Global Review of Library and Information Science (GRELIS)
Vol. 17, No. 2, 2021 ISSN: 3428-0009

Application of Preventive Information Security Mechanisms for Combating Pharming Attacks on the Websites of the Universities in Northern States of Nigeria

By

Abdulrashid Abubakar
Zakari Mohammed
and
Umar Babangida Dangani

Abstract

This paper investigates the "Application of preventive information security mechanisms for combating pharming attacks on the University Websites in Northern States of Nigeria". Two objectives were formulated: to identify the causes of pharming attacks on the University websites and to determine the type of preventive mechanisms applied in combating pharming attacks on the websites of the Universities. Quantitative research methodology was used for the study. Nine universities in Northern States of Nigeria with 127 ICT personnel were selected. Questionnaire was used as an instrument in collecting the data. Mean and standard deviation were used to present and analyse the data collected in the study. The research found that pre-existing bugs; lack of security standard compliance; security vulnerabilities and weakness of the system; lack of filtering out fake redirects sites and unauthorized disclosure or modification of sensitive information were the causes of pharming attacks. The paper concludes that, if security safeguards are not adequate, pharmers affect the functionalities of the University websites undetected. They pharmers can attack a website using skills the software developers never imagined. The study recommended that, to ensure robust preventive security mechanisms the ICT personnel need to establish benevolent Internal Network detection system, use of server certificate and application of DNS server patching among others.

Keywords:
Pharming Attacks; Preventive, Information Security Mechanisms, University, Websites.

 ISSN: 3428-0009

Introduction

Advancement in Information Technology (IT) has enhanced universal electronic connectivity which poses new challenges to information security such as pharming attacks which include, domain configuration attack, domain name spoofing attack, Domain Name System (DNS) cache poising, hosts file modification and border router attack, to mention a few. There is no time in which information security does not matter. Many organizations such as Universities and Firms relying on the Internet are facing significant challenges to ensure that their networks operate safely and their systems continue to provide critical services even in the face of attacks.

Pharmers are very sharp, well-equipped, skilful and ready to take astounding efforts to attack websites. In order to combat them, there is the need to be acquainted with their strategies and methods, study how to protect information and follow the best practices with respect to information security. Achieving information security especially in an academic environment requires vast arrays of technical security mechanisms and legal skills. Abauabkar (2014) remarked that "as the volume of information grows and continues to be increasingly stored and communicated electronically, it is mandatory for educational institutions, especially Universities, to safeguard their sensitive information".

Pharming is one of the topmost cybercrimes of the twenty-first century demanding very slight talent on the part of the impostor. The need of protecting vital information such as users' credentials safe from the hands of pharmers becomes necessary. Users are becoming accustomed to accessing wireless routers in airports, restaurants, conferences, libraries, and other public spaces. Pharmers can set up malicious wireless routers in these areas that offer free Internet access but redirect users to spoofed websites. Oshinsky Oshinsky, Lorelie, Kenneth, Cherylyn, Briggs, Jenner and Block (2010) remarked that "pharmers can cripple the day to-day operation of organizations. Viruses from hackers or disgruntled employees can disable computers or overload the network, leading to business interruption.

Organizations also risk the loss of valuable intellectual property if the security of their computer network is breached".

Security Mechanism is an aspect of information security. It refers to a technique, apparatus, scheme, appliance, device or process for enforcing security. According to Stallings (2005), "Security Mechanism is any process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack. Examples of security mechanisms are encryption algorithms, digital signatures and authentication protocols among others". There are numerous devices or mechanisms to combat pharming attacks. They include: cryptographic techniques, authentication, authorisation, accounting (auditing), physical security, packet filters, firewalls, intrusion detection and prevention system to mention a few. The rapid advancement and extensive storing and transmitting of information via Internet along with frequent incidences of cybercrimes in academic environments gave rise to the necessity to enhance the method of securing the institutions vital information.

Statement of the Problem

The advancement in IT undoubtedly improved the business processes and efficiency in many organizations such as Universities and financial institutions like banks. They opened avenues for the malicious attackers like pharmers to illegitimately get in touch with someone else's banking credentials by pretending to be a legal customer to create illicit businesses. Pharming could cause the law investigation become harder. Access to University's resources for academic and administrative purposes have become essential to faculties, staff and students. At the same time, internal and external threats to the confidentiality, integrity and availability of these resources have elevated. Security vulnerabilities are prevalent and Universities remain target for pharming attacks. Pharmers rely on altering the DNS settings of the organisation's website

Various factors have led Universities to become popular targets of pharming attacks. They have different user-base consisting of students, staff and faculties. Also, they grasp the delicate private

 ISSN: 3428-0009

information for these users as well as Alumni. More so, Universities are involved in frequent funding and innovative researches which are valuable to motivated pharmers. It is against these backdrops that it is expedient to investigate the preventive mechanisms to combat pharming attacks on the websites of the universities in Northern States of Nigeria

Research Questions

This study sought to provide answers to the following research questions:

1. What are the causes of pharming attacks on the websites of the Universities in Northern States of Nigeria?
2. What type of preventive mechanisms are applied in combating pharming attacks on the websites of the Universities in Northern States of Nigeria?

