International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Cyber Security Current State, Processes, Roles, and Operating System

Gbaden, Terlumun[1]; Uyoo, Stephen[2]
[1]Computer Science Department, Joseph Sarwuan Tarka University, Makurdi, Nigeria
[2]Directorate of Information & Communication Technology, Joseph Sarwuan Tarka University, Makurdi, Nigeria
Email: [1]gbaden.terlumun@uam.edu.ng, gbaden2014@gmail.com, [2]uyoo.stephen@uam.edu.ng, donesteve09@gmail.com

Abstract**—***As cyber attacks are growing exponentially, Cyber security knowledge has become essential in today's world. At a prominent level, the responsibility of cyber security specialist is to protect it's infrastructure, user equipment, networks, and data. Cyber hits come in diverse forms. All sectors can be the main focal point of any attack; as a result, procedures must be in place to curtail the impact of any form of attack. This paper intends to identify the current state of cyber security preparedness, Processes, Roles, and Operating System (OS) Security. the preliminary results indicates that cyber security is at "maturing stage", the paper also proposes an immediate solution to increase cyber security awareness through constant cyber security tutoring programs across all domains to serve as an initial phase for ever-increasing the awareness of cyber security attacks.*

Keywords**—** *Cyber Security, Awareness Level, Nigeria, Cyber Attacks, Intrusion, Cyber Threats, Masquerading*.

I. INTRODUCTION

Any form of data (information) stored in cyber-space is subjected to intrusion; it includes government, individual, financial, and military. Security breaches occur as a result of the new invention of either hardware or software. This new device results in new vulnerabilities. (Garba, et al., 2020). The emergence of cyber security is at its prime as the transition of the computer, any information that is transmitted through the internet is at risk of getting compromised without the knowledge of the sender. The materialization of cyber security is subjected to the expansion of the cyber domain in the 1950s (Tikk-Ringas, 2015).

Cyber security is essentially about entities, processes and technology operating together to cover the full range of threat prevention, risk impediment, deterrence, foreign intervention, incident response, buoyancy and recovery policies and practices, including functions of computer networks, information preservation, enforcement agencies, and so on. It is a collection of technologies, procedures, and practices designed to secure networks, computers, programs, and information from attack, theft, harm, alteration, or unauthorized access. It can also be attributed to as protection for information technology.

Cyber security is a technique of defending organization assets, through the identification of threats that can compromise vital data stored in the organization systems, it also involves the fortification, identification, and responding to threats. The use of cyber as cyber power as weapon has also been used by the Russian in 1980s when it attaches 400 military computers include the pentagon computers, this resulted to new demission being added to the research of cyber security (Dunn, 2012; Rueter, 2011; Taylor, et al., 2014).

The 21century is regarded as the concentration stage of cyber security because it provides solid premises for the advancement of new theories in cyber security as the world becomes more connected. Sometimes the world cyber is not only refers to as technology but also a political idea that is cantered in several technologies. The functionality of Cyberspace has been as a financial souk, political background, and also as social sight by utilizing the prospect of the sector (Moody et al, 2018: Weishaupl, et al., 2018). The cyber security sector emerged as a result of Robert Morris testing the worlds' network defenselessness in 1980 when he uses a virus he created to test the size of the internet. His work indicated key loopholes of cyber security in the world of the internet (Healy & Grindal, 2013).

The world is so connected today that people from one continent can see or video chat with others in other continents, also people connect to the internet using their computers, phones, cars, etc., even workforce come to hook up with the outside world as their workplaces. Some organizational operations are performed remotely these days as stakeholders or contractors can converse a thousand miles away from the location of the company. This is possible and makes life easier but at the same time if there is no control over the devices, the infrastructure of the workplace is in danger of cyber-attacks. People now connect to public Wi-Fi to do their business anytime and a huge amount of personal data is being processed over the unprotected medium. An organization is most vulnerable to cyber security attacks because employees can compromise the network of the organization through the connection to the internet.

Langer, (2017). It's a requirement that Organizations should adopt an optimized security measure that works within and outside the network to protect their perceptive information. Also, the organization needs sophisticated machines to detect infrequent behaviors' from the workforces and security levels that protect or control all the access points. (Taylor et al., 2014). Mediums of data transmission channels mostly used are not that secured, therefore, superfluous measures are required to protect the organizational information, and also the workforce behavioral patterns must be guided as well. Cyber security has become a necessity for all to learn the basic activities on how to protect their personal information (Garba et al., 2020).

