GJR Publication
OPEN ACCESS

Global Journal of Research in Engineering & Computer Sciences
ISSN: 2583-2727 (Online)
Volume 03| Issue 02 | March-April | 2023
Journal homepage: https://gjrpublication.com/gjrecs/

Review Article

Management of Vulnerabilities in Cyber Security

*Muhammad Ahmad Baballe[1], Aminu Ya'u[2], Sirina Farouk Ibrahim[3], Bello Abubakar Imam[4], Mustapha Aliyu Yusif[5], Abubakar Sadiq Muhammad[6], Aliyu Musa Lawan[7], Abdulmuhamin Muhammad[8]

[1]Department of Computer Engineering Technology, School of Technology, Kano State Polytechnic, Kano, Nigeria
[2]Department of Architecture, School of Enviromental Studies Gwarzo, Kano State Polytechnic, Kano, Nigeria
[3]Department of Architecture, School of Enviromental Studies Gwarzo, Kano State Polytechnic, Kano, Nigeria
[4]Department of Computer Science, School of Technology, Kano State Polytechnic, Kano, Nigeria
[5]Department of Civil Engineering Technology, School of Technology, Kano State Polytechnic, Kano, Nigeria
[6]Department of Computer Engineering Technology, School of Technology, Kano State Polytechnic, Kano, Nigeria
[7]Department of Computer Engineering Technology, School of Technology, Kano State Polytechnic, Kano, Nigeria
[8]Department of Computer Engineering Technology, School of Technology, Kano State Polytechnic, Kano, Nigeria

DOI: 10.5281/zenodo.7779507 **Submission Date: 15 March 2023 | Published Date: 29 March 2023**

***Corresponding author:** Muhammad Ahmad Baballe
Department of Computer Engineering Technology, School of Technology, Kano State Polytechnic, Kano, Nigeria
ORCID: 0000-0001-9441-7023

Abstract

Cybercriminals frequently use phishing attempts to trick unwary individuals into disclosing their personal information. The detection of the cybersecurity (CS) state of Internet of Things (IoT) devices determines the necessity to search for and create techniques of detecting various threat types. Thanks to the unification used in the mass manufacture of IoT devices, it is simpler to make software and hardware modifications in order to prohibit some built-in protection mechanisms from the standpoint of a potential intruder. It becomes vital to offer standard ways of data analysis from both internal and external information sources in order to evaluate the level of device cybersecurity

Keywords: Vulnerabilities, Cybersecurity, Cyberattacks, Internets, Internet of Things.

INTRODUCTION

Nearly every aspect of our lives today depends on internet applications, including education, online shopping, software services, and entertainment. The user's vital data, including their online banking account, are therefore managed by a special secure account [6]. Online and in the digital era, security is becoming more and more important. In all spheres of human activity, digitalization is swiftly establishing itself as the norm. An review of science and technology trends shows that people, organizations, banks, and governments are increasingly reliant on digital tools, databases, and software to manage their strategic weapons. Every day, no matter who the owner is, organized gangs of knowledgeable cybercriminals seize control of other people's computers and gadgets and launch a number of destructive programs against websites. In a matter of seconds, everything stops operating, including ATMs, companies, phone lines, and even the presidential websites of the world's superpowers. The world tends to focus more on cybersecurity and information resource management. Because it was unexpected, no one could have predicted that the financial crisis of 2007–2008, which began with the US housing crisis, bank failures, and falling stock prices, would result in a global economic catastrophe (also known as the "Great Recession"). A infectious disease that was identified in humans for the first time in December 2019 in China posed the next threat to humanity [2]. A pandemic was caused by an outbreak of the disease. The primary cause of the illness was the SARS-CoV-2 coronavirus [3, 4]. The illness has had a terrible impact on both human health and the entire global economy. A sizable portion of the global population was compelled by the illness to think about the issue of distant work. Institutions of higher learning have shifted to online instruction. Every day, there are a lot of online conferences, meetings, and business gatherings. Unquestionably, this sparked a tendency toward extending the use of digital technologies. Given the aforementioned, it was impossible to predict the financial crisis and contagious diseases like "black swans" in time to establish effective countermeasures [5]. Therefore, one shouldn't rule out the possibility of devastating, global cyberattacks in the future. The social, economic, and political ramifications of

the Internet ceasing, even for a day, are currently impossible to anticipate. It should be mentioned that our digital operations and personal and business computer networks need to be securely protected [25].