Literature Review

Randed (2018) pointed out that, "the causes of this pharming attack could be due to lack of following the domain transfer process properly. Domain Hijacking has the broadest effect due to the fact that the pharmer targets the domain registration information itself. Therefore, there's need for high awareness of this form of attack". In Similar vein, (Randed, 2018) "described another causes of pharming attack: Registration of Similar Sounding Domains. This is another source of security issue for internal users. In this case a pharmer can register a domain 'www.uba.com' and lung out pharming on gullible users who do not care to differentiate the letter "i" being substituted with "1". The cause of this pharming attack is that, domain names made by typos on the original words (e.g., www.uba.com) cause a lot of traffic.

It could be deduced from this assertion that, lack of noticing the correct domain would lead to this type of pharming attack which can cause a devastating effect on users. Therefore, there is need for proper guidance for the users on surfing the Internet. Luckily, majority of the DNS servers have inbuilt security to safeguard them against pharming attacks. Yet they are not necessarily safe, since pharmers

endure to discover means of accessing them. Paladin (2016) revealed numerous causes of pharming attacks on University websites. Such as:

1. "Illegal access to sensitive information;
2. As a result of technical issues;
3. System security weakness;
4. Unauthorized use;
5. Pre-existing bugs;
6. Intimidating with scare ware;
7. Lack of changing the default logging credential of the router;
8. Using the links in an email to access any websites;
9. Unregularly checking all transactions are legitimates;
10. Lack of security patches;
11. Not updating software/browser;
12. Lack of running separate Name servers for redounding in different network segment;
13. Lack of separating external and internal server and use forwarding;
14. Giving personal data to strangers;
15. Insecure development practices;
16. Lack of filtering out fake redirect's sites;
17. Lack of using trust worthy ISP;
18. Lack of using robust Internet security solution;
19. Lack of guarding against domain hijacking;
20. Lack of restricting dynamic DNS updates when possible; and
21. Lack of using FraudWatch" (Paladin, 2016).

The implication of the aforementioned causes of pharming attacks on websites is that, the pharmer would be able to spy on a victim's web traffic, exploit security flaws and hijack search result.

Therefore, it is imperative for all websites owners to implement risk security control measures and review their risk profile.

Prevention is the process of stopping something from happening. Banday & Qadri (2007) posited that "pharming is relatively new, complex and continuously evolving phenomenon that includes social engineering as well as malicious technology. There is no fool proof technology or legislative system that can protect against or prevent pharming attacks from getting through. However, properly deployed combinations of technology coupled with employee education and diligence can significantly reduce the likelihood that a business or a customer will succumb and fall victim to this growing threat. Further, public reporting mechanisms established by governments and the law enforcement community."

Various approaches have been proposed for preventing website or link from phishing and pharming attacks. For example, in 2010, Sengar and Kumar "presented a solution for phishing attacks by classification of web pages. They proposed "PageSafe" which is an anti-phishing tool that prevents access to phishing web pages and also detects DNS poisoning attacks. PageSafe tool uses a machine learning approach (Neural Network) for automatic classification. Authors can build pharming detection module to detect pharming attacks. Pharming detection module compares the IP addresses from Local DNS and Network DNS with the IP address from remote DNS for the requested URL. If they do not match, then pharming is detected and alert is made to the user. Authors can also introduce the PageSafe a novel tool that does not completely rely on automation to detect phishing. Instead, PageSafe relies on user input to decide on the legitimacy of a URL".

It is vital to stress that the loss of data assets in a University is a serious and huge loss capable of affecting the progress of the University. It will also portend a gloomy picture and a terrible pointer to the University's reputational crises. Aslam Wu & Cliff (2010) "presented a solution to protect users from phishing and pharming attacks. This solution is based on a hashed password which is the hash value of the user-typed password and the authentication server's IP address. The solution rests on the fact that the server connected by a client using Transmission Control Protocol (TCP) connection can't fraud about its

IP address. If a user goes to a malicious server (by a Phishing or a Pharming attack), the password obtained by the malicious server will be the hashed password (tied to the malicious server's IP address) and will not be usable by the attacker at the real server, thus defeating Phishing or Pharming attack. Authors use PwdIP-Hash for specific browser, but it might not be useful for other famous web browsers such as Firefox, Chrome, etc".