The Development of Cyber Security

Gbaden, Terlumun and Uyoo, Stephen, "Cyber Security Current State, Processes, Roles, and Operating System," *International Research Journal of Advanced Engineering and Science*, Volume 8, Issue 1, pp. 249-257, 2023.

Intense changes has been undertaken in Cyber security recently, massive deals are put in place to see how to intensify security to ensure that the organization's sensitive information, data, and other assets are properly secured. In 1980s and the beginning of 1990s security was highly focused on protecting users' computers and operating systems, it aims at shielding the devices against malicious code or viruses which can affect the working of the computer. After the materialization of the internet, organizations' enterprises started to work on how to secure and establish network connectivity. The idea of being connected to a network introduced much vulnerability that could be misused by a hacker. The hacker aims at accessing vital information via a site or system or channel where no one had an idea of protecting to reach or infect a system through the use of malware or any other mechanisms. This hacker can attack individuals, organizations, state, and a nation just to get access to critical information using a complicated method or by buying a program on the deep web for the exploitation of vulnerabilities to obtain that information. Many organizations have tried to protect their information using technological approaches.

Peppard & Ward (2016). Introduce the following technologies to protect organizational information:

- *Intrusion Detection System (IDS):* These systems are used to detect and monitor unauthorized accesses in a network (Effendy, et al., 2017).
- *Intrusion Prevention System (IPS):* Monitoring traffic by these systems to detect attack vectors in a network is prohibited by blocking them. Honey pot is the best example, where venerable computers that do not have critical information are designed to attract and detect hackers (Jin et al., 2013).
- *Security Information in Event Management (SIEM):* Keeping the record for further analysis, launching actions according to the set alerts, and integrating different devices for event correlation and alert generation is actualized by this system.

Hackers always device new ways of attacking, therefore organizations must have strategies to protect their assets as information security evolves. Investments must be done in information security by having security policies designed and included into the premeditated plans of the organization's operations (Moody, et al., 2018). Organizations should always understand and know how much their critical assets worth, business processes, and the kind of likely security breaches vulnerable to an attack. Cyber threats are inevitable and can only be minimized; therefore, organizations must be acquainted with the state of all their security stand at all times to subdue attacks to the bareless minimum. Notwithstanding, an organization must define and integrate security policies into their strategic plans, a risk to critical assets must be quantified, and business continuity must be identified in the event of an attack as well as disaster recovery plans.

Tagarev & Stoianov, (2017). There are major four threats known to cyberspace, which includes:

- Coercion to infrastructures
- Coercion to people's assets
- Threats to organization assets
- Threats to essential goods

In the 1960s, Computer networks developed by the Agency of Research and Advanced Project (ARPA) and the evolution of the third generation of computers in 1965 made the computer more attuned and popular when the internet was developed during the ARPA project interconnecting large computers in the US, from there the awareness of the internet got popular. In the 1980s, due to the convolution of the computer, the UK government created a best practice model for information management which is the Information Technology Infrastructure Library (ITIL), afterward, HP company adopted the best practice and made it popular, in 1995, the term computer security become accepted as the US release control of the internet act and by 1997 Charles Plefeer generated an arrangement of information security properties, which are Confidentiality, Integrity, and Availability (C.I.A). The beginning of policies and standard designs started from 2005 when the ISO/IEC 27000 family of the standard was formed for the information security management system, followed by the International Telecommunication Union of the US generated the ITU-T X.1205 standard as Data Networks for Communication of Open System and Telecommunications Security in 2008 and many others follow like the ISO/IEC 27032 in 2012. These standards make it easy by given that the synopsis of cyber security defined as a set of tools, best practices, guides, policies, security concepts, security safeguards, risk management, action, and technology that can be used to shield the assets of an organization and also the use of cyberspace. The emergent recognition of the internet as one of the basic infrastructures for economic and social development in many organizations has made researchers focus on how to deal with this emerging technology. Cyber security is more technical perceptions that cover the challenges of securing the organizational infrastructures by presenting a solution to the internet security problems, routing, system authentications, and DNS (Denardis & Raymond, 2013).