Fig. 1: A model of cyber security

RELATED WORKS

Due to their complexity, there is no single technique to effectively stop all types of cyberattacks. Increasing user awareness and using more programmed tools are fundamentally two separate sorts of security solutions [7]. Several methods for identifying phishing websites have been developed during the past ten years in response to a number of phishing scams that try to fool individuals into providing their personal information. One of a number of techniques, including list-based detection, machine-based learning detection, heuristic detection, or deep learning methods, can typically be used to stop cyberattacks, including phishing [8]. To assess the dependability of websites, more modern techniques have updated machine learning algorithms. In the review of recent detection strategies in this section, the use of machine learning techniques to enhance the detection of phishing websites has been discussed. Rajithaet and VijayaLakshmi (2016) proposed oppositional Cuckoo search and fuzzy logic categorization to identify harmful cyber-attacks. The OCS algorithms have been used to pick the most important features from the four different types of features during the feature selection step. In order to calculate the fuzzy score, the second stage involves training the selected features with FLC. A fuzzy score is used in the testing stage to identify harmful universal research locators (URLs) [9]. A twin support vector machine-based heuristic technique was proposed by Rao et al. in 2020. By comparing the differences between hyperlink and URL properties for both the URL of the visited page and the home page to categorize phishing websites, this method detects malicious phishing sites registered on susceptible servers [10]. To increase the accuracy of phishing detection, Tan et al. (2020) have extracted a new characteristic. The suggested approach starts with the extraction of hyperlinks from the webpage and a group of related URLs. In order to create a web graph and a classifier to recognize phishing web pages, the page linking data was gathered during this procedure [11]. The research study carried out by ALI et al. (2020) determines the weighting of various features using the particle swarm optimization (PSO) method. Websites that are phishing can be recognized. According to the findings of their research, using fewer website features allows suggested machine learning algorithms to identify phishing websites more accurately [12]. Convolutional neural networks (CNN) have been utilized by Aljofey et al. (2020) to identify phishing websites. It is possible to record URL strings without being aware of phishing. They then accelerate the current URL classification using the sequential pattern functionality [13]. Convolutional layers in a deep neural network were suggested by Wei et al. (2020). To identify fraudulent URLs, our work just analyzes URL text. In contrast to earlier studies, this technique finds zero-day attacks more quickly. The performance of mobile devices can also be used with it without suffering considerably [14]. Using extraction and representation paradigms, Feng et al. (2020) suggested a hybrid deep learning network to identify phishing websites. The approach first treats the architectures of HTML, DOM (Document Object Model), and URL as a string of characters. The representations of webpages are automatically learned using representational technology, and these representations are then submitted to a deep learning hybrid network made up of a coevolutionary neural network and a bidirectional memory network to retrieve local and global information [15]. A support vector machine (SVM) binary classifier was used by Anupam and Kar (2020) to predict if a website was valid or not using several aspects of the URL (IP address length, HTTP request). The Firefly, the Bat, the Grey Wolf, and the Whale are offered to identify the ideal hyperplane of the SVM in addition to the help of four optimization algorithms [16]. In order to replace the knowledge base of the expert system, Mahdavifar and Ghorbani (2020) developed a knowledge base by employing Deep Embedded Network Expert Systems (DeNNeS) to extract precise rules from a trained deep network (DNN) architecture [17]. By combining the best possible set of characteristics and criteria, Kumar and Indrani (2020) proposed a phishing detection method that uses a deep neural network classifier and fuzzy logic to categorize websites into three categories: phishing, non-phishing, and suspicious. Additionally, the Frequent Rule Reduction algorithm (FRR) has created a greedy selection algorithm (GSA) to find the best subset of rules with the most accurate prediction of phishing websites [18]. An artificial neural network-based anti-phishing model for a company has been put up by Sankhwar et al. (2020). The Fuzzy Inference System is used to construct the URL categorization procedures and provide results with erroneous data on social attributes utilizing two ANNs (Levenberg-Marquart and feed-forward backpropagation). To reduce phishing cyberattacks, this methodology is effective at figuring out if emails are known or unknown phishing emails [19]. In order to learn how to imitate them, Tharani and Arachchilage (2020) displayed and discussed a collection of phishing URLs.

