International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Initial Study of Cyber Security for Web Services in Malaysian Organizations

Firkhan Ali bin Hamid Ali[1]*, M. Khairul Amin M. Sukri[2], M. Azahari M. Yusof[3], Mohd Zalisham Jali[4], Moh Norazmi Nordin[5], Miswan Surip[6]

Submitted: 15/02/2023 **Revised:** 19/04/2023 **Accepted:** 10/05/2023

Abstract: In the recent and next years, Malaysian enterprises have seen an increase in the development of information technology (IT). This is a result of the Malaysian government actively promoting IT usage throughout all companies in Malaysia, whether they are in the public or private sectors. Utilizing IT including web services will increase an organization's production and quality. Therefore, they require a well-planned implementation of the IT infrastructure and tools. Using web services will ensure that its operations are successful in supporting long-term business ambitions. Besides that, the cyber security play important role to ensure that the web services and IT infrastructures execute well along the organization's business successful. So, is these digital environments in Malaysian organizations safe it is not a Malaysian IT culture and didn't have enough and tough knowledge of cyber security. However, how to promote cyber security to Malaysian organizations for web services? So, promotion can be done by using the web services itself by putting more knowledge and study on the secure usage of IT facilities in Malaysian organizations.

Keywords: *Cyber security, information Technology, Malaysia, web services*

1. Introduction

Many firms in Malaysia have used IT facilities including web services to conduct their operations in an efficient and effective manner in order to support high-quality production. In the study, the topic of cyber security in web service usage will be covered. Many Malaysian enterprises do not place a great deal of importance on concerns related to cyber-environment security. Because there are numerous web services in IT facilities, this topic occurs in a digital world. The Malaysian populace was now familiar with IT.

Governments and the corporate sector had hardly ever used incentives like parties, contests, or advertisements to promote IT technology including web services. They encouraged programming, networking, online applications, multimedia technologies, and other related fields of IT technology, but they abandoned or only partially addressed the issue of cyber security.

Information and communication technology, or ICT refers to all the tools and parts used in the digital world for communication, including software, hardware, systems, databases, networks, the Internet, and other related items.

By employing IT infrastructure and communications, we can use cyber security to secure our digital environment from dangers including disasters, system failures, and illegal access that could cause harm or financial loss especially use of web services [1].

2. Threats to The Web Services

There are numerous reasons that can deactivate or negatively affect how web services are used in Malaysian organizations. The organizations' output will decrease [2]. All of these elements could be caused by one of these agents, which include people, processes, software mistakes, applications, electromechanical issues, unclean data, hardware, and communication components, whether directly or indirectly.

In addition, terrorism, social unrest, and natural disasters can all pose a threat. Additionally, it may occur in situations that are directly or indirectly related. Therefore, it would be simpler for us to ensure that the cyber security in Malaysian firms is secure if we first understand all of these risks [3].

2.1 Errors and accident in Web Services

These risks arise from a variety of sources, including human mistake, improper procedure, software malfunction, electromechanical issues, and dirty data

1,2,3 Department of Information Security & Web Technology, Fakulti Sains Komputer & Teknologi Maklumat, Universiti Tun Hussein Onn Malaysia, 86400 Parit Raja, Johor, Malaysia
4Faculty of Science & Technology, Universiti Sains Islam Malaysia, Nilai, Malaysia
5Faculty of Education, Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia
6Pusat Pengajian Diploma, Universiti Tun Hussein Onn Malaysia, 86400 Parit Raja, Johor, Malaysia

issues. Example, they didn't use the rule to use the devices properly such as using of printers [4].

2.2 Natural and other hazards in Web Services

Some of these threats can potentially bring all systems or web services completely and permanently offline. Natural hazards include events like fire, flood, earthquake, tornadoes, and others that are connected. All of the systems will be broken or severely damaged. In other hazards, it occurs in specific circumstances like civil unrest or terrorism.

2.3 Crimes Against the Web Services

This type of threat concerns an illegal act committed against web services. Theft of the hardware, software, computer time, cables, telephone services, or unlawful information acquisition are just a few of the ways this danger to web services might manifest itself.

