eJAICT
ISSN 2355 1771
JOURNAL OF APPLIED INFORMATION, COMMUNICATION AND TECHNOLOGY
Published by:
Research Center of Technology and Innovation
Academic Research and Community Services
Swiss German University

Improving Cyber Security of Internet Web Gateway using NIST Framework

Azzam Fahmy

Department of Information Technology, Swiss German University, Tangerang 15143, Indonesia

Article Information

Received: 3 December 2018
Accepted: 4 February 2019
Published: 25 April 2019
DOI: 10.33555/ejaict.v6i1.63

Corresponding Author:

Azzam Fahmy
Email: azzam.fahmy@student.sgu.ac.id

ISSN 2355-1771

ABSTRACT

The internet utilization is become more growth for every year where the cyber-attack also taking part into risk in the organization. The existing cyber security infrastructure (Web gateway) shall be replacing to answer adequate of respond to threat, Vulnerabilities or viruses. Therefore, company using NIST Framework. to improving Infrastructure Cyber Security thru identification of risk. The framework will help Company to identify, asses and managing cyber security risk in regards with replacing the old Web Gateway. And future outcomes of the replacement of Internet web gateway shall address the current and future profile and managed security program base on risk evaluation.

Keywords: *Analysis Risk, Risk Management, Implementation Information System, Cobit 5*

1. Introduction

1.1. Background

The internet utilization is become more growth for every year where the cyber-attack also taking part into risk in the organization. The existing cyber security infrastructure (Web gateway) shall be replacing to answer adequate of respond to threat, Vulnerabilities or viruses. Therefore, company using NIST Framework to improving Infrastructure Cyber Security thru identification of risk. The framework will help Company to identify, asses and managing cyber security risk in regards with replacing the old Web Gateway. And future outcomes of the replacement of Internet web gateway shall address the current and future profile and managed security program base on risk evaluation.

According research conduct by ISACA's Cyber security Nexus found that Malware and malvertising threats destructive align with services move from desktop to mobile devices. In 2016 frequency of malvertising will increase by injecting malicious advertisement. In the ICT operation where in 2015 we have experienced incident breach with unauthorized end point which accessing internet from our internal network and introduce many viruses to our system. ICT Department response with policy where all devices which not provided by ICT is prohibit to access internal network and for every contractor in Offshore area the access for internet has revoked. Therefore, virus activity also getting high with introducing by malware from the internet or brought from external storage where users download from outside Office network. After the policy applied many unauthorized devices and users tries to gain access our network and cyber infrastructure by doing password cracking or stealing password using illegal software. Once password is compromise, they shared the account and used together the internet without adequate control mechanism which ICT Department can't see the false or true sessions.

They activity not only jeopardize the reability and integrity of the data or system but also made our network and bandwidth is high utilization. The legitimate users who having difficulties to access the internet as part of the work activity including online training, Online transaction and others information. This paper scope is to improve existing Infrastructure gateway by using NIST framework to made profiling of current situation and future outcomes (expectation) without making changes or evaluate the network environment. The Cyber Security definition is the body of technologies, processes and practices to protect networks, computers, programs and data from attackers, damaged from unauthorized access. How Company managed its Cyber security risk in order to replace the existing web gateway. By evaluate the existing Cyber security profile and establish Cyber Security program to improve cyber security infrastructure

2. National Institute of Standards and Technology (NIST) Framework

Cybercrime become popular in day to day, every company has force to protect against Malware, Viruses, attacker or unauthorized users or devices for gaining access thru Internet or Internal network. Therefore, many organizations establish IT policy inclusive guidelines and objectives in order to managed and secure they network environment as part of Confidentiality, Integrity and Availabilty, and to govern appropriate usage of ICT resources or to comply with standards or regulations. The Framework from National Institute of Standards

and Technology focuses for business drivers to guide cyber security activities and align cyber security risks as part of the organization's risk. The NIST Framework has of three parts such as Framework Core, Framework Implementation Tiers and Framework Profile. Framework Core have five (5) concurrent activities start from Identity, protect, detect, response and recover. The Framework Tiers consist of Tier 1 to Tier 4 which helps Company to consider its current risk management practices, threat environment, legal and regulatory compliance, and organizational constraints. The Framework profile helps Company to evaluate the existing risk profile with target (desire) outcomes based on business needs.

