Efficient Diagnostic Process for Technical Vulnerability

Miyang Cha

Abstract- With the development of IT came advances and expansions in major information and communications infrastructure, which have in turn resulted in studies being continuously conducted to analyze the administrative and physical vulnerabilities of the operating institutions. However, such institutions are exposed to the threat of cyber attacks because these studies often exclude technical aspects due to technological difficulty. Furthermore, web services limit their security checks to certain vendors and are therefore unable to identify the exact level of security in place. This paper demonstrates that these limitations, when performing a diagnostic test for technical vulnerability, can impact security levels. Therefore, this paper proposes a process that considers several environmental factors when checking for technical vulnerability in order to minimize the impact on security levels.

Keywords: technical vulnerability, security levels, environmental factors

I. INTRODUCTION

Recently, key infrastructure become a new target of cyberattacks as they shift from a closed environment to a more open one while also expanding their scope into cyberspace. The government does suggest a diagnostic checklist for analyzing and assessing the vulnerabilities of the information and communications infrastructure. However, there is no management of new vulnerable areas, while the level of vulnerability and cyber-attacks keep increasing as the system changes to be more open [1]. This is because the vulnerabilities are inevitably caused by connecting to external networks from to technological and environmental changes; using general purpose OS and applications for reduced costs and improved performance, as well as allowing portable electronics such as laptops and USBs to access the control system. In addition, there are standards in place for designating checks for the information and communications infrastructure. However, the scope of composition and characteristics differ per infrastructure sector such as administration, finance, and energy. Even so, most infrastructure undergo a vulnerability diagnostic check based on the same administrative/technical standard.

In today's IT environment that changes in real-time, over 75 percent of hacking incidents are reported as attacks on web servers [2]. The very nature of web servers makes them exposed to externalities, making them the target of most attacks.

If externalities, making them the target of most attacks. If corrective measures are not taken for the web server's vulnerabilities, this puts not only the server but also the users at risk. Thus, it is important to constantly reinforce the security of web servers[3].The checklist for server vulnerability for the information and communications infrastructure only includes Apache services from UNIX and IIS services from Windows. Since other web services are not checked, institutions that use WebtoB or Nginx are not subject to the diagnostics check. In addition, the web service checklist for the vulnerability of the information and communications infrastructure only checks certain vendors, which poses limitations in measuring the level of security.

New vulnerabilities and security issues have arisen over the years, but these have not been reflected in the vulnerability checklist nor settings of the information and communications infrastructure. In particular, from a technical viewpoint, there is a lack of preparation against, management of, and practical analysis of risks although they are becoming increasingly diversified [4]. As such, technical elements should be identified and applied following detailed standards set based on the impact that changes in the IT environment have on the control system, in order to ensure the systematic operation and management of technical elements.

This paper ran diagnostics for technical vulnerability for infrastructure in a real-world environment and saw differences in results, which can be considered as implying that such tests can have an enormous impact on the security level of the operating institutions. Therefore, this paper proposes a process in which risk management and technical diagnostic elements can be prepared in order to perform an objective and efficient vulnerability check that considers several environmental factors

II. RELATED STUDIES

2.1 Comparison of the Cybersecurity of Major Technological Infrastructure

As the scope of key infrastructure is expanded into the cyberspace, cybersecurity indicators are utilized to analyze their level of security. In general, standard checklists comprised of laws, regulations, operating organizations, public-private partnerships, detailed cyber-security plans, education, etc. are used to assess the nation's cyber-security. Assessment is

Revised Manuscript Received on July 22, 2019.

Miyang Cha, Professor, Department of General Education Namseoul University, 91, Daehak-ro, Seonghwan-eup, Seobuk-gu, Cheonan, Chungcheongnam-do, 31020, Republic of Korea

carried out for the criteria on a scale comprised of four stages ('Present', 'Absent', 'Partially present' and 'Not Applicable') [5][6].

Table 1 presents three international cyber-security indexes: The Global Cyber Security Index (GCI) of the International Telecommunication Union (ITU), the Cybersecurity dashboard (CSD) of the Business Software Alliance (BSA), and the Cybersecurity Maturity in the APAC region (CSM) of the Australian Strategic Policy Institute (ASPI). These indexes were selected among the many currently in use to measure cybersecurity levels internationally, based on the existence of quantitative results that are scored or ranked, and the existence of specific assessment criteria.