2.4 Crimes Using the Web Services

Prior to then, it had been addressed how crimes affect web service facilities; now, it has been discussed how crimes take place with the aid of web service facilities. For instance, a clerk in a Malaysian financial institution used the system to claim several cents from every customer's account and deposit them into its own account.

2.5 Malware

This type of high-tech wick nesses exists. It is software or computer programs that can slow down or completely destroy computers, systems, or other IT facilities. It also spreads to other IT facilities that have interacted with it.

2.6 Computer criminals

The categories of people participating in these web service's threat are discussed. Persons in the organization, such as employees, and people outside the business, such as suppliers, customers, hackers, crackers, and professional criminals, can be categorized as those types [5]. They might sell the data or steal the equipment, or they might utilize the organization's IT resources dishonestly for their own financial gain [6]. The persons who can gain unauthorized access to the company's IT infrastructure, however, are the hackers and crackers, who are typically considered to be outsiders [7].

Due to the advancement of more knowledgeable users who are exploiting their capacity for illegal access and the creation of several programs that can compromise any organization's cyber security, all of this threat to web services has grown more significant for all enterprises. By virtue of this issue, every organization must be in charge of and protect its IT infrastructures, which will be discussed in more detail in the following section.

3. Cyber Security Malaysia

Cyber Security Malaysia, also known as Malaysia Computer Emergency Response Team (MyCERT), is a government organisation in Malaysia that is in charge of handling any difficulties and solving any problems relating to digital security [8]. It was established on January 13, 1997, and by March 1, 1997, it was completely operational.

Cyber Security Malaysia has given the Malaysian Internet and computer community a point of reference for dealing with computer security incidents and providing prevention techniques. Examples of incident statistics supplied by Cyber Security Malaysia for the year 2019 are shown in Figure 1. Cyber Security Malaysia classified the different incident types as follows: intrusion, destruction, denial of service, virus and hacker threat, forgery and harassment, spam, and mail bomb. According to the reports they got from all-Malaysian groups, this statistic was presented [9].

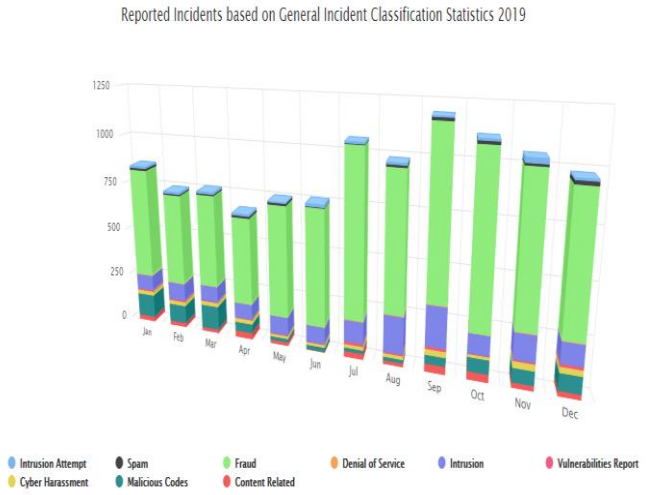

Fig. 1. Incidents statistics 2019

4. Cyber Security Control for Web Services

Every Malaysian organization needs controls in their structure to guarantee the reliability and security of all IT resources, such as information systems, hardware, software, networks, web services and data. Controls are required to avoid computer-based system errors, unauthorised use of IT, and purposeful or unintentional destruction of data and software.

The accuracy, integrity, and safety of IT activities including web services and resources will grow if control is successfully given to the organization's, IT components because of their capacity to reduce errors, fraud, and network environment damage in that Malaysian organisation. Additionally, it would guarantee the quality of IT facilities and lessen any potential harm to Malaysian organization and business strategies.

Any organisation in Malaysia that wants to successfully use IT especially in web services must build three key types of controls: IT, procedural, and facilities control.

5. Security Auditing for Web Services

The internal auditing team from the business division must frequently review or audit the IT department of organisations in Malaysia. Periodic audits conducted by external auditors from a reputable accounting firm can serve as an additional audit. That is a wise organisational approach. Auditing should examine and assess if managerial controls that were engaged in their development and implementation, such as IT controls, procedural controls, facility controls, and other aspects, are proper and adequate.