In ISO 31000:2009, Risk Management defined as principles and guidelines for managing risk. The risk management helps company to identify the opportunity and threats and prepare for risk treatment. Identification and evaluation of risk including consequences where likelihood and impact will be quantified into ranking, score or priority. The risk management helps Company to produce better decision or programme in order to mitigate, managed or to improve the business needs. In project management there are several types of risk that shall be effectively allocated with available resources such as Scope risk, technology risk, resources risk, schedule risk, etc.

3. Improving Cyber security program

This paper using NIST framework to evaluate the existing Cyber Security Profile and future outcomes which represent in replacing the old infrastructure. Scope of NIST Framework only using Framework Core to identify and evaluate risk and gaps. The cyber security program consists of Scope, orientations, creating current profile, conducting risk assessment, target profile and determine, analyze and prioritize Gaps. This program act as continuation of the existing program which required improvement in the cyber security.

3.1. Scope

According to ICT Policy, the objective of the CNOOC SES Ltd IT Policy is intended to:

- To ensure prudent and appropriate usage of IT and Communication resources.
- To ensure IT and Communication operations as a support function of the whole company operation is carried out in effective, efficient and secure/safe manners.

This Policy inclusive with guidelines to how ICT govern the best way to archives above objectives, therefore control and measurement shall be available such as balance score card. With annual target is zero for security breach. The scope of this program is to improve cyber security infrastructure where lead to zero high incident in replacing the old Internet gateway

3.2. Orientation

As data (information) integrity and availability thru protection become Company priority which required from Indonesian government to establish and enforce IT Policy in order to secure the business and Company data (information) against unauthorized users or devices and

the event of disaster due to system or hardware failure, viruses attacked , or lacked of control or monitored.

3.3. Current Profile

The current profile in improving the cyber security infrastructure in Framework core is Function of Identify with category of Risk Assessment (ID.RA) with aim for organization understands the cyber security risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. With sub category is ID.RA-4: Potential business impacts and likelihoods are identified. The current profile of cyber security infrastructure of web gateway using Bluecoat SG to protect and managed access thru internet, where the configuration is limited and without bandwidth management to managed utilization or priority

3.4. Risk Assessment

Risk assessment to overview risk, thread and vulnerabilities of cyber security to get insight about likelihood and impact to the organization as describe on below figure

Consequence		**Likelihood**				
		1	2	3	4	**5**
		Rare	Unlikely	Possible	Likely	**Almost Certain**
5	**Disaster**	5	10	15	20	25
4	Major	4	8	12	16	20
3	Moderate	3	6	9	12	15
2	Minor	2	4	6	8	10
1	Insignificant	1	2	3	4	5

Figure 1. Consequences and Likelihood table.

Risk Level	**Score**
Low Risk	1-3
Moderate Risk	4-6
High Risk	8-12
Extreme Risk	15-25

Figure 2. Risk Scoring base on Consequences and Likelihood table.

3.5. Create Target Profile

The target profile is to improve consistently of risk assessment about Potential business impacts and likelihoods are identified to provide course of action for ICT Department to minimize the Gap to the lowest / lower level. The future cyber security infrastructure web gateway shall address and have adequate control to eliminate risk. The future system shall

have minimum requirement as below:

- URL filtering
- HTTPS scanning
- Malware detection, both inbound and outbound
- Threat intelligence feeds
- Application control
- Threat and traffic visualization

