the management organization [7]. The Information Technology Infrastructure Library (ITIL) is a framework of best practices that promote quality computing services in IT sector [1]. ITIL was first developed by the British Central Computer & Telecommunications Agency merged [7]. Incident Management and Problem Management are two main activities of ITIL service operation framework which handles incidents and their root causes respectively [2].In figure 1 is shown all of the parameter ITIL. ITIL have four parts [7]:

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

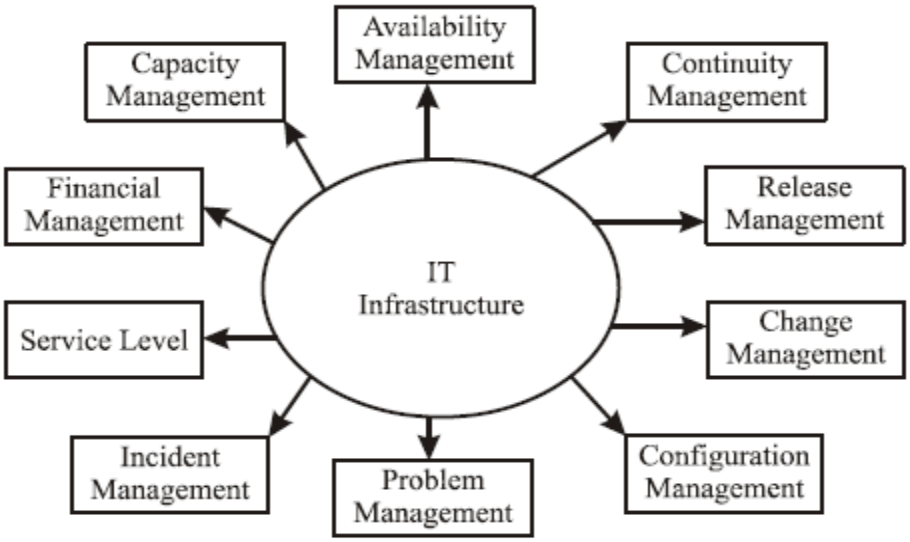

Figure1. ITIL parameter [9]

NIST:

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347 [3]. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate security information for all agency operations and assets [1]. NIST have 3 categories in the field security Computer,

[1] Information technology infrastructure library

Internet, Information. This provided as a guide and recommendation [1].

Cyber security framework NIST 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.

NIST sp800-61:

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 [3]. NIST sp800-61 includes Organizing a Computer Security Incident Response Capability, Handling Incident and Coordination and Information Sharing [1]. This standard explain how manage organ and what do and how do when incident occur and make response incident [1].

Attacks and parameter:

Incidents can occur in countless ways, so it is infeasible to develop step-by-step instructions for handling every incident [3]. So every organ should ready for detect every incident. Incident in the every organ or company is different. But incident have some important title that can classify incident in that. One of the title is ways occur and method incident. External/removable media, attrition, web, Email, impersonation, improper usage and etc are some methods of the incident. Different types of incidents merit different response strategies [3]. For many organizations, the most challenging part of the incident response process is accurately detecting and assessing possible incidents—determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem [3]. Most of the incident occurs in an organ related to work that organ do. So, teams of CERTs[2] that have detecting duty should know about organ work and cyber threats of the organ work.

Method:

In this part of paper explained suggested architecture for discovery and diagnose incident. This architecture has four parts; Discovery incident, diagnose incident, identification and classify incident, registration incident. All of these parts of architecture do especial work. Therefor this architecture is in the form pipeline. At first this architecture discovery incident with controlling and monitoring, then diagnose incident. Next, incident is identification and classify. And at last, incident is registration. In the following is explained all of these parts.

Discovery incident:

It is important that known incident is every event that make problem and get out system of the way. So, incident parameter in every organ, company and etc is different. But could been specify some parameter that popular incident and base parameter incident. For example some of the important ways that incident occur is attack of out of the system, DDoS, web, Email, forgery of identity, improper of Us, equipment theft and etc. Therefore, in this part should control and monitor all of the system. In this architecture, control all of the input and output and control all of the system and parameter that make incident. Addition control, monitoring is help for discovery incident. Monitoring all of the parts of system and checked important parts of system. This tip is important when a report receive of a system doesn't do right, in this time monitoring should active and checked system. Therefor controlling and monitoring are parts of discovery of incident and these are for discovery incident are very important.

Diagnose incident:

[2] Computer emergency reports team

After occurring incident and discovery by controlling and monitoring, should been it's important this is reality incident or not. Is explained this part by one of the example. When a system turned off and doesn't turn on, it may isn't system connect with power. This isn't incident. But if reason turned off is hacking, it is incident. In the other words in this part incident is fact finding and determine reality incident. This work is done by CERTs. CERTs should attention that incident doesn't attack for destroy system. Therefor this work should been done by especially team of CERTs that diagnose reality incident.

identification and classify incident:

Now, should been certain exactly incident is which type of classify incident. Therefore should been used table incidents in the NIST sp 800-61 standard or organ CERTs make a table of incidents especially occur in the organ or company. In this part, is certained exactly parameter of incident. As mentioned parameters of incident are different for every company or organ, but is called public in the following:

- Which part of organ occur incident?
- Which does system occur incident?
- What is the detailed explanation?
- Who does work with system?
- What time does incident occur?
- What does do system?
- How does understand system doesn't work well?
- Is incident repetitious?
- How long is occur at first incident?