Table 1: Cybersecurity International Index

Agency	ITU	BSA	ASPI
Index Name	GCI	CSD	CSM
Publication Year	2015	2015	2012
Target (members)	193state	EU 28 /APAC 10	APAC 16
Score/ Rank	Score/ Rank	Score	Score
Criteria/ specific	5/17	5 / 25	5 / 11
Evaluation Standard	Average	4 point scale &Sum.	Weighted

2.2 Checking Server Security Vulnerability

The criteria for checking the vulnerability of UNIX servers are account management, file and directory management, service management, patch management, and log management, while that of Windows servers are account management, service management, patch management, log management, security management, and DB management [7][8]. Account management in UNIX servers consists of criteria such as setting account lock thresholds, setting passwords, and removing unnecessary accounts. The file and directory management consist of checking criteria such as settings for file ownership and permission, world writable files, accessible IPs, and port restrictions. Service management consists of criteria such as checking for unnecessary services (e.g. finger services) and those related to Apache services. Patch management consists of criteria that apply the latest security patches. Log management consists of criteria such as regular log reviews and reports [1][8].

For Windows servers, account management consists of criteria such as renaming administrator accounts, setting passwords, and removing unnecessary accounts. Service management consists of criteria such as removal of basic hard disk sharing and unnecessary services, as well as inspection of IIS services. Patch management consists of criteria such as applying the latest patches and antivirus program patches. Log management consists of criteria such as regular log reviews and reports, as well as event log management settings. Security management consists of checking criteria such as the existence of antivirus programs, screen-saver settings, Windows security policy settings, and settings for unnecessary programs at startup. DB management consists of Windows authentication mode settings [1][8].

2.3 Market Share of Web Servers

All websites are based on computing devices called web servers. These servers are always connected to the Internet. There are various vendors for web servers such as Apache, IIS, Nginx, Lighttpd, and Jigsaw. Table 2 shows web servers with the world's top market share [9].

Table 2:Market Share of Web Servers

Product	Vendor	10/ 2016	12/ 2017	12/ 2018	01/2019
Apache	Apache	23.84%	30.9%	18.94%	21.30%
IIS	Microsoft	44.61%	25.7%	41.53%	31.96%
Nginx	NGINX	13.77%	22.8%	21.63%	24.74%
GWS	Google	1.51%	1.2%	1.44%	1.58%

The most popular web servers are Apache and IIS. However, there are many other web servers and recent reports indicate that Nginx is quickly increasing its market share. This means that one needs to consider the functional characteristics of the web servers based on the needs of the market, and that existing checklists for web server vulnerability is insufficient in checking for technical vulnerability in the information and communications infrastructure. Therefore, a basis should be established that reflects the market environment.

2.4. Implications

Checklists for major information and communications infrastructure server vulnerability only cover Apache and IIS services, meaning no other web services are being inspected. That is, if the institution uses WebtoB or Nginx, diagnostics will not be performed. Web services that only check certain vendors will be limited in measuring the exact level of security.

Therefore, for an objective check for vulnerability, diagnostics should be run for each information system type in order to eliminate the diverse risk factors. In other words, following the changes in the IT environment, it is necessary to develop intrusion responses and technical security elements in the latest technology areas such as Big Data, Clouds, mobile, smart grid and so on in order to strengthen the level of security of the information and communications infrastructure.

III. PROPOSED PROCESS

3.1 Conceptual Diagram Outlining the Diagnostics Process for Effectively Testing Technical Vulnerability

A variety of environmental factors should be reviewed and addressed in order to efficiently analyze and respond to recurring vulnerabilities. In addition, a database should be created and regularly updated with the analyzed vulnerabilities and a vulnerability test should be periodically run based on the identified factors. Figure 1 illustrates the process in which risk management and technical diagnostic elements can be prepared to perform an objective and efficient test for vulnerability in

which various environmental factors are considered.