Ollman (2015) had earlier posited that "pharming attacks tend to be harder to defend against that traditional phishing attacks due to the distributed nature of the attack focus and the use of resources not under the control of the victim organization". "The defenses that will be most successful in preventing pharming attacks focus upon the following areas:

1. "Change Management, Monitoring and Alerting: the potential for an administrator or other employee to maliciously modify DNS resolution information without detection is great. As financial incentive increase, organizations and ISP's will need to ensure that adequate change control, monitoring and alerting mechanisms are in place and enforced" (Ollman, 2015).
2. "Third-Party Host Resolution Verification: Many third-party developed plug-in toolbars designed to detect phishing attacks are deceived by pharming attacks. Some toolbars provide IP address allocation information such as clearly stating the geographic region associated with a particular net block. This is useful for identifying possible fake pharming sites" (Ollman, 2015).
3. "Server Certificates: To help prevent pharming attacks, an additional layer can be added to the authentication process, such as getting the server to prove it is what it says it is. This can be achieved through the use of server certificate" (Ollman, 2015).
4. "DNS Server Patching, Updating and Configuring: as with any inter-based host, it is vital that all accessible service can be configured in a secure manner and that all current security updates or patches be applied. Failure to do so is likely to result in an

exploitation of any security weaknesses, resulting in loss of data integrity" (Ollman, 2015).

5. "Search Engine Control: Internet search engine are undergoing constant development. Many of the methods used by attacks to increase their page ranking statics are known of by the search engine developers, and a constant cycle of detection and refinement can be observed by both parties.

For instance, Google modified its search algorithm to "rest" the page rank statics of web sites that had recently changed ownership, this was to reduce the impact of instant "backlinks" and the weighting they attach to a ranking" (Ollman, 2015).

To this end, the initiative by Google should be emulated by other giants' industry and Universities in order to reduce the impact of pharming attacks. Paladin (2016) outlined various mitigation security mechanisms to combat pharming attacks which include:

1. "Use of SSS certificate to help establish the true Identity of websites;
2. Ensure that the DNS servers have been secured and hardened;
3. Switch off recursive queries in the DNS server configuration;
4. Use of readily available online services to alert any changes on Domain's registrar or DNS configuration, e.g., Markmornitor.com, Domain monitor, Name Warden, Whois.sc Mark Alert;
5. Visual cue e.g., identity cues;
6. Anti-pharming tool;
7. Multifactor and Token based Authentication;
8. Educating Website users;
9. Keep simple names for domain;
10. SfoofStick, Google Safe browsing for Mozilla, Firefox;
11. NetCraft Toolbar; and

 ISSN: 3428-0009

12. Cloud Mark Anti-Fraud Toolbar" (Paladin, 2016).

"Fortunately, most DNS servers have safekeeping structures to safeguard them against pharming attacks, yet they are not inevitably resistant, since impostors linger to get ways to access them. There is need for many organisations such as Universities and firms to employ mitigation security mechanisms to combat pharming attacks on their websites".

Methodology

Quantitative research methodology was adopted for this study. The target population of this study consisted of all the 61 Universities in the Northern States of Nigeria recognised by the National University Commission (NUC). However, the study population (subjects of this study) were the Information and Communication Technology (ICT) personnel of the Universities studied. They comprised of the Directors, the staff of the Software Development Units and the staff of the Networks Infrastructure and Security Units. This gives a total number of seven hundred and thirteen (713) personnel. A sample of 9 Universities was used for the study with 127 respondents (ICT personnel). The data collected were analysesd using quantitative technique (mean, standard deviation, frequencies and percentages) to answer the research questions raised in the study.

Results and Discussions

The data collected and analysed were presented and discussed as follows:

Causes of Pharming Attacks on the Websites of the Universities Studied in Northern States of Nigeria

The first research question sought to determine the "causes of pharming attacks on the websites of the Universities studied in Northern States of Nigeria". In order to answer this research question, a list of causes of pharming attacks on websites was outlined for the respondents to indicate as many causes as applicable in their various Universities as shown in Table 1. The acceptable response benchmark was 3.0 mean score. Thus, any item less than 3.0 mean scores was not accepted as really the cause of pharming attacks.