They may entice users to carry out harmful actions like clicking on malicious links. On a phishing dataset, IG and Chi-Squared feature selection approaches are utilized along with dual machine learning (ML) techniques [20]. By depending on URLs on the mobile device, Haynes et al. (2021) recommend using phishing detection-based lightweight algorithms. Only phishing websites are detected by deep transformers (BERT and ELECTRA) [21]. Spear phishing, clone phishing, and whaling attacks are the three main types of phishing cyber-attacks. The first type monitors user and victim information to maximize the likelihood of a successful assault, targeting individuals or numerous organizations. The second kind of attack spreads from a victim who is already infected and is historically and properly identified by getting cloned or mirror emails with attachments. The third kind of phishing is spear phishing, designed for top executives and other high-rated individuals. An overhead manager is used to compose the text that is sent to the destination [22], [25].

The different forms of cyber dangers and the measures taken to prevent them

1. **Ransomware**

This is a form of malware (malicious software) that attempts to encrypt (scramble) your data and then extort a ransom to release an unlock code. Most ransomware is delivered via malicious emails. Follow these key steps to protect your company.

• Staff awareness: staff should be wary of unsolicited emails, particularly those that ask for a prompt response.
• Malware protection: install and maintain good anti-virus and malware protection software.
• Software updates: keep your applications up to date.
• Data backups: a series of well managed data backups will allow you to recover from an unencrypted version of a file. Make sure you regularly test your backups.

2. **Phishing**

Phishing is an attempt to gain sensitive information while posing as a trustworthy contact, for example a bank or online service. Spear phishing is a highly targeted attempt to gain information from an individual. Phishing emails may look completely convincing, often with faultless wording and genuine logos. There is a form of spear phishing, where a fake email from a CEO applies pressure on a CFO into making an urgent payment, this has become known as Whaling. It is worth considering ways to add additional safeguards to protect the identity of CEOs and CFOs to prevent impersonation. Here are a few steps you can use to protect yourself.

• Keep in mind that companies simply do not ask for sensitive information.
• Be suspicious of unexpected emails.
• Make use of anti-malware software.
• Make sure you have spam filters turned on. Check them regularly in case they have accidentally trapped an innocent email.

3. **Data leakage**

While cyber security in the office may seem challenging, it is essential to understand that security extends well beyond the office these days. The use of smart phones and tablets has become widespread. The ubiquitous and cheap nature of portable storage devices makes them a useful tool for the backup and transportation of data. Those features mean they are also a target for data thieves. The following pointers provide useful first steps to prevent data leaking from your organization.

• Ensure mobile devices have passcode locks.
• Turn on the tracking by GPS and the option to remotely wipe the device if it is lost.
• The use of encryption software is highly recommended when using portable storage devices.
• Keep an eye on your mobile devices and paperwork at all times. A large proportion of crime is opportunistic, taking your eye off your briefcase or smart device could result in a serious loss of data.

4. **Hacking**

Gaining access to IT systems from outside an organization still offers rich pickings for criminals. Traditionally they have attempted to gain access to bank account information or credit card databases. However, intellectual property is another source of value. The use of social engineering, tricking staff into revealing user names and passwords, remains a threat.

• The primary methods to protect yourself from hacking are network firewalls, data access security, procedures for providing and removing access, and user awareness and training.

5. **Insider threat**

If your organization employs staff (full time or as contractors), there is a possibility they could leak data by mistake or maliciously. The potential damage from a leak of documents cannot be underestimated. Use these tips to mitigate the size of any data leak.

• Educate your team to be alert to issues and minimize careless mistakes.
• Limit how much data staff has access to. The principle of least privilege accesses should apply to all IT systems. Only provide staff with the minimum access they need to do their roles.
• Control the use of portable storage devices, such as USB memory keys, portable hard drives and media players.
• Consider using applications in certain situations to monitor staff behavior − who copies what. In all these areas it is key to remember that alongside technology, well-developed processes, procedures and staff training go a long way to protecting your valuable data. For example, if someone leaves your employment, make sure you remove their access. The

reality today is that you should protect your digital assets with the same vigilance as you do when locking your office door at the end of the day [23].

Management of Vulnerabilities in Cyber Security

Vulnerability management is the cyclical practice consisting of identification, classification, remediation, and mitigation of security vulnerabilities. There are three essential elements of vulnerability management. vulnerability detection, vulnerability assessment, and remediation.

1. **Vulnerability Detection**

Vulnerability detection includes the following three methods. Vulnerability scanning, Penetration testing, and Google hacking.

- **Cyber Security Vulnerability Scan**

As the name suggests, the scan is done to find vulnerabilities in computers, applications, or networks. For this purpose, a scanner (software) is used, which can discover and identify vulnerabilities that arise from misconfiguration and flawed programming within a network.

Some popular vulnerability scanning tools are SolarWinds Network Configuration Manager (NCM), ManageEngine Vulnerability Manager Plus, Rapid7 Nexpose, Acunetix, Probely, TripWire IP 360, etc.

- **Penetration Testing**

Penetration testing or pen testing is the practice of testing an IT asset for security vulnerabilities that an attacker could potentially exploit. Penetration testing can be automated or manual. It can also test security policies, employee security awareness, the ability to identify and respond to security incidents, and adherence to compliance requirements.

- **Google Hacking**

Google hacking is the use of a search engine to locate security vulnerabilities. This is achieved through advanced search operators in queries that can locate hard-to-find information or data that has been accidentally exposed due to the misconfiguration of cloud services. Mostly these targeted queries are used to locate sensitive information that is not intended for public exposure.

2. **Cyber Security Vulnerability Assessment**

Once a vulnerability is detected, it goes through the vulnerability assessment process. What is a vulnerability assessment? It is a process of systematically reviewing security weaknesses in an information system. It highlights whenever a system is prone to any known vulnerabilities as well as classifies the severity levels, and recommends appropriate remediation or mitigation if required.

The assessment process includes:

- **Identify vulnerabilities:** Analyzing network scans, firewall logs, pen test results, and vulnerability scan results to find anomalies that might highlight vulnerabilities prone to cyber-attacks.
- **Verify vulnerabilities:** Decide whether an identified vulnerability could be exploited and classify its severity to understand the level of risk
- **Mitigate vulnerabilities:** Come up with appropriate countermeasures and measure their effectiveness if a patch is not available.
- **Remediate vulnerabilities:** Update affected software or hardware wherever possible

3. Vulnerability Remediation

To always be one step ahead of malicious attacks, security professionals need to have a process in place for monitoring and managing the known vulnerabilities. Once a time-consuming and tedious manual job, now it is possible to continuously keep track of an organization's software inventory with the help of automated tools, and match them against the various security advisories, issue trackers, or databases.

CONCLUSION

The number of phishing websites has been rapidly increasing as more advanced phishing kits are made available. These kits are used by the attackers to spread the fake pages. Also, there is a lot of overlap between the chosen qualities, which causes conventional algorithms that rely on isolated features to misclassify objects in an impressive way. These distinctive traits are something that phishers always attempt to exploit. Mechanisms for phishing detection must be created in order to enhance the classes. The strategies for preventing this cyberattack are also explored in detail.

REFERENCES

1. Jordà, Ò., Schularick, M., & Taylor, A. M. (2016). The great mortgaging: housing finance, crises and business cycles. Economic policy, 31(85), 107-152.
2. Zhao, J. Y., Yan, J. Y., & Qu, J. M. (2020). Interpretations of "diagnosis and treatment protocol for novel coronavirus pneumonia (trial version 7)". Chinese medical journal, 133(11), 1347

3. Zhou, H., Chen, X., Hu, T., Li, J., Song, H., Liu, Y., ... & Shi, W. (2020). A novel bat coronavirus closely related to SARS-CoV-2 contains natural insertions at the S1/S2 cleavage site of the spike protein. Current biology, 30(11), 2196-2203.
4. Wu, C., Liu, Y., Yang, Y., Zhang, P., Zhong, W., Wang, Y., ... & Li, H. (2020). Analysis of therapeutic targets for SARS-CoV-2 and discovery of potential drugs by computational methods. Acta Pharmaceutica Sinica B, 10(5), 766-788.
5. Aven, T. (2013). On the meaning of a black swan in a risk context. Safety science, 57, 44-51.
6. Ravi, R. (2020). A performance analysis of Software Defined Network based prevention on phishing attack in cyberspace using a deep machine learning with CANTINA approach (DMLCA). Computer Communications, 153, 375-381.
7. Vijayalakshmi, M., Shalinie, S. M., & Yang, M. H. (2020). Web phishing detection techniques: a survey on the state-of-the-art, taxonomy and future directions. IET Networks, 9(5), 235-246.
8. Trisanto, D., Rismawati, N., Mulya, M. F., & Kurniadi, F. I. (2020). Effectiveness undersampling method and feature reduction in credit card fraud detection. Int. J. Intell. Eng. Syst, 13(2), 173-181.
9. Rajitha, K., & VijayaLakshmi, D. (2016). Oppositional cuckoo search based weighted fuzzy rule system in malicious web sites detection from suspicious URLs. Int J Intell Eng Syst, 9(4), 116-125.
10. Rao, R. S., Pais, A. R., & Anand, P. (2021). A heuristic technique to detect phishing websites using TWSVM classifier. Neural Computing and Applications, 33(11), 5733-5752.
11. Tan, C. L., Chiew, K. L., Yong, K. S., Abdullah, J., & Sebastian, Y. (2020). A graph-theoretic approach for the detection of phishing webpages. Computers & Security, 95, 101793.
12. Ali, W., & Malebary, S. (2020). Particle swarm optimization-based feature weighting for improving intelligent phishing website detection. IEEE Access, 8, 116766-116780.
13. Aljofey, A., Jiang, Q., Qu, Q., Huang, M., & Niyigena, J. P. (2020). An effective phishing detection model based on character level convolutional neural network from URL. Electronics, 9(9), 1514.
14. Wei, W., Ke, Q., Nowak, J., Korytkowski, M., Scherer, R., & Woźniak, M. (2020). Accurate and fast URL phishing detector: a convolutional neural network approach. Computer Networks, 178, 107275.
15. Feng, J., Zou, L., Ye, O., & Han, J. (2020). Web2Vec: Phishing Webpage Detection Method Based on Multidimensional Features Driven by Deep Learning. IEEE Access, 8, 221214-221224.
16. Anupam, S., & Kar, A. K. (2021). Phishing website detection using support vector machines and natureinspired optimization algorithms. Telecommunication Systems, 76(1), 17-32.
17. Mahdavifar, S., & Ghorbani, A. A. (2020). DeNNeS: deep embedded neural network expert system for detecting cyber attacks. Neural Computing and Applications, 32(18), 14753-14780.
18. Kumar, M. S., & Indrani, B. (2021). Frequent rule reduction for phishing URL classification using fuzzy deep neural network model. Iran Journal of Computer Science, 4(2), 85-93.
19. Sankhwar, S., Pandey, D., Khan, R. A., & Mohanty, S. N. (2021). An anti-phishing enterprise environ model using feed-forward backpropagation and Levenberg-Marquardt method. Security and Privacy, 4(1), e132.
20. Tharani, J. S., & Arachchilage, N. A. (2020). Understanding phishers' strategies of mimicking uniform resource locators to leverage phishing attacks: A machine learning approach. Security and Privacy, 3(5), e120.
21. Haynes, K., Shirazi, H., & Ray, I. (2021). Lightweight URL-based phishing detection using natural language processing transformers for mobile devices. Procedia Computer Science, 191, 127-134.
22. Barraclough, P. A., Fehringer, G., & Woodward, J. (2021). Intelligent cyber-phishing detection for online. Computers & Security, 104, 102123.
23. https://www.icaew.com/-/media/corporate/files/technical/business-and-financial-management/smes/bas-for-pba/top-five-cyber-risks.ashx.
24. https://intellipaat.com/blog/vulnerability-in-cyber-security/#:~:text=A%20vulnerability%20in%20cyber%20security%20refers%20to%20any%20weakness%20in,through%20the%20points%20of%20vulnerability .
25. Muhammad A. B., Adamu H., Mukhtar I. B., Usman S. M. (2022). Online Attacks Types of Data Breach and CyberAttack Prevention Methods, Current Trends in Information Technology, 12(2), 21-26.

CITE AS
Muhammad A. B, Aminu Ya'u, Sirina F. Ibrahim, Bello A.Imam, M. Aliyu Yusif, Abubakar S. M, Aliyu M. Lawan, & Abdulmuhamin M. (2023). Management of Vulnerabilities in Cyber Security. Global Journal of Research in Engineering & Computer Sciences, 3(2), 14–18. https://doi.org/10.5281/zenodo.7779507