Malaysian organisation may conduct an IT audit in one of two methods. There are two types of auditing: auditing through the computer and auditing surrounding the computer. Since all IT facilities depend on computers, whether indirectly or not, they are being used as the auditing subject.

It will evaluate the precision and reliability of computer systems, Its facilities and web services. Additionally, the input and output of the IT systems will be examined. It necessitates understanding of network administration, software development, and data flows in web services and IT systems. For some computer systems or applications, this auditing can be expensive.

Testing the accuracy of an application audit trail is the most crucial step in this auditing process. The presence of documentation that enables a transaction to be tracked through all phases of its information processing is known as an audit trail.

6. Safeguarding of Web Services and IT Facilities

With web services and IT, cyber security must be vigilant. Concerns include identification and access, encryption, software and data protection, and disaster recovery planning. These four areas might be seen as separate concerns.

Anybody can access the Internet anywhere today. Anyone's name and email address can be quickly found using this tool. After that, it can determine if those folks are working online while at the office and where exactly they really logged on to the computer. In order to protect IT from disasters, system failures, and illegal access that could cause damage or loss, security is a system of defences.

Numerous components make up security safeguards in cyber security. This includes identification and access, encryption, protection of software, firewall, network security and data and disaster recovery plan.

We can employ this thing for our protection based on who you are because, in most cases, only we are well-known for ourselves [10]. Similar to your physical character, it is difficult to spoof this type of identity. The science of measuring an individual's physical traits is known as biometrics. Therefore, security devices are using this knowledge in accordance with its features.

A camera automatically compares a student's hand's shape to a picture of the same hand taken from an ID card's magnetic strip. The cafeteria turnstile automatically clicks open if the pattern matches. If not, they would move on to mooch off of someone else [11].

The most popular encryption technique makes use of a set of public and private keys that are personal to each user, similar to PGP [12]. As an illustration, emails might be encrypted and scrambled using a recipient-specific public key that is known only to the sender. Only the recipient's secret private key could decrypt the email after it was sent.

Network Security Monitoring Systems, a class of specialised software or systems, are frequently used to offer this network security. These applications are used to keep an eye on how the computer systems, networks, or IT facilities are being utilised and to safeguard against unauthorised access, fraud, and destruction [13]. The control of access, audit control, and personnel control are all part of the security technique for protecting data and software [14].

By acting as a filter and secure transfer point for access to and from the Internet and networks, a network firewall protects an organization's IT facilities on the network from infiltration [15]. It can effectively discourage but not entirely stop illegal access to computer networks. Therefore, it occasionally might restrict access to its

systems to those coming from reliable Internet sources and might only permit secure information to pass [16].

A disaster recovery plan is a method or system for recovering data about an operation's workflow following damage or an accident. Its strategy entails conducting a significant fire exercise. It contains a list of the relevant technology, software, data, business functions, people who support those functions, and alternative locations [17].

7. Discussion

According to data provided by Cyber Security Malaysia, Malaysian organizations are now dealing with a lot of problems with cyber security. The utilisation of the IT facility including web services will be damaged, slowed down, or rendered useless. This will have an impact on the organization's production quality and volume, failing business plan.

Threats from their activity are theoretically and technically known. After that, the company may create a solid plan for implementing digital security. The goal is to protect all IT facilities from threats by using specific hardware, software, IT infrastructure, policies, and other associated controls [18].

There are currently far too many IT resources and tools available to assist an organization with cyber security [19]. These IT resources and technology have always undergone updates, adjustments, and growth, just like threats. Therefore, Malaysian organisations must constantly be aware of and act upon any updates to IT facilities and technologies in accordance with cyber security.

Otherwise, auditing the IT facilities is the last thing that is crucial after the firm has provided the IT facilities and technologies are to overcome the dangers against the organisation. It is crucial to make sure that the organization's use of IT facilities, particularly with regard to digital security, is efficient, functional, and ready for use [20].

In the global digital world, are Malaysian organisations secure? That company alone will have the solution to your query. The participation of top management and the organization's readiness to combat threats using current and appropriate IT facilities, technology, and policies are the most crucial factors. Through Cyber Security Malaysia, other clever people are sharing information about problems with digital security among all Malaysian organisations [21].