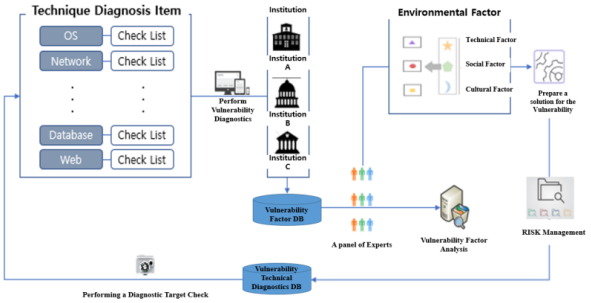

Figure 1: Conceptual diagram outlining the process for efficiently testing technical vulnerability

Based on the current list of vulnerabilities in operation, the institution carrying out the diagnostics can test the vulnerabilities present in the information and communications infrastructure. The vulnerability of each infrastructure will then be collected and stored in the database. The stored information should be analyzed by experts to identify patterns within repeated vulnerabilities. In other words, by dividing according to OS/Device/APP, it is possible to isolate and collect vulnerabilities periodically occurring within those categories. Experts should be consulted and efforts should be made create ways to resolve the vulnerability issues. Therefore, environmental factors should be reviewed based on the analyzed vulnerability and should be tested whether they can be resolved with technology/policies. In other words, measures and solutions (such as updates and replacement solutions) that can overcome periodically occurring vulnerabilities in the operating systems should be prepared. For risk management, a technical vulnerability diagnostic DB should be managed that reflect risks, and technical vulnerability diagnostics should be run.

3.2. Conceptual Diagram for Risk Management

Risk management is a collaborative tool that reduces cybersecurity risks based on technical vulnerabilities diagnostics. It prioritizes risk management by taking environmental factors, relevant regulations, and best practices into account. As shown in Figure 2, by comparing the Current Profile with the Target Profile, it is possible to identify the gap that needs to be addressed in order to achieve the goal of cybersecurity risk management.

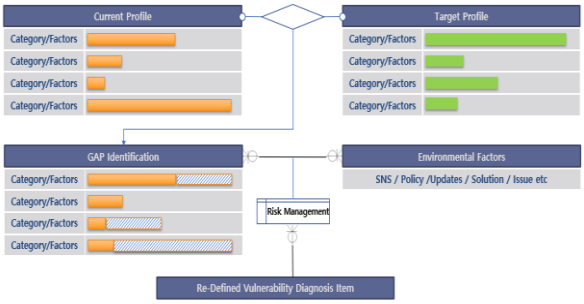

Figure 2: Conceptual diagram for risk management

Defining the relationship between the gap and environmental factors (social media, policies, updates, solutions, etc.) enables a realistic redefining of the Target Profile. While the Current Profile shows the diagnostic results of the technical vulnerability diagnostic elements currently in operation, the Target Profile represents the elements necessary to minimize risk management in each infrastructure. It is necessary to identify the differences (the gap) in order to achieve the risk management goals, and by reflecting the environmental factors (categories, subcategories, industry standards, best practices, risk acceptance, and organizational resources) in the goals, it will be possible to identify the appropriate technical vulnerability diagnostic elements for each infrastructure as well as reprioritize the measures that need to be implemented.

3.3. Conceptual Diagram of the Process for Extracting Common Diagnostic Criteria

Since institutions use web services that are well suited to the characteristics of the infrastructure, they need to understand the functions and characteristics of the web servers being used. However, most institutions only consider the resulting service and not the security issues when installing servers. Despite new vulnerabilities and security issues arising over the years, existing vulnerability checklists for IT infrastructure have not been updated with the latest risks nor settings, and are thereby unable to prepare against new threats in this rapidly changing environment [10]. This can cause issues such as directory indexing, where the file information stored in a can be exposed via incorrect security settings; information leakage, where information about which web server or version is being used is exposed; and location exposure, where information about location is exposed due to unnecessary files. As such, it is important to check the security settings and related criteria relevant to web services.

Figure 3 presents a conceptual diagram of the process for extracting common and characteristic items based on a vulnerability checklist that takes the functions and characteristics of each web server into consideration.

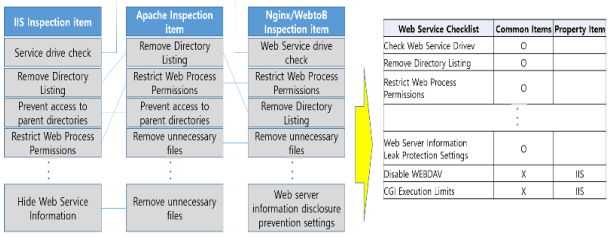

Figure 3: Conceptual diagram of the process for extracting common checking items

Directory listing removal is common to all web servers, while the service run check is only applicable to certain web servers. In addition, it can be considered whether web server exposure prevention setting functions can be matched with other similar items (hiding web service information, separating web service areas). Through this process, it is possible to extract common items that take the functions and characteristics of all web servers into account. A checklist can be prepared that allows users to select additional criteria that reflects the unique

functions and characteristics of the web server.

IV. COMPARISON OF WEB SERVICE VULNERABILITY CHECKLISTS

This study carried out a technical vulnerability diagnostics of two infrastructures (Institution A and Institution B) with two conditions (existing items and improvement items) in a real-world environment. Institution A uses the Apache Web Server while Institution B uses Nginx Web Server. The existing criteria were based on an existing checklist of technical vulnerabilities, while the improved criteria were based on a list reflecting the functions and characteristics of the web servers operated by the institutions. Table 3 presents the results of a technical vulnerabilities check of the two institutions in a real-world web service environment by applying the existing and improved checklist.

Table 3 : Results of the Web Service Vulnerability Check(Institution)

Criteria Classification : Service Management	Application of Existing Criteria		Application of New Criteria	
Checklist	A	B	A	B
Finger service deactivation	Good	Good	Good	Good
Anonymous FTP deactivation	Good	Good	Good	Good
r-affiliated service deactivation	Good	Good	Good	Good
Cron file owner and permission settings	Good	Good	Good	Good
Deactivation of services vulnerable to Dos attacks	Good	Good	Good	Good
NFS service deactivation	Good	Good	Good	Good
NFS access control	Good	Good	Good	Good
automountd removal	Good	Good	Good	Good
RPC service check	Good	Good	Good	Good
NIS, NIS + Check	Good	Good	Good	Good
tftp, talk service deactivation	Good	Good	Good	Good
Sendmail version check	Good	Good	Good	Good
Spam mail relay restriction	Good	Good	Good	Good
User-run Sendmail restriction	Good	Good	Good	Good
DNS security version patch	Good	Good	Good	Good
DNS Zone Transfer settings	Good	Good	Good	Good
Web service drive check			Good	Good
Directory listing removal			Good	Good
Web process permission restriction			Bad	Bad
Unnecessary file removal			Bad	Bad
Link usage restriction			Bad	Bad
Web server information leak prevention settings			Good	Good
Hide web service information			Good	Good
Web service area separation			Good	Good
Upper directory access restriction			Good	N/A
File upload and download restriction			Good	N/A
Logging directory and file permission control			Bad	Bad
Security patch application			Bad	Bad
directory listing removal for Apache	Good	N/A	Good	N/A
Web process permission restriction for Apache	Bad	N/A	Bad	N/A
Upper directory access restriction for Apache	Good	N/A	Good	N/A
Unnecessary file removal for Apache	Bad	N/A	Bad	N/A
Link usage restriction for Apache	Bad	N/A	Bad	N/A
File upload and download restriction for Apache	Good	N/A	Good	N/A
Web service area separation for Apache	Good	N/A	Good	N/A
Allow ssh remote access	Good	Good	Good	Good
ftp service check	Bad	Bad	Bad	Bad
ftp account shell restriction	Bad	Bad	Bad	Bad
Ftp users file owner and permission settings	Bad	Bad	Bad	Bad
Ftp users file settings	Bad	Bad	Bad	Bad
at file owner and permission settings	Good	Good	Good	Good
SNMP service run check	Good	Good	Good	Good
SNMP service community string complexity settings	Good	Good	Good	Good
Warning message upon log-in	Good	Good	Good	Good
NFS setting file access permission	Good	Good	Good	Good
extn, vrfy command restriction	Good	Good	Good	Good
Hide Apache web service information	Good	N/A	Good	N/A
Vulnerability Score	81.9	88.4	78.2	76.9

Existing web service vulnerability diagnostic standards are comprised of criteria that only covers Apache and IIS, and as such are unusable for checking other web services. Thus, Institution B had a higher security level than Institution A. However, Institution A had the higher level of security when applying the improved checklist. These differing results were because the web service checklist reflected the functions and characteristics of Nginx, the web server used by Institution B, which resulted in higher accuracy measuring Institution B's level of security. The tests show the differences in diagnostic results, which can be considered as implying that such tests can have an enormous impact on the security level of the operating institutions. This indicates that entries for new security vulnerabilities should be added to the checklist when they occur. Therefore, risk management and technical diagnostic elements should be prepared that can perform objective and efficient vulnerability diagnostic tests that takes various environmental factors into consideration.