According to Dunn, (2016), affirmed that most academic invention in the discipline can be divided into these subsequent groups' Formulation of policies, generally in the field of the "think- tanks". Studies focused on the relationship between information and power (Day, 2001) Production of insecurity on the internet based on surveillance practice and censorship (Deibert & Rohozinki, 2010) Studies on the creation of threats in cyberspace (Hansen & Nissenbaum 2009). Lately, concentration has been given to the link between internet governance and cyber security, because cyber security issues have challenged internet governance institutions like jurisdictional conflicts (Mueller & Klein, 2014).

Nigeria Resent Research in Cyber Security

The development of technical structures has been permissible by the internet, cyberspace is part of everyday life and therefore information technology has become an essential factor for innovation. Cyber security is currently a worry to companies due to the continuous breaches which result in the theft of data and destroying critical assets (Johnson, 2016). These attacks can cripple the financial institution and the economy as well. Africa is growing in consumer credits, but

lack of data protection serves as a major setback (Makulilo, 2016). Only 16 nations in the world have data protection, including Nigeria, which is particularly bad because it is one of the top 10 countries in the world for reported cybercrimes and the African Union recognises 55 countries while the UN only recognises 54. Cybercrime includes any illegal conduct that makes use of the internet as a medium as well as any illegal action that makes use of a computer to obtain unfair advantages. Cybercrimes have long rumpled the reputation of Nigerians worldwide (Ibikunle & Eweniyi, 2013) these threats have increased exponentially as the dramatic rise of mobile communication, the drive of the banks in the country to introduce careless economy, using internet technology in the government and online trade.

Andoh, et al., (2014), they recommended that elected and state governments, the public organization well as privates all have parts to play through the enactment, the reception of international standards, introducing education about information and intrusion crusade to further deal with cyber threats and ensure zero resilience in the abuse of the internet. Right now, the most used cybercrime that goes unrestricted is electronic fraud, which is equipped for taking all individual or cooperate bank account and sent a wrong flag against the monetarily related incorporate drive.

Orji, (2012). The word "419" is associated with Nigerian Computer Advanced Fee Fraud. The CBD recent introducing of Bank Verification Number (BVN), to reduce the number of account individual or organization can manage, and the creation of the Nigerian Electronic Fraud Forum, Nigerian Interbank Settlement System (NBISS), and Deposit Money Banks (DBM) all in the name of protecting customers financial transactions, but scammers turn out to be faster in reaching their goals by defrauding the clueless customer of banks and other financial instruction in the country billions of naira. A critical part of cyber security is communication, which is lacking in Nigerian organizations. the power of cybercrime hacking networks depends on their need to share privileged data by exposing or selling to organizational rivals who restrict correspondence with their companies due to fear of rivalry. The next section will explain more on the issues reported regarding cybercrime activities and how much losses they cost to both government and organizations.

Organizational Common Cyber Types and Attacks

An amount of contexts, from enterprise and organization to mobile computing, cyber-security can be divided into a few common classes.

- *Information Security:* This class of cyber-security preserves data confidentiality and authenticity, in both transit and storage.
- *Application Security:* It aims basically on keeping threats free from apps to computers. An application that is compromised may grant access to the information it is supposed to protect. In the design stage, long before a program or system is implemented, effective protection starts.
- *Operational Security*: The operational protection requires processes and decisions for managing and securing data assets. When accessing a network, the permissions users have and the mechanisms that decide how and where data can be stored or exchanged all come under this umbrella.
- *Network Security*: This is the practice of protecting a network of computers from hackers, whether targeted attacks or opportunistic malware.
- *Company Continuity and Disaster Recovery:* It explains how an entity reacts to an incidents of cyber security or some other event that causes processes or data to be lost. In order to return to the same operational capability as before the incident, policies of disaster recovery determine how the company recovers its operations and records. Continuity of business is the strategy on which the company falls back when attempting to survive without such resources.
- *Education for End-users:* People are the most potentially harmful cyber security factor. By ignoring to follow the ethical security policies, anybody can unintentionally implement a virus to an otherwise secure system. Informing people to delete potentially malicious unwanted emails, avoiding to plug in unknown USB drives, and several other valuable points is very important for the protection of any organization.

Korte, (2017), Annually, $500 billion was lost by cybercrime and the numbers continued increasing as institutions continue to adopt the internet in carrying their business processes. The most wieldy attacks are the return of Ransom ware.