3.6. Determine, analyze and prioritize Gaps

Risk	Likelihood	Consequences	Risk Score	Risk Level
Steal Password	**3**	**5**	**15**	**Extreme**
Shared Password	2	5	10	High
Malware Infection	**4**	**4**	**16**	**Extreme**
Phishing & Social Engineering	2	3	6	Moderate
Viruses, Worms & Trojans	2	4	8	High
Bandwidth Latency	2	3	6	Moderate
Quota Issues	2	2	4	Moderate
Document leakage	3	3	9	High
System Failure	1	4	4	Moderate

Figure 3 Risk Assessment

Based on the above figures, Stealth Password and Malware Infection are extremely high if the event occurred in our Company and become 1st priority to close the Gap in replacing the Old Web Gateway. The new system shall introduce more control for ICT department in order to managed cyber security risk.

3.7. Action Plan

Stealth Password and Malware Infection become high priority in order to mitigate risk, ICT Department convey a security program to protect and socialized and communicate risk management strategy. Protection shall refer to best practice in order to manage legitimated internet session a long with bandwidth management and virus protection. Company also campaign security awareness to assess asset vulnerable and threat of existing services regularly. The end point get the latest update of antivirus and security patch. The number of security breach shall be no more than one (1) incident (High) / annual and recorded into Key Performance indicators. Company also using additional SANS top 20 security control to evaluate and campaign security program

4. Conclusion

The function of Identify in NIST Core Framework, help Company to portray the current and future profile to minimize the Gap with selective action and program in order to review the cyber security infrastructure, However the IT policy need to establish as preliminary guideline. Below figures the summary of the risk profile capture from the current and future outcomes

Problem and Risk statements	Profile		Gap Analaysis and Outcomes
	Current Blue Coat SG	Future McAfee Web Gateway	
Malware Infection	Limited	Available	Bluecoat using antivirus protection to protect against virus , where McAfee advance with their global threat intelligence (GTI) protection database
Bandwidth Management **(Bandwidth Latency)**	Limited	Available	Blue Coat using white list and blocklist while McAfee has additional to manage bandwith base on destination
Dual Sesion Logging **(Shared Password),**	Not Available	Available	McAfee can manage only single session apllied to reduce Password Sharring / Hacked Issues
Only Joint Domain Users Can Access Internet **(Stealh Password)**	Not Available	Available	McAfee align with Single sign on (SSO) to protect unauthorize end point connect to Internet
Volume Quota **(Quota Issues)**	Limited	By Users, Groups & Destinations	Blue Coat volume Quota only for Selected group, while McAfee cant enhance to individual and also destination sites
Session Prioritations **(Document Leakage)**	Limited	Available	Blue Coat System has limited to create primary site which will have more bandwith or un challenge for designated websited, while McAfee enhance primary applied to individual or groups.
Users Managements	Limited	Available	in case of operational to monitor and managed system bluecoat has minim information while McAfee have more rounded view to observe and manage changes due to request or incidents

Figure 4 Summary of Risk Action conclusions

Based on our case study CNOOC SES Ltd decide to procure McAfee even though is not in leaders' quadrant by Gartner research, therefore others justification such as of Budget and the experience of managing web gateway previously is primary concern beside ability to solve the

Gap. By having proper evaluation and managing Web Gateway ICT Department can improve their services and Security level to support the business.

References

http://balancedscorecard.org/Resources/About-the-Balanced-Scorecard

http://www.networkworld.com/article/2992503/security/sans-20-critical-security-controls-you-need-to-add.html

http://whatis.techtarget.com/definition/cyber security

http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

https://www.nist.gov/cyberframework

http://www.isaca.org/About-ISACA/Press-room/News-Releases/2015/Pages/ISACA-Identifies-Five-Cyber-Risk-Trends-for-2016.aspx

http://www.iso.org/iso/home/standards.htm

http://www.iso.org/iso/home/standards/iso31000.htm

http://www.ldac.org.nz/assets/documents/1.-Defining-the-policy-objective.pdf

http://www.tanzania.go.tz/egov_uploads/documents/IT-Policy01_sw.pdf