All of these answer and else parameter helped to the else phase of CERTs. In this part all of information collection about incident. Next, characterized which is incident type incident?

Registration incident:

The last part, is made database of incident. This database is similar table and in front of the incident name write all of the parameter same time occur, which system, how occur and etc data of incident. In table1 showed sample of database.

Table1. Database of incident organ

Last Repeat Date	Actions taken to respond to the incident	Description of incident detection and identification	Number of occurrences	incident name	number
					1
					2

In the following is shown BPMN of this architecture.

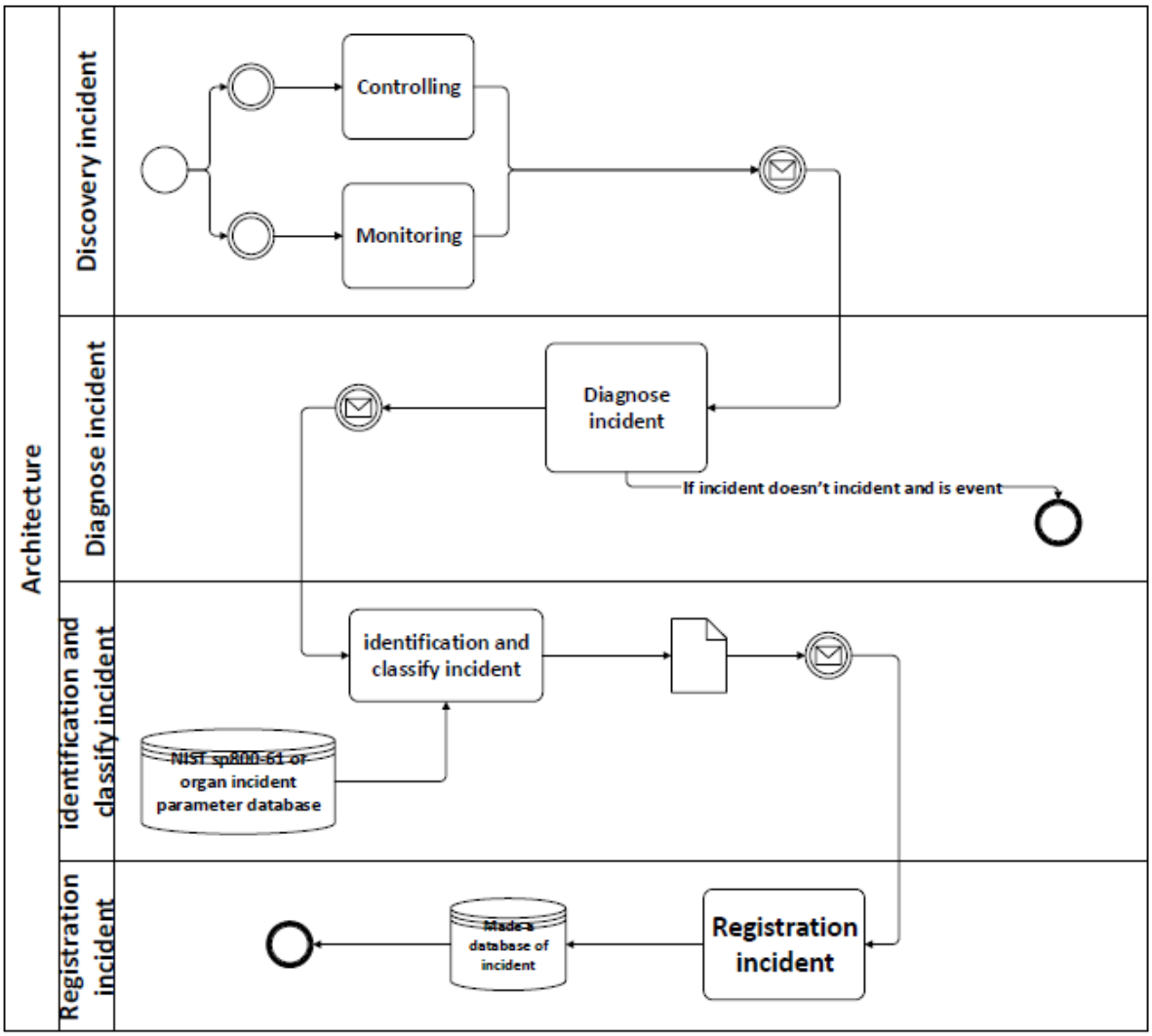

Figure2. BPMN of architecture

Conclusion:

This paper provided architecture for discovery and registration incident. This architecture has cycle form. This paper has pipeline form and made from 4 parts. This architecture can find incident with controlling and monitoring and discovery type of incident and save all of important parameter. This database can help to CERTs for responding incident and if repeatedly incident can use of last data. Also with pipeline form, in architecture all of parts are expert about their work and do works faster. This architecture is in ITIL framework and in NIST sp 800-61 standard. All of the type and parameter of discovery incident are in the form of NIST. At the end this architecture can use in the defense center for finding especial offensive incident that attack to the system. Defense center certain parameter offensive incident and every time these parameter occur sending alarm for the defense center.

Reference:

1- Sadeghi Ghahareh, M & Modiri, N.(2020). Provide architecture for response to computer incident in framework NIST sp800-61 and ITIL. International Journal of

Innovation in Computer Science and Information Technology.

2- 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*

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

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

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

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

7- 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*.

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

9- D. Dabade, T. (2007). INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL). Proceedings of the National Conference; INDIACom-2007.