Ransom ware is a style of cyber-attack that is known as information hijacking, where the hacker uses a code to get access to the organization's server and then demand a payment to give access back to the data if payment is not made the hacker destroyed the data or sell it online (Wueest, 2017; Richardson & North, 2017). Other attacks include Advanced Persistent threats. Nigerian financial organizations have used these chances to grow their e-business through the use of the internet and mobile applications, which has also lead to an increase in cybercrimes. The most recent cybercrime using mobile devices in Nigeria is the SMS sim splitting or swapping technique, where a hacker takes over users' identity after gaining access to their cell phones. The hacker then downloads financial applications and log in using stolen credentials through a social engineering approach.

Customers, especially those that have less knowledge of the cyber world or the financial institutions with sole to sell or distrust transactions are mostly vulnerable and aimed at by the subsequent attacks.

- *Malware:* Malware is a malicious program designed, installed and executes without the knowledge of the owner. This attack commonly used to get personal data and electronic benefits, it can be operated remotely and automatically.
- *Browser Hijacker:* This is a program designed to make changes to the configuration of the web browser. For example, changing the normal home page of a website to an advert page.
- *Dialer:* Its a concealed program designed to connect internet through a modem thus allowing the hacker to make calls to phones at a special rate.

- *Backdoor:* this is an intended program designed to open computer access to the malware developer, ignoring the main or genuine process of authentication. It gives easy access to the hacker to remotely control the hacked device.
- *Spyware:* spyware is an application program designed intentionally to collect personal or organizational data. This application aims at getting information to sell to a third party.
- *Keylogger:* This application is used to store all keystrokes so that hackers can capture sensitive information like banking details or passwords.
- *Masquerading:* This is a situation where a hacker overrides the identity of any system to gain access to the resources stored on the system. The hacker can impersonate a base station network by emitting a signal of more power than the actual legitimate user.
- *Denial of service / Distribute Denial of Service (Dos/DDoS):* Dos/DDoS is a most commonly used cyber-crime where the hacker makes network service unreachable or unavailable to the legitimate users. It mostly affects financial organizations, airlines, and other reputable organizations. It also makes a normal site temporary out of service due to the amount requests sent to the server, which makes it busy.
- *Phishing:* Phishing is a program designed such that it deceives users to provide their access keys to a malicious site, thinking is a legitimate site. Phishing is an elaborate attack and is often exposed as a clear example of so-called social engineering, Miedema (2018).
- *Worm:* Worm is a malicious program that replicates itself and spread all over a network. It worm has the same agenda as the virus.
- *Viruses:* Virus is a nasty program designed to infect other files on the system, change or make them useless, it becomes effective when the user activates it by clicking on the file, some of its purposes include: getting the password, deleting all computer files and denial of service.
- *Eavesdropping:* Here the hacker obtains information from the communication channel, where he is neither the emitter nor the receiver. It is referred to as a passive attack. The information obtained can be used to perform masquerading attack.
- *Trojan:* Small program hidden in another program. The program gets installed by the user without noticing it and it performs various activities without the consent of the user. (Aliyu, et al, 2014).

These are some of the most frequently used cyber-attacks hacker indulge in to defraud financial organizations and enterprises. Organizations normally focus on protecting their networks and critical assets, especially customers or employees in financial institutions are left out of the loop and often neglected, unknowingly they might be the weakest link to the organization networks. High dependence on the internet makes it paramount for everyone to be responsible in protecting their data, organizations should educate their employees and consumers about the risk and measure to protect their personal information and also have knowledge of the most recent cyber-crimes.

Importance of Cyber Security

A digital world that recognizes the vulnerability of our personal confidential information on government networks to online banking, where data is kept on computers and multiple devices connected together. Confidential information, be it financial information, private information, intellectual property, or other forms of data for which unauthorized access may have negative implications, may be part of that data.

Cyber-crime is now a global concern such that the worldwide economy may be affected by hacking and other security threats. Businesses and organizations convey delicate data over the network along with other devices, cyber security describes the fortification of that data and the systems used to process and store it. As cyber attacks increases, organizations, businesses ought to take drastic measures to guard their confidential business data and personal information, especially those dealing with information related to national security, health, or financial records. (Miedema, T. E. 2018).

The Importance of Cyber Security in an Organization

The increase in personal computers in day-to-day life has brought about added security threats. The probability of a network-enabled cyber-attack to companies has risen exponentially. At whatever point on the internet, threats can take place where there is a possible weakness that hackers can exploit either through a phishing email message, a spoof posting on a social media, or maybe even a compromised hardware. The capacity for attack and destruction rises as the number of devices increases.