V. CONCLUSION

Protection measures currently in use for key infrastructure remain the way they had been established in the past, and as such fail to respond to new threats caused by the rapid changes in the IT environment and the expansion of social and cultural issues. To counter these threats, studies have been continuously conducted that suggest analysis and assessment criteria for the administrative and physical vulnerability specific to operating institutions. However, these studies have neglected technological vulnerability due to difficulties in objective verification of methodology as well as limited technical skills. Therefore, relevant information (status, vulnerability, etc.) should be collected and managed, technical updates should be made, and collaboration with partners should be carried out periodically to actively respond to changes in the times and the environment.

Currently, vulnerability checklists for the information and communications infrastructure are unable to accurately measuring security levels as only certain vendors are checked in the case of web services. Generally speaking, different threats exist for different types of information systems when checking for vulnerability. As such, diagnostics should be performed by dividing areas by type to eliminate threats. Through checking web server-related vulnerabilities, this paper confirmed that

improvements should be made to reflect various web services vendors in vulnerability checklists are necessary. Thus, it is more important to create and expand diagnostic items on a regular basis than to periodically run diagnostics in order to actively respond to newly discovered vulnerabilities. In addition, it is necessary to cooperate with experts to analyze vulnerable areas and environmental factors so that this can be reflected in the collected information, as well as to manage the risk in vulnerable elements.

In the future, research and reviews of confidence index measures that can overcome the vulnerabilities collected in technological environments that can reflect value in the real world (e.g. new ICT technology, mobile technology, etc.) should be made.

Conflict of Interest

The authors declare no conflict of interest.

ACKNOWLEDGMENT

Funding for this paper was provided by Namseoul University

ACKNOWLEDGMENT

It is optional. The preferred spelling of the word “acknowledgment” in American English is without an “e” after the “g.” Use the singular heading even if you have many acknowledgments. Avoid expressions such as “One of us (S.B.A.) would like to thank ... .” Instead, write “F. A. Author thanks ” *Sponsor and financial support acknowledgments are placed in the unnumbered footnote on the first page.*

REFERENCES

1. Seon-Jin, Kim, Improvement in Vulnerability Diagnostic Items and Methods for Server Security: Graduate School of Information Science, Soongsil University; 2017. 28p
2. Korea Internet and Security Agency, 2016 Cyber Threat Trend Report; 2016.19p
3. Hyung-Soo, Lee, A Study on SCCN Technology to Enhance Web Service Security: Soongsil University, 2017.33p
4. I-news(2016.12.22.), Urgency of Social Infrastructure Security Management from:http://news.inews24.com/php/news_view.php?g_serial=997828&g_menu=020200
5. BSA, from:EUCybersecurity Dashboard; 2015
6. BSA, from:APACCybersecurity Dashboard; 2015
7. Tae-Ho, Kim, A Study on Improving Checklists for Infrastructure Vulnerability: Graduate School of Information and Communications, Konkuk University; 2016.42p.
8. Ministry of Public Administration and Security, Korea Internet and Security Agency, Detailed Guide for the Analysis and Assessment of Technical Vulnerabilities in Major Information and Communications Infrastructure; 2014. 63p.
9. From: https://news.netcraft.com/
10. Young-Kyu, Lee, A Study on Improving Checklists for the Administrative and Physical Vulnerabilities in Major Information and Communications Infrastructure: Graduate School of Information and communications, Konkuk University; 2017. 68p

VI. AUTHORS PROFILE

The author received a Bachelor’s degree in System Biology at Yonsei University in Korea, a Master’s degree in TESOL at the University of Malaya in Malaysia, and a Ph.D in English Linguistics from Jawaharlal University in India. She has been teaching at the College of General Education, Namseoul University in Korea since 2002. Her areas of research include, but are not limited to, English education, IT-applied engineering, and small and medium-sized business (SMB). Her interest in diverse fields have resulted in recent publications such as: ‘The Effects of Overseas Internships on Development of English Competence (2019)’, ‘Pattern Analysis of Risk Situations Using Multi-Sensor (2018)’, ‘An Analysis of Customized Personal Health Information for Smart Healthcare Systems (2017)’, ‘Enhancement of SMB Global Compentency for Overseas Market Entry (2017)’. She is currently involved in several academic associations such as Convergence Society of SMB, The Korean Association of English for Specific Purposes, and The English Teachers Association in Korea.