 ISSN: 3428-0009

Table 1: Causes of Pharming Attacks on the Websites of the Universities Studied in

Categories of Universities

S/N	Causes of Pharming Attacks on University Website	Federal University F1 Always	F1 Seldom	F1 Never	F2 Always	F2 Seldom	F2 Never	F3 Always	F3 Seldom	F3 Never	F	%	X	SD	State University S1 Always	S1 Seldom	S1 Never	S2 Always	S2 Seldom	S2 Never	S3 Always	S3 Seldom	S3 Never	F	%	X	SD
1	Pre-existing bugs	2	1	13	3	2	10	12	1	5	#	#	3.06	0.81	1	5	5	1	5	5	1	5	5	#	67	3.52	0.91
2	In-secured development practices	2	2	14	3	2	10	12	1	5	#	#	3.67	0.87	2	2	12	1	1	4	1	3	7	#	67	3.38	0.71
3	Lack of security standard compliance	1	2	11	3	2	13	2	2	13	#	#	3.11	0.82	2	2	9	4	0	9	0	0	7	#	67	3.59	0.62
4	Lack of following domain transfer process properly	3	2	12	3	3	8	2	2	14	#	#	3.43	0.71			15	1	1	5		4	7	#	67	2.12	1.01
5	Lack of guarding against domain hijacking	4	1	10	5	3	8	2	1	15	#	#	3.78	0.71	2	2	10	1	3	4	0	3	8	#	67	3.12	0.67
6	Unpatched security vulnerabilities	1	3	14	2	2	12	1	2	12	#	#	2.86	1	2	4	5		5	4	1	4	8	#	67	2.70	1.08
7	Ignoring fundamental security polices	2	1	15	2	3	11	1	2	12	#	#	2.96	8.12	2	3	6	1	3	4	2	6	6	#	67	3.78	0.74
8	Insufficient IT security management	1	2	15	1	2	12	2	1	13	#	#	2.18	0.96	0	0	5		3	11	2	6	6	#	67	2.57	1.1
9	Poorly configured firewalls	3	2	14	2	2	11	2	2	11	#	#	3.04	0.81	0	4	11	0	4	5	0	3	6	#	67	2.85	1.11
#	Shortage of cyber security personnel	1	2	14	1	1	16	2	2	10	#	#	2.78	0.96	0	5	4	2	5	5	1	7	4	#	67	2.94	0.91
11	Lack of frequent security	1	3	14	2	2	12	1	2	12	#	#	2.87	1.01	2	3	9	2	1	5	0	3	8	#	67	3.52	0.76
#	Security vulnerabilities and weakness of the system	2	2	14	3	2	10	1	2	15	#	#	3.67	0.76	2	5	5	1	3	5	1	5	6	#	67	3.52	0.63
#	Lack of filtering out fake redirects sites	4	1	10	5	3	8	2	1	15	#	#	3.18	0.71	2	2	7	2	3	5	2	4	6	#	67	3.70	0.77
#	Lack of using trustworthy Internet Service Providers	1	2	16	1	3	11	1	2	12	#	#	2.71	1	2	1	7	1	3	5	2	6	6	#	67	3.15	0.92
#	Lack of using robust Internet security solution		2	19		1	13	1	2	11	#	#	2.35	1.11		5	4	4	2	5	1	7	5	#	67	4.42	0.51
#	Vulnerability of wireless access point	2	1	13	3	2	10	1	2	15	#	#	2.71	0.81	2	4	5	4	5	2	2	5	4	#	67	4.55	0.5
#	Lack of reducing dynamic DNS updates when	3	2	14	2	2	11	2	2	11	#	#	3.04	0.61		4	8		3	5		7	6	#	67	2.85	1.11
#	Unauthorized disclosure or modification of sensitive information	3	2	12	3	3	8	2	2	14	#	#	3.43	0.8	2	5	5	1	2	6	1	5	6	#	67	3.52	0.71
#	Poorly understood aspect of misconfiguration and malfunctioning	1	3	14	2	2	12	1	2	12	#	#	2.86	0.9	1	2	5	2	2	11	2	3	5	#	67	3.51	0.61
#	Lack of changing the default logging credential of the router	3	2	12	3	3	8	2	2	14	#	#	3.43	0.72	1	2	5	2	2	11	2	3	5	#	67	3.71	0.71
	Cluster Mean												3.06	0.9												3.40'	8