8. Conclusions

The study covered various vulnerabilities to organisational cyber security as well as how these threats were created via IT resources and web services. One government agency in Malaysia, Cyber Security Malaysia, hid this issue.

With reference to Malaysia's cyber security, Cyber Security Malaysia served a purpose. It will take any information about problems with cyber security and strive to fix them. It has also been highlighted how Malaysian organisations might use IT resources and technologies to prevent these hazards in the web services.

The organisations' ability to control and audit their IT facilities is one of the most crucial factors. It will help shield Malaysian organisations from any dangers. Finally, the utilisation of IT facilities and web services in Malaysia enjoys good budgetary backing from the top management of organizations. Therefore, it might be done to integrate cyber security in an organisation to make the use of IT facilities safe, accessible, and effective.

Acknowledgement

This research was supported by Universiti Tun Hussein Onn Malaysia (UTHM) through TIER 1 (vot Q152)

References

[1] Definition for Common Security Terms, http://www.mycert.org.my/html [1 MARCH 2020]

[2] Davis, G.B. and Olson, M.H. (1985) Management Information System: Conceptual Foundations, Structure and Development (2nd edn), McGraw-Hill.

[3] Firkhan Ali, H. A., Maziah Na'aman, "Vulnerability Assessment on the Network Security" in NCSTIE 2006: *Proceedings of the International Conference on Science and Technology 2006*. PWTC, UiTM Pulau Pinang.

[4] Galliers, R. and Sutherland (1991) Information System Management and Strategy Formulation: The 'Stages of Growth' Model Revisited, *Journal of Information Systems*, Vol 1 No 2 pp. 89-114.

[5] Firkhan Ali, H. A etl. , "Development Of Dual-Factor Authentication For Web Based Application Using SMS", *Proceedings of the ICITS 2008*, Kusadasi, Turkey, 2008.

[6] Firkhan Ali, H. A etl., "Development of Vulnerability and Security Reporting System for Computer System and Networking" in SITIA 2008*: Proceedings of the Seminar In The Intelligent Applications 2008*, Surabaya, Indonesia, 2008.

[7] Guomin Yang, Duncan S. Wong, Huaxiong Wang dan Xiaotie Deng (2006). "*Formal Analysis and Systematic Construction of Two-factor Authentication Scheme*." City University of Hong Kong, China.

[8] MyCERT About Us', http://www.mycert.org.my/html [1 MARCH 2020]

[9] Incident Statistic (2017-2019), http://www.mycert.org.my/html [1 MARCH 2020]

[10] Wendy, R. (1997) *Strategic Management and Information Systems* (2nd edn), Prentice Hall.

[11] Lederer, A.L and Gardiner, V. (1992) The Process of Strategic Information System Planning, *Journal of Strategic Information System Planning*, Vol 1No 2 Mar pp. 76-83

[12] Hatch, B., Lee, J. and Kurtz G. (2001) *Hacking Linux Exposed: Linux Security and Solutions*, Osborne/McGraw-Hill.

[13] Scambray, J., Mcclure, S. and Kurtz G. (2001) *Hacking Exposed: Network Security and Solutions*, Osborne/McGraw-Hill.

[14] Richard A. Kemmerer et al., (2002), *Intrusion Detection: A Brief History and Overview*, *SECURITY & PRIVACY–2002*, Reliable Software Group, Computer Science Department, University of California Santa Barbara.

[15] Norton, P and Stockman, M. (1999) *Peter Norton's Network Security Fundamentals*, SAMS Publishing.

[16] Wenke Lee et al., (2000), A Framework for Constructing Features and Models for Intrusion Detection Systems, *ACM Transactions on Information and System Security* (TISSEC), Volume 3 Issue 4, ACM Press.

[17] Williams, B.K., Sawyer, S.C. and Hutchinson, S.E. (1995) *Using Information technology*, Richard D. Irwin, Inc.

[18] Ward, J. and Griffiths, P. (1996) *Strategic Planning for Information Systems* (2nd edn), Wiley.

[19] Zacker, C. (2001) *Networking: The Complete Reference*, Osborne/McGraw-Hill.

[20] Tipton, H.F. and Krause, M. (2000) *Information Security Management Handbook (4th Edition*), Auerbach Publications.

[21] Security FAQs', http://www.mycert.org.my/html [1 MARCH 2020]