The increase of cloud services and cloud computing, extra security threats has also increased. A corporate cloud computing study view that, 28 percent as part of the IT technology, among all enterprises would rely on private cloud computing platforms. This is in evaluation to the nearly 32 percent who would use the collective space or cloud computing hybrid model. A Cisco review of the cloud infrastructure industry showed that in the coming years, 83 percent of all data center traffic will be centered in the cloud. Mutual with the additional budget increases cited in the Forrester Study, this growth would further accelerate the need for improved cyber defense initiatives in the coming years. (Bernardo, et al., 2007)

Fortification of Data Proficiency in Organizations

Despite the advancement of technologies, the capacities of the hackers also overshadow the competence of security personnel within organizations. The evidence of this is the effective number of attacks. Skilled and well-trained engineers are in high demand with the amplified value of cyber protection. Organizations require persons who have learned the skills to secure networks and guard against attack, disruption and/or unwanted right of entry to infrastructure, computers and records. (Cerpa, et al., 2001)

Cyber Security Enlisting Problems

Lack of security proficiency is a dilemma that is being faced. While budgets are generous, Chief Information Officer's (CIOs) still struggle to find trained workers with advanced security skills. Cisco's Chief Security Officer John Stewart said,

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

"The industry is short of over a million security professionals worldwide." Cyber security is facing a enlisting crisis. Organizations are desperate to locate and fill key personnel roles with trained security professionals. More than 3,400 Information System Audit and Control Association (ISACA) members surveyed by the ISACA State of Cyber security, 27 percent of cyber security experts say they cannot find qualified applicants, leaving employment unfulfilled, and another 14 percent are unsure whether they can fill the vacancies. 50 percent of companies expected to raise their cyber security budget, according to the same report.

About 3.5 billion cyber security positions are assumed and expected to be unfilled in the nearest few years, due to skill shortages and market needs. As cloud storage and technology continue to expand and security threats rise, the need for qualified professionals will only increase. A research by Burning Glass Technologies shows that security work posts have risen by 74 percent and that is because of the lack of skills in the industry today, security jobs take nearly 24 percent longer to fill than normal IT jobs. Information Technology (IT) security crisis comes at a time when employers in the government and private sectors are looking to fill vacancies in the wake of cyber security attacks, data breaches, vulnerable stealing of resource, and compliance mandates are being expanded. With the emergence of new vulnerabilities and Distributed Denial of Service (DDoS) attacks that have disrupted internet access in recent years, as qualified professionals in cyber security, cloud computing, and other strategically critical IT positions, more and more professionals are expected to be on alert. (Luis, 2012).

Cyber Security Training Improvement for Officials

Specific contemporary teaching methods may not work for every learner, the gaps in the cyber security field require skills to be filled which are highly lacking. Therefore, it is imperative to use a learner-centric method which will be able to work for everyone and everyone will be able to take the full benefit of the opening. Several ways are considered to assure that good cyber security is practiced by an organization. One of the best ways is to inform and educate workers on the significance of cyber security and the rewards of keeping the business safe. Cyber security services presented by a reputable cyber security firm are another product company use.

A company that has perceptive data and information they cannot afford to lose, cyber security is fundamental. Many enterprises are unprotected to threats when it falls to hackers. The clarification for this is partially due to the lack of proficiency ability of staff and the lack of sufficient service for cyber security. Companies continue to defend themselves from threats and a great deal can be helped by education. When workers are conscious of the worth of cyber security, they will do their best to achieve protection for their business. (Gabra, et al. 2020).

Effective Cyber Security Strategies

Here are few procedures which are considerably possible precautions that can be taken to prevent network from major network attacks:

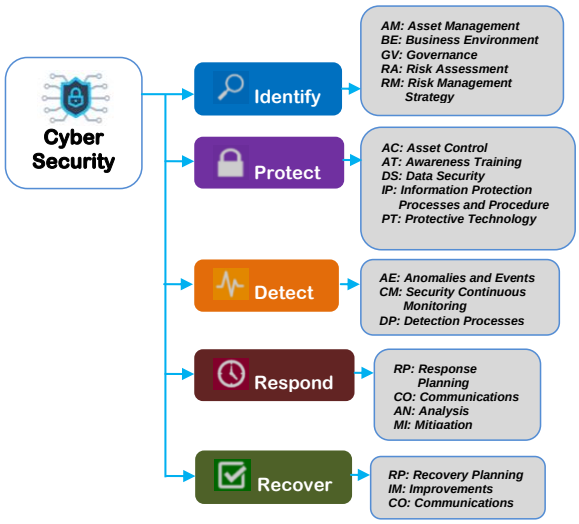
Passwords Handling Strategies

Everyday management of passwords is very important and should be addressed by daily personnel in all security training. A safe collection of passwords is at the core of any secure system. This procedure aims at providing the most vulnerable data with security. It gives only a small number of individuals who have access to the data inside large organizations who have requirements to keep customer or client data secure. This procedure is designed to provide someone who would usually not have these permissions with short-term access.

Some examples of Privileged Password Management such as; Keeper Password Manager & Digital Vault, LastPass, Dash line, Bit warden Premium are measures for authorization, documentation, and safe access control throughout the process. It is handled by the appropriate IT specialist-IT manager or risk manager-and aims to provide a non-intensive way to provide high-level protection. (Chawathe, et al., 2003)

Day to Day Responsibilities for Network Administrator

The network administrator is the first line of protection against malware threats most of the time and plays a vital role in protecting the enterprise. The network administrator is also the unlikely hero of organization activities. This checklist is to list a set of main daily tasks undertaken by the network managers and provide room for tracking those duties. As a result, in order to cover the inveterate rudiments, a network administrator will be able to run the checklist each day and cycle through the various tasks posed. The network administrator may report as much information as they want with any of the tests they perform, in the inclusion of type fields in the checklist. One of the examples of it is Process Street templates which changes over time to better address the needs of the everyday life of the network administrator, because of the highly editable existence made with consideration of machine learning to provide better experience. (Greenstein, et al., 2003).



Cyber Security Framework

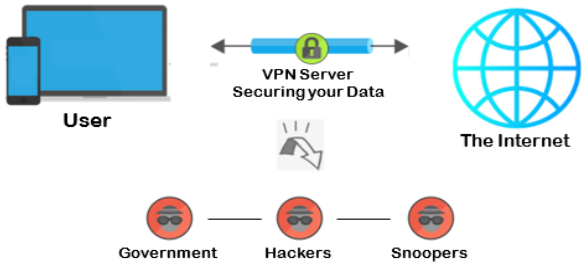
Use of Virtual Private Network (VPN)

Virtual Private Network is a service that creates a safe, encrypted online connection that has turn out to be progressively more popular to use. Some IT security experts

Gbaden, Terlumun and Uyoo, Stephen, "Cyber Security Current State, Processes, Roles, and Operating System," *International Research Journal of Advanced Engineering and Science*, Volume 8, Issue 1, pp. 249-257, 2023.

recommend that everyone should use it to protect their personal security. However, for diverse reasons, this method utilizes a VPN. It becomes a threat to authorize remote access while operating inside a safe office network. For business trips and other related conditions, remote access to the office network is basic. In this process, a VPN is set up on the laptop of a staff, which enables the staff to connect remotely to the office network.The checks and balances that come with using a method to handle configuration are built in to this method.

Both the IT department and the HR department are examples would have collected information on who has remote access to office networks as part of the security precautions. This reduces exposure to threats that might otherwise have been triggered by bad communication practices. Some of the best examples of VPN are Express VPN, Surf Shark, NordVPN, ProtonVPN. (Bernardo, & Pinto, 2004).



Virtual Private Network Architecture.

The Use of Diverse Servers for Email

The first common ways someone will try to intrude into your business is by email. Phishing attacks and other falsified attempts to compromise the safety of an email depend on a good technological resilience as well as a high degree of professional training to combat them. There are many steps to take from a technological point of view to protect emails:

1. *Enable SPF (Sender Policy Framework):* An email authentication protocol that domain owners use to specify the email servers they send email from, making it much complicated for the fraudsters to spoof sender information.
2. *Enable DKIM (Domain Keys Identified Mail):* A protocol that allows an organization to take responsibility for transmitting a message by signing it in a way that mailbox providers can verify.
3. *Enable DMARC (Domain-based Message Authentication Reporting and Conformance):*This is an email validation system that detects and prevents email spoofing.
4. *Enable DNSSEC (Domain Name System Security Extensions):* It's a set of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP)

There is eagerness to set up robust training processes for the workers beyond the technical steps. No matter how many technological strategies you put in place, you will be faced with problems if people keep unintentionally downloading malware. (Vidhya, 2014).

Architectural Framework for Cyber Security

Network security architecture, also known as Cyber-security architecture, is a structure that describes a computer network's organizational framework, functional behavior, policies and principles, covering both security and network features. The architecture of cyber-security is the way in which different components of cyber infrastructure or computer system are synchronized, coordinated and incorporated. One part of the overall architecture of a system is a cyber-security architecture framework. It is designed and developed to provide instructions for the whole product or system during the design. Security architecture helps to place security controls and countermeasures in breach and how they contribute to the company's overall system structure.

The main intend of these controls is to protect the quality characteristics of critical system, such as honesty, confidentiality and availability. It is also a synergy of software and hardware expertise with programming skills, analysis skills and policy creation.

A security architect is a person who anticipates future cyber-threats and designs mechanisms and systems quickly to avoid them. Most companies are vulnerable to cyber-security threats, but you can introduce and track the network security systems of your business via a cyber-security architecture plan. A structure for cyber-security architecture places all of your security measures against some kind of malicious actors and how they contribute to the overall architecture of

systems. In defending the enterprise from external attacks, various components of cyber-security strategies such as firewalls, antivirus programs and intrusion detection systems play a huge role. Organizations should develop a comprehensive security framework that incorporates these various components for the networks in order to manage and maximize these security tools as well as already defined and usable policies and procedures (Aman, & Aniket, 2020).

Cyber Security Architecture.

Cyber Security Architectural Purpose

The cyber-security design simply intends to ensure that company's main network architecture, which including essential applications and confidential data, is completely secured from any existing or potential threats and breaches. In

Gbaden, Terlumun and Uyoo, Stephen, "Cyber Security Current State, Processes, Roles, and Operating System," *International Research Journal of Advanced Engineering and Science*, Volume 8, Issue 1, pp. 249-257, 2023.

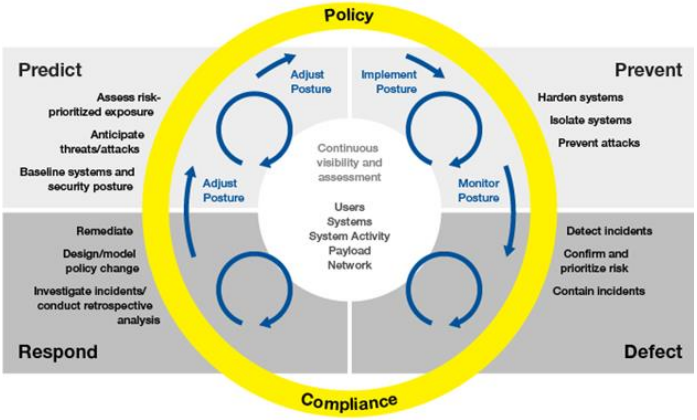
International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

order to provide a solution efficiently and rapidly, it is important that you thoroughly understand the different weak points in the system. The easiest way to find the weak point of a system is to hire the services of an architect of cyber-security. To efficiently protect the confidential data and critical applications, a cyber-security architect will thoroughly analyze surface vulnerabilities for various network topologies and cyber-attacks. (Sunit, & Nina, 2011).

The cyber-security architecture key successful objectives are:

1. To ensure that all confidential and sensitive information is strongly encrypted and, during transition, subject to end-to - end encryption techniques.
2. Using countermeasures like Moving-Target Defences, all cyber-attacks are actively tracked, mitigated, and countered.
3. To ensure the minimization, prevention, hiding or dynamic of all cyber threats.
4. Secretly stored, to ensure that cyber-attack surfaces should be relatively limited in scale, so that they are stealthy in moving to threat objectives and difficult to detect and infiltrate cyber-attacks.

Why Cyber-Security Architects are Important In detecting possible threats, cyber-security architects are particularly qualified. Computer and network systems are properly understood to design security architecture plans, execute these plans, and oversee the consistent execution.



A Four Stage Adaptive Security Architecture

Security Virtualization

Virtualization is the technique of operating a computer on a single physical hardware resource with several virtual instances. It is also the process, procedure and strategy that assures that the virtualized hardware infrastructure is steady and protected.

Virtualization, while enhancing scalability and workloads, it centralizes administrative activities and contributes to network infrastructure reduction, lower OPEX, and ease of management. Virtualization, however, also creates security issues that cannot be effectively defended against by physical security systems:

- File sharing is not safe between hosts and guests.
- Weakened isolation between components such as guest OSs and software, hypervisors, hardware.
- Consolidation of multiple servers increases the risk that a compromise can multiply from applications on the same host.
- Intrusion Prevention Systems (IPS), virtual network infection is triggered by malware affecting physical and virtual machines.
- Unauthorized access, denial of service, and vulnerabilities provide other security risks.

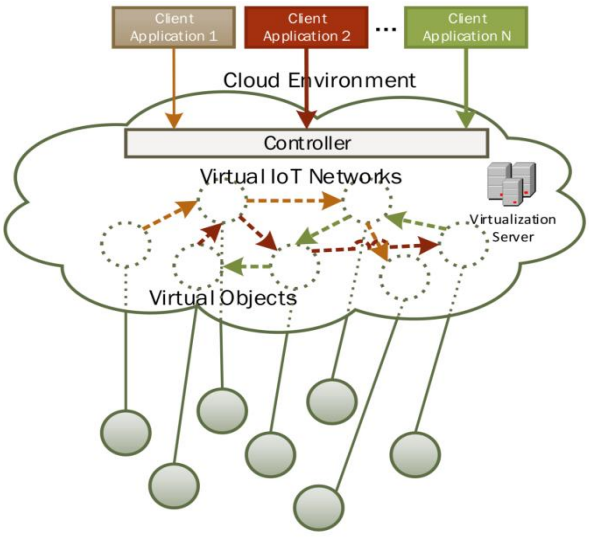
Many companies may not know that they may be vulnerable to these forms of attacks and data loss by using their current legacy protection solutions.

Need for Virtualization Security

Virtualization for protection serves as a barricade to a network's protected perimeter access. As an extra managed service, it offers dedicated security services and assured traffic remoteness within the cloud, along with customizable firewall controls. Enterprises and service providers will make the most of their investment in virtualization to build an authentic security perimeter, offering tenants and service subscribers dedicated security services within a cloud construct.

Segmentation Isolation of Virtualization Security uses virtual security network installed software to control workloads, processes, and VM access. Security policies for access to virtual networks and workloads may also be handled by security. (Luis, 2012).

Two common concepts are considered in virtualized protection, they are Segmentation and Isolation. Segmentation only specified applications and users accessibility to a particular network resource. In addition to physical protection equipment, this can be done with virtual applications. Isolation enables discrete programs and workloads to run independently on the same network, its another important approach. Segmenting the portion of the network dealing with confidential information, such as credit card data, will be an instance of this.



Virtualization Security Architecture

Gbaden, Terlumun and Uyoo, Stephen, "Cyber Security Current State, Processes, Roles, and Operating System," *International Research Journal of Advanced Engineering and Science*, Volume 8, Issue 1, pp. 249-257, 2023.

Segmentation can be built into virtual network fabrics with the advent of Software-Defined Networking (SDN). For instance, depending on policies allocated to different applications, an SDN network may be set up to have several secure layers. The micro segmentation approach is another trend in SDN protection, which is driving protection virtualization, whereby additional layers of security can be introduced at the level of application and workload. (Nikhita, &Ugander, 2012)

An approach that is prevalent in today's virtual infrastructure known as Micro Segmentation. Micro segmentation applies workloads and applications with unique security policies, in a way that can allow security features to monitor workloads across the network if they are relocated.

So far as more applications are running in the cloud and networks are gradually virtualized, security virtualization is an obvious development that is likely to last for several years. It will require new types of security software that can be installed to track and control virtual infrastructure data security policies. (Hartung, et al., 2006)

III. Conclusion

The above review has indicated how much cyber security knowledge is very crucial in all aspect of life, precisely in Nigeria, opinions by various experts in the field shows that Nigeria has policy and strategy to combat cyber Security but most organization are not adhering to it, due to lack of proper awareness to the employees on the issue of a cyber security threat, also the general public as a whole are less or have no knowledge on the dangers of cyber-attacks and tend to ignore it. This research also indicated the way forward which is "education on cyber security" i.e. proactive cyber security awareness programs are needed to be implemented all over the section to increase the level of consciousness and minimize basic cyber security attