Securing Nigeria's Ivory Towers from Cyber Attacks

Clement Amone Keyamo
Department of Cyber Security
Dennis Osadebay University,
Anwai,Asaba, Nigeria
Clement.keyamo@dou.edu.ng

Dr. Ejeh Patrrick Ogholuwarami
Department of Computer Science
Dennis Osadebay University,
Anwai,Asaba, Nigeria
Patrick.Ejeh@dou.edu.ng

DOI: 10.56201/ijcsmt.v9.no1.2023.pg52.58

Abstract
Nigerian Universities have been reported to be lackadaisical concerning Cyber security which may account for the rising attacks on their IT infrastructure by Cyber criminals. This paper aims to provide information that can enlighten the University stakeholders on the threats to their IT infrastructure and how to secure them. The paper concludes that There is a need for the institution to be proactive in combating the threats posed by Cybercriminals and that it should take advantage of Cyber insurance coverage available to ameliorate potential attacks.

Keywords: Cybercrime, Cybersecurity, Countermeasures, IT Security, computer Security.

1. Introduction

The increasing use of computerized systems in universities for learning, administration, and other activities, has exposed them to Cyber attacks and associated challenges. The educational sector in Nigeria is vulnerable to Cyber attacks as most universities are not proactive in securing their IT infrastructures. The above is due, in most cases, to ignorance (Olayede, Guardian,31 May 2021; Sodiya et al., 2011),

Paul (2020) states that Nigerian Universities appear not to care about the weaknesses in their information Technology systems. For instance, bugs discovered in some Nigerian University sites in 2017 have not been removed as of 2020. Ahmadu Bello University, Zaria, and the University of Benin are examples of universities that have been identified with vulnerabilities that are not being handled.

The aforesaid lackadaisical attitude may account for attacks on some Nigerian university sites over the years. For instance, Sodiya et al., (2011) discovered that 86% of academics in southwestern Nigerian universities experienced breaches in their research data. In addition, Paul

(2020) claimed that thousands of users had their personal information stolen from the ABU website. In light of the above, Nigerian universities must improve the security of their IT infrastructure.

This paper aims to enlighten University stakeholders on Cyber security issues that concern them, identify IT security Vulnerabilities/Risks/threats/attacks, and proffer countermeasures.

2. Vulnerabilities in IT Infrastructure in Universities in Nigeria

According to Sodiya et al (2011), a vulnerability is a weakness in a computer system that makes it susceptible to a Cyberattack. The probability that the weakness would be exploited is a Risk, while a Threat is any entity that can take advantage of a weakness to cause Damage.

Furthermore, Binuyo (2019) defines Vulnerabilities as "weaknesses in a system or its design that allows an intruder to execute commands, access unauthorized data, and/or conduct denial-of-service attacks".

There is a high level of vulnerability in most Nigerian university IT infrastructure (Paul, 2020; Badamasi, 2018; Sodiya et al., 2011,) that poses an attraction to Cyber criminals that may be part of a large number of users of the IT infrastructure.

Sterbenz et al., (2010) and Badamasi, (2018) agree that universities have a high volume of people who make use of their IT infrastructure and thus, this makes it difficult to detect and respond to incidents. Badamasi (2018) identifies the admission page and accommodation pages of the registration portal of the IT system as often vulnerable to attacks. Insider-created back-doors can be used to give unauthorized access to users to defraud the university. Admissions and hostel rooms can be allocated to students illegally using these backdoors. Many students can be defrauded by these insiders.

Also, evil twin sites have been known to be created by Cyber criminals that lure unsuspecting individuals to pay fees that do not get to the universities the sites mimic (Badamasi, 2018).

3. Common Cyber attacks on university's IT infrastructures in Nigeria

Some researchers have identified the attacks common to IT infrastructures in general. However, Badamasi (2018) and Binuyi(2019) enumerate some of the Cyber attacks commonly perpetuated against university infrastructures to include the following:

Social Engineering Attacks: This kind of attack involves manipulating people, or in some cases, intimidating them to perform actions or leak information criminals used to attack a system. The purpose of this is to gather relevant information about a network to compromise it ;

Phishing attacks: A phishing attack involves Cyber criminals creating a fake website and then using manipulation and other means to attract unsuspecting victims to those sites to defraud them.

Password Sniffing: this involves the use of a sniffing tool like Wireshark and NMAP to access network traffic and collect passwords and other information that can be used to penetrate the school system;

Denial-of-Service (DoS) Attacks: These attacks often cause users of the university systems to be denied system resources. These attacks often occur when attackers make illegal use of system resources.

Malware attacks: malware or malicious software is a computer program that is harmful to a computer system. Examples of malware are Viruses, ransomware, worms, Trojan horses, and spyware. Malware is used by attackers to steal data, encrypt or delete sensitive data, hijack computing services, and for monitoring users' computer activity without their permission.
Pharming Attacks: this kind of attack targets admission seekers. Victims are lured to websites owned by Cybercriminals and extorted under pretenses. Vulnerabilities in Domain Naming Systems (DNS) are often exploited to perpetuate this attack.

Website Defacement Attacks: The attacker changes the visual appearance of the site or a web page. The cybercriminal adds extra content to genuine websites that serve as bait to lure unsuspecting students to a rogue site, where they defraud them.

Port Scan Attacks: in this kind of attack, the attacker uses a scanning tool to scan a network to detect open and vulnerable ports that may be used to attack the system. Open ports may be used to infect the system with a virus or institute a denial-of-service attack.

4. Cyber attack control measures and Mitigation in Universities in Nigeria
According to Badamasi (2018), Cyber attacks may be checked if appropriate measures are in place.

Binuyo(2019), identified physical security, authentication, authorization, accounting (auditing), encryption, and firewall as Cyber security mechanisms that may be implemented to control and manage Cyber-attacks. Badamasi (2018), closely aligning with Binuyo(2019), classified them into security measures and security tools as defined below:

I. Common Security Baselines: According to Badamasi(2018), the basic set of security objectives of any given service or system, is the security baseline. As an example, patch management (that includes deciding on the relevant patches for systems and making sure the patches are installed) is one of the objectives in security baselines. Also, Vulnerability Assessments and Penetration Testing are security objectives in a university's IT infrastructures.
Penetration Testing can be viewed as the simulation of attacks against the university system and network to determine weaknesses that may be exploited and thus take proactive measures to repair the loopholes (Binuyo, 2019). Common Penetration Testing tools used by the University System are Metasploit and NMAP. Vulnerability Assessment and Penetration Testing results are useful in the protection of IT infrastructures from high-profile attacks such as sabotage, espionage, and malware infection.

Figures 1 and 2 illustrate typical Vulnerability Assessment and Penetrating Testing Procedures

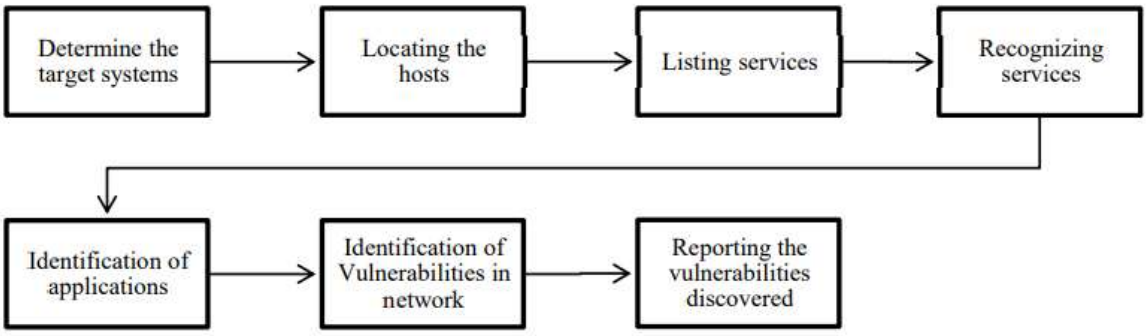

Figure 1: vulnerability assessment steps (source: Badamasi (2019)

Figure 2:Penetration Testing steps (source:https://www.123rf.com/)

The Incident Response: This is another security measure identified by Badamasi, (2018) and Binuyo (2019). Incident response is concerned with the premeditated plan put in place as a response plan when a specific Cyber-attack occurs. How quickly a university can detect and responds to an attack and what plans are in place to counter the attack plays a major role in security. Risk Analysis where the organization identifies, quantifies, and prioritizes risks to a system, is an important process that often precedes the development of an incidence response plan.

II. Common Security Tools:

Sodiya et al (2011), Binuyo (2019), and Badamasi(2018) have identified various tools used to prevent Cyber security breaches. These tools are itemized below:

Firewalls: these are used to implement access control policies between two or more networks. A firewall can be viewed as a security system, software-based or hardware-based, that manages

incoming and outgoing network traffic using a set of rules predetermined by the administrator (Binuyo, 2019).

Firewalls may be seen as guardians that stop unauthorized Internet users from intranets. They may be pre-set to protect specific segments of a network from untrusted users.

Anti-Virus software: Sodiya et al., (2011), Binuyo (2019), and Badamasi (2018) agree that anti-virus software is an effective tool used by universities to defend against cyber attacks. These tools must be updated regularly since the malware they combat is regularly changing in capacity. However, antivirus is not good enough to stand on its own. The university must implement multilevel security.

Password authentication: Password authentication has also been identified as an effective cybersecurity tool on a university network. Badamasi (2018) reports that unauthorized access is minimized when password authentication is available within a university's network. Also, Binuyo (2019) adds that password authentication is used to identify the entity requesting a specific network service, and describes Authentication to also refer to authenticating devices or software processes.

To further enhance authentication schemes, Binuyo (2019) highlights the use of public key cryptography, digital signature, and multi-layer, multifactor authentication (MFA), to augment password schemes. In addition, authentication protocols can be used in designing secure authentication schemes, including Secure Sockets Layer (SSL), Internet Protocol Security (IP SEC), and Secure Shell.

Intrusion Detection Systems: Debar (2000) defines an Intrusion-detection system (IDS) as a system that aims at detecting attacks against information systems. IDSs are designed to monitor computer systems with the intent to detect insecure states.

Categories of IDS exist depending on the intended usage. Debar (2000) identifies the Host-based, Network-based, and Hybrid IDSs. Host-based IDS are used in stand-alone systems to monitor for intrusions on that system. They can support the activities of anti-viruses and firewalls. The network-based IDS stand in network systems and serves several networked nodes while the hybrid can implement both functionalities.

While firewalls secure networks using packet filtering, IDS can go a step further by scanning packet content for malicious content (Debar,2000).

5. Developing a Cyber-based Business Continuity Plan for the University

Heng, (2015) defines Business Continuity Plan (BCP) as the product of a management process that identifies potential threats to an organization and the impacts on business operations of those threats and provides a framework for building organizational resilience with the capability to safeguard its human and capital assets.

Heng, (2015) itemizes the various steps in a BCP planning process. The process provides a cyclical framework for efforts, requirements, and outputs. Figure 3 illustrates the planning process.

Figure 2 : BCP methodology (source: https://www.alamy.com/)

6. Financial/Institutional Damage from Successful Cyber Attack on A University IT Infrastructure

Fouad (2021) identifies some damage that can be realized by universities due to Cyber attacks including loose of personal information such as social security numbers and addresses as in the case of the university of Yale where over students and staff were victims in 2018, disruption of academic operations such as cancellation of exams as in the case of North Umbria University in the UK, financial losses from ransomware attacks such as the case were the university of California is reported to have paid about $1.14 million in 2020, and legal actions on the universities by victims for allowing their sites to be compromised.

7. Insurance in Cyber security.

Onaikhena (2022) defined Cyber insurance as a contract between an insurer and an individual or a company to protect against loss arising from an attack on a computer-based system. Cyber insurance is a product line in insurance that has been available for over 25 years, designed to cover all costs and expenses related to breaches on an organization's IT system.

Onaikhena (2022) also identifies typical insurance policies that can be purchased by an individual or an organization (including a University) to include:

Media Liability: For those involved in media and entertainment. This can include universities with specialized departments that deal with media-related issues.

Network Security: This coverage includes malware damage from malware, DoS, Ransomware attacks, and so on.

Network Business Interruption: one can recover expenses incurred and not lose profits if this coverage is taken. It covers online businesses and protects them from downtime due to cyber incidents.;

However, Onaikhena (2022) itemizes some issues that cyber insurance presently does not cover including financial damage from loss of intellectual property; reputational cost; potential profits; cost of losing customers due to loss in reputation; and so on.

8 Conclusion

The threats to the Nigerian University IT infrastructure are humongous. There is a need for the institution to be proactive in combating the threats posed by cybercriminals to the university IT space. Investing in Cybersecurity infrastructure and tools relevant to combating the common vulnerabilities spotted in the university IT space, is paramount to securing the sites. Also, insurance policies available for various Cyber security breaches should be purchased to succor the university in the case of damages occurring from Cyber breaches.

References

Badamasi, B. (2018). *The effects of security protocols on cybercrime at Ahmadu Bello University, Zaria, Nigeria*(Doctoral dissertation).

Binuyo, G. O. (2019). An Assessment Of Cyber-security Technologies In the Selected University In southwestern Nigeria.

Debar, H. (2000). An introduction to intrusion-detection systems. *Proceedings of Connect*, *2000*.

Fouad, N. S. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. *Journal of Cyber Policy*, *6*(2), 137-154.

Heng, G. M. (2015). Business continuity management planning methodology. *International journal of disaster recovery and business continuity*, *6*(1), 9-16.

Onaikhena V. (2022) Cyber Insurance: the state of nimbleness in Nigeria. Retrieved from: www.mondaq.com/nigeria (06/11/22)

Paul , M. (2020), Hackers Have Access to Data from Nigerian and Kenyan Universities. Retrieved from: www.Techpoint.africa/2020/06/01 (1/11/2022)

Sodiya, A. S., Ibrahim, S. A., & Ajayi, O. B. (2011). The state of information security in south-western Nigerian Educational Institutions. *College of Natural Sciences Proceedings*, 38-45.

University of Notre Dame (2021), Business continuity Program. Retrieved from: www.riskmanagement.nd.edu

Vyas, G., Meena, S., & Kumar, P. (2014). Intrusion detection systems: a modern investigation. Int. J. Eng. Man. Sci.(IJEMS), 1(11).

Sterbenz, J. P., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., & Smith, P. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. Computer networks, 54(8), 1245-1265.