S/N	Causes of Pharming Attacks on University Website	Private University P1 Always	P1 Seldom	P1 Never	P2 Always	P2 Seldom	P2 Never	P3 Always	P3 Seldom	P3 Never	F	%	X	SD	ΣF
1	Pre-existing bugs	1	4	5	1	4	5	1	5	5	31	96.9	3.5	0.71	112
2	In-secured development practices		4	7	2	2	3			12	31	96.9	2.4	0.101	112
3	Lack of security standard compliance	1	4	1		2	6	2	4	10	31	96.9	3.4	0.711	112
4	Lack of following domain transfer process properly	2	3	2	1	1	6	2	2	12	31	96.9	3.5	0.617	113
5	Lack of guarding against domain hijacking	2	3	8		1	8	1	8	6	31	96.9	2.7	0.912	113
6	Unpatched security vulnerabilities		8	7		4	2	1	2	10	31	96.9	2.6	0.101	113
7	Ignoring fundamental security polices	1	2	8	2	2	9	2	8	3	31	96.9	3.1	0.691	113
8	Insufficient IT security management	1	1	4		4	11		1	9	31	96.9	2.6	0.101	112
9	Poorly configured firewalls		1	5		1	9	1	5	9	31	96.9	2.8	0.961	113
#	Shortage of cyber security personnel	1	4	4		2	6	2	2	8	31	96.9	3.3	0.671	113
11	Lack of frequent security	5		6	1	2	4	1	2	10	31	96.9	3.5	0.731	113
#	Security vulnerabilities and weakness of the system	1	4	5	1	5	4	1	5	5	31	96.9	4	0.012	113
#	Lack of filtering out fake redirects sites	2	2	7	2	2	6		4	5	31	96.9	3.6	0.721	112
#	Lack of using trustworthy Internet Service Providers	1	1	6	1	1	11	2	5	3	31	96.9	3.4	0.711	113
#	Lack of using robust Internet security solution	1	1	3	4	6	5	4	4	3	31	96.9	4.7	0.512	113
#	Vulnerability of wireless access point	3	1	10		2	10	1	1	3	31	96.9	3.2	0.901	113
#	Lack of reducing dynamic DNS updates when	2	3	2	1	1	6	2	2	12	31	96.9	3.5	0.712	113
#	Unauthorized disclosure or modification of sensitive information	1	4	4		2	6	2	2	8	31	96.9	3.3	0.678	112
#	Poorly understood aspect of misconfiguration and malfunctioning	1	4	1		2	6	2	4	10	31	96.9	3.4	0.712	112
#	Lack of changing the default logging credential of the router	2	4	7	3	4	2	2	1	6	31	96.9	3.9	0.691	113
	Cluster Mean												3.3	0.8	

Table 1 shows the response mean scores and standard deviation of the "causes of pharming attacks on the websites of the 3 categories of the Universities (Federal, State and Private) studied in Northern States of Nigeria". It revealed that, for the Federal Universities studied, items 1, 2, 3, 4, 5, 9, 12, 13, 17, 18 and 20 respectively have response mean scores and standard deviation above the acceptable benchmark of 3.00. This implies that they are indeed the "causes of pharming attacks on the websites of the Federal Universities studied in Northern States of Nigeria". In contrast, items 6, 7, 8, 10, 11, 14, 15, 16 and 19 are below the acceptable benchmark of 3.00. Hence, they are indeed not accepted as the real "causes of pharming attacks on the websites of the Federal Universities studied in Northern States of Nigeria".

On the other hand, for the State Universities studied, items 4, 6, 8, 9, 10 and 17 respectively have response mean scores and standard deviation below the acceptable benchmark of 3.00. It can be said that, they are not accepted as the real "causes of pharming attacks on the websites of the State

 ISSN: 3428-0009

Universities studied". On the contrary, items 1, 2, 3, 5, 7, 11, 12, 13, 14, 15, 16, 18, 19 and 20 have response mean scores and standard deviation above the acceptable benchmark of 3.00. This means that the items are the real "causes of pharming attacks on the websites of the State Universities studied in Northern States of Nigeria".

Similarly, for the Private Universities studied, items 2, 5, 6, 8 and 9 respectively have response mean scores and standard deviation below the acceptable benchmark of 3.00. This indicates that the items are not accepted as the real causes of pharming attacks on the websites of the Private Universities studied. On the other hand, items 1, 3, 4, 7, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19 and 20 have response mean scores and standard deviation above the acceptable benchmark of 3.00. Thus, the items are indeed accepted as the real "causes of pharming attacks on the websites of the Private Universities Studied in Northern States of Nigeria".

An in-depth analysis of the cluster response mean scores and standard deviation of the 3 categories of the Universities studied reveals that, the Federal Universities have cluster mean scores of 3.06, StD= .853; State Universities have the cluster mean scores of 3.40, StD=7.92; and Private Universities have the cluster mean scores of 3.32, StD=.755. Hence, it is clear indication that the State Universities have the highest cluster response mean scores. In effect, this implies the websites of the State Universities are the worst heat. This suggests that State governments need to embark on periodic evaluation and upgrading of their State University websites by making provision for funds in its annual and supplementary budgets to include ICT maintenance and training of ICT personnel.

By and large, it can be concluded that there are various "causes of pharming attacks on the websites of the Universities studied in Northern States of Nigeria". These include among others: "the presence of pre-existing bugs, lack of security standard compliance, security vulnerabilities and weakness of the system, lack of filtering out fake redirects sites, unauthorized disclosure or modification of sensitive information and lack of changing the default logging credential of the router among others".

This finding is in consonance with the submissions of Paladin (2016) and Crash & Schaller (2017) who found that the "major causes of pharming attacks on websites include illegal access to vital information of organisation and security vulnerabilities or weaknesses". Thus, the management of Universities need to invest heavily on technical controls of their information system.

Contrary to conventional wisdom, this finding disagrees with the earlier findings of Randed (2018) who identified "DNS Cache poisoning, domain hijacking and registration of similar sounding domains as causes of pharming attacks on websites". This may be that the Universities studied have employed more robust security mechanisms in order to identify the pros and cons of this new trend of pharming. On the other hands, much of the identified causes of pharming attacks on the websites of the Universities studied in Northern states of Nigeria could be that the administrators and websites managers do not care to secure and monitor the new techniques being employed by the fraudsters in the cyber business.

Lack of review of risk security control measures and risk profile may have been responsible for such vulnerability. So therefore, the University management should take an extra level of security, which may come into picture if someone has already breached the access security such as getting hold of a valid username and password, which can help getting access to the online database. So, the security mechanism implemented within the database such as encrypting the data inside prevents the data to be compromised even if someone has got unauthorized access to the database.

Preventive Mechanisms Applied to Combat Pharming Attacks on the Websites of the Universities Studied in Northern States of Nigeria

The second research question of this study was aimed at identifying the "types of preventive mechanisms applied to combat pharming attacks on the websites of the Universities studied in Northern States of Nigeria". In order to ascertain this objective, the responses of the respondents were rated using five Points Likert Scale of Measurement in the following order: Always, Often, Occasionally, Seldom, and Never. But, for the Researcher's convenience, the options were merged into 3 to ease

 ISSN: 3428-0009

comprehension in the discussion as shown in Table 2. The acceptance benchmark was 3.0 response mean scores. Thus, any item less than 3.0 response mean scores was not accepted as being a detective information security mechanism applied to combat pharming attacks on the Universities studied.

Table 2: Preventive Mechanisms Applied to Combat Pharming Attacks on the Websites of the Universities Studied in Northern States of Nigeria

S/N	Preventive Mechanisms to Combat Pharming Attacks on the University Websites Studied	Categories of Universities: Federal University F1 Always	F1 Seldom	F1 Never	F2 Always	F2 Seldom	F2 Never	F3 Always	F3 Seldom	F3 Never	F	%	X	SD	State University S1 Always	S1 Seldom	S1 Never	S2 Always	S2 Seldom	S2 Never	S3 Always	S3 Seldom	S3 Never	F	%	X	SD	Private University P1 Always	P1 Seldom	P1 Never	P2 Always	P2 Seldom	P2 Never	P3 Always	P3 Seldom	P3 Never	F	%	X	SD	∑F
1	Use of server certificate	2	3	14	3	5	8	2	2	10	49	86	3.7	0.822	1	2	10	4	1	8	0	0	7	33	87	2.39	0.821	2	2	2	1	2	6	4	2	10	31	97	3.92	[illegible]	113
2	Provision of SSL issued vouches with certificates	3	4	8	3	3	8	4	2	14	49	86	3.8	0.774	2	4	5	1	3	4	2	6	6	33	87	3.04	0.752	1	2	4	2	4	9	2	4	3	31	97	3.53	0.713	113
3	Gathering and securing DNS secrets	4	4	11	5	5	8	2	5	5	49	86	3.7	0.791	2	5	4	2	2	6	1	5	6	33	87	2.15	0.901	1	4	5	1	5	4	1	5	5	31	97	3.68	0.759	113
4	Provision of switch off recursive queries in the DNS server configuration	1	3	14	2	2	12	3	2	10	49	86	3	1.011	2	1	7	3	3	8	1	1	7	33	87	3.19	0.671	2	3	5	4	1	4	2	4	6	31	97	3.94	1.521	113
5	Use of DNS configuration	5	2	10	4	1	13	1	2	11	49	86	3.4	0.98	2	4	5	4	5	2	2	5	4	33	87	3.78	0.566	3	1	5	5	2	10	1	1	3	31	97	3.56	0.634	113
6	Use of BloofStick	1	3	14	2	2	12	1	2	12	49	86	3	1.011	2	4	4	1	3	4	4	3	8	33	87	3.43	0.704	3	1	3	2	6	5	4	4	3	31	97	4.84	0.634	113
7	Application of file change monitoring system	7	1	10	6	2	10	1	2	10	49	86	4	0.871	2	6	7	1	3	5	1	1	7	33	87	3.18	0.841	1	4	1	2	3	6	3	3	8	31	97	3.72	0.648	113
8	Use of Web Application Firewall (WAF)	2	2	14	3	2	11	9	2	4	49	86	3.7	0.721	2	3	5	3	3	5	1	5	6	33	87	3.52	0.761	1	4	1	3	3	3	2	4	10	31	97	3.41	0.748	113
9	Application of Content Delivery Network (CDN)	5	1	10	3	2	10	12	1	5	49	86	3.6	0.811		3	8	3	3	3	4	7	2	33	87	2.85	0.931	3	1	10	5	2	5	1	1	3	31	97	3.77	0.413	113
10	Use of Site Seal	2	3	14	2	2	12	4	2	8	49	86	3.9	0.823		5		4	2	7	6	5	4	33	87	4.12	0.532	2	4	7	3	4	2	2	1	6	31	97	3.92	0.342	113
11	Use of Secure Sockets Layer certificate	3	3	12	3	6	8	2	6	6	49	86	3.4	0.658	2	3	8	2	1	4	5	3	5	33	87	3.42	0.761	2	1	3	6	1	8	3	5	4	33	97	2.86	0.759	113
12	Safeguarding domain registration information	3	1	8	5	3	8	8	7	6	49	86	3.3	0.912	2	2	10	5	3	4	5	3	8	42	87	3.173	0.841	3	2	4	3	4	2	1	2	10	31	97	2.58	1.042	113
13	Frequent updating of installed software	1	2	15	1	2	12	2	1	13	49	86	3	1.091	2	3	6	1	3	4	2	6	6	33	87	3.36	0.742	1	6	5	1	1	7	2	5	3	31	97	2.35	0.478	113
14	Creation of complicated passwords	2	2	12	2	2	14	2	2	11	49	86	3.6	0.804	2	2	5	1	1	4	5	7	6	33	87	3.39	0.754	2	4	5	1	5	3	1	5	5	31	97	2.58	0.413	113
15	Using trusted and legitimate Internet Service Provider	3	2	12	3	2	8	5	6	8	49	86	3.5	0.679	2	4	5	4	5	2	2	5	4	33	87	4.05	0.521	2	4	5	1	5	4	1	5	4	31	97	3.02	0.712	113
16	Frequent updating of compiler	1	2	5	7	3	8	5	6	12	49	86	2.8	1.001		5	4	5	5	2	1	7	4	33	87	2.91	1.152	2	3	2	1	7	6	2	2	6	31	97	2.52	0.759	113
17	Use of transport security mechanism	1	3	14	2	5	12	5	2	5	49	86	3	1.003	1	3	10	1	1	2	5	4	7	33	87	2.06	1.173	5		6	1	2	4	1	2	10	31	97	3.82	0.372	113
18	Use of Security Assertion Markup Language authorization over SSL	4	1	10	5	3	8	2	1	15	49	86	3.8	0.769	2	1	7	1	3	5	6	1	7	33	87	3.44	0.762	1	2	7	2	2	2	4	4	7	31	97	3.41	1.201	113
19	Creation of complicated passwords	2	1	13	3	2	10	1	2	15	49	86	3.8	0.667	2	2	4	4	3	5	3	8	4	33	87	2.85	0.961	2	2	7	2	3	5	3	4	3	31	97	3.05	0.629	113
20	Use of Secure Token Service (STS) Issued Token	2	1	15	2	3	11	1	2	12	49	86	2.7	1.004	2	2	3	5	1	3	6	5	6	31	87	3.72	0.641	1	1	3	2	4	6	4	1	9	31	97	2.08	0.548	113
	Cluster Mean												3.4	0.831												3.22315	0.871												3.328	0.9	

Table 2 revealed the response mean scores and standard deviation of the "preventive mechanisms applied to combat pharming attacks on the websites of the 3 categories of the Universities (Federal, State and Private) studied in Northern States of Nigeria". It shows that, for the Federal Universities studied, items 1, 2, 3, 5, 7, 8, 9, 10, 11, 12, 14, 15, 18 and 19 respectively have response mean scores and standard deviation above the acceptable benchmark of 3.00. This implies that they are indeed the "preventive mechanisms applied to combat pharming attacks on the websites of the Federal Universities studied in Northern States of Nigeria". In contrast, items 4, 6, 13, 16, 17, and 20 are below the acceptable benchmark of 3.00. Hence, they are indeed not accepted as the real "preventive mechanisms applied to combat pharming attacks on the websites of the Federal Universities studied in Northern States of Nigeria".

 ISSN: 3428-0009

On the other hand, for the State Universities studied, items 1, 3, 9, 16, 17 and 19 respectively have response mean scores and standard deviation below the acceptable benchmark of 3.00. It can be said that, they are not accepted as the real "preventive mechanisms applied to combat pharming attacks on the websites of the State Universities studied". On the contrary, items 2, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 18 and 20 have response mean scores and standard deviation above the acceptable benchmark of 3.00. This means that they are the real "preventive mechanisms applied to combat pharming attacks on the websites of the State Universities studied in Northern States of Nigeria".

Similarly, for the Private Universities studied, items 11, 12, 13, 14, 16, and 20 respectively have response mean scores and standard deviation below the acceptable benchmark of 3.00. This indicates that they are not accepted as the real "preventive mechanisms applied to combat pharming attacks on the websites of the Private Universities studied". On the other hand, items 1, 2, 3, 4, 5, 6, 8, 9, 11, 12, 13, 15, 17, 18 and 19, have response mean scores and standard deviation above the acceptable benchmark of 3.00. Thus, they are indeed accepted as the real "preventive mechanisms applied to combat pharming attacks on the websites of the Private Universities Studied in Northern States of Nigeria".

An in-depth analysis of the cluster response mean scores and standard deviation of the 3 categories of the Universities studied reveals that, the Federal Universities have cluster mean scores of 3.42, StD= .831; State Universities have the cluster mean scores of 3.22, StD=.871; and Private Universities have the cluster mean scores of 3.33, StD=.868. This means that all the 3 categories of the Universities studied have response mean scores and standard deviation on (preventive mechanisms) above the acceptable benchmark of 3.00. Hence, it is a clear indication that the Universities studied accepted the "preventive mechanisms as the type of information security mechanisms applied in combating pharming attacks on their University websites".

By and large, it can be concluded that there are various "preventive mechanisms applied in combating pharming attacks on the websites of the Universities studied in Northern States of Nigeria".

These include: "provision of SAML sender vouches with certificates mechanism, Use of DNS configuration; application of file change monitoring system; use of Web Application Firewall (WAF); use of site seal; using trusted and legitimate Internet Service Provider; and use of Security Assertion Markup Language authorization over SSL among others". This finding is in consonance with the submissions of Banday & Qadri (2007); Sengar & Kumar (2010); Aslam Wu & Cliff (2010) and Ollman (2015) who found that "preventing mechanisms are important in protecting and safeguarding the number of pharming attacks on websites".

Conclusion

From the analysis and findings of the study, it is clear that the ICT staff of the Universities studied have realized the need for the application of preventive mechanisms as part of defense-in-depth strategy for providing reasonable protection of sensitive information vis-à-vis the means of detection and remediation of security breaches. However, the ICT staff did not explore, to a large extent, the advantages of use of PageSafe detective mechanism, use of server certificate and application of DNS server patching mechanisms to protect the occurrences of most pharming on the websites of the University, which include the human factors attacks, local host and local networks attacks, domain configuration attack, domain name system spoofing attack, static pharming attack, pharming attack via sending email and domain hijacking attack. This paved way for cyber-crimes.

Recommendations

The following recommendations are made;

1. There is need for the ICT expertise to identify the pros and cons of pharming attacks by carrying out regular security reviews on the University websites in the areas of software development, software testing, bug fixes, quality assurance implementation, user security, internal security controls and monitoring the traffics on DNS servers.

2. Ensuring robust information security mechanisms such as: use of benevolent Internal Network detection system, use of server certificate and application of DNS server patching, updating and configuring are in place and enforced in order to effectively combat pharming attacks on the websites of Universities.

Referees

Abubakar, A. (2014). Application of Cryptography for Information Security in Umaru Musa Yar'adua University, Katsina. Unpublished M.Sc. Thesis at Ahmadu Bello University, Zaria.

Aslam, B., Wu. L. & Cliff C. Z., (2010). "PwdIP-Hash - A Lightweight Solution to Phishing and Pharming Attacks", N*inth IEEE International Symposium on Network Computing and Applications*, pp.198-203.

Banday, M.T., & Qadri, J.A. (2007). "Phishing - A Growing Threat to E-Commerce," The Business Review, ISSN: 0972-8384, 12(2), pp. 76-83.

Ollman, G. (2015). "The Pharming Guide". Understanding and Preventing DNS-Related Attacks by Phishers. Retrieved on 5th, August, 2018 from www.ngssofotware.com.

Oshinsky, J., Masters, S.L, Lee, K., J. Briggs, C.J, & Block, J (2010). Fighting Phishing, Pharming, and Other Cyber-Attacks: Coverage for High Tech Liabilities. RMIA Journal.

Paladin (2016). Pharming on the Net. Retrieved on 12th August, 2019 from https: new.pladinet/blog/pharming on-net.

Randed (2018). How Pharming Work. Retrieved on 23rd august, 2019 from https://randed.com-pharming.

Sengar, P. & Kumar, V. (2010). "Client-Side Defense against Phishing with PageSafe", *International Journal of Computer Applications*, P6-10.

Stallings, W. (2005). Cryptography and Network Security, Principles and Practices. Third Edition. USA: Pearson Education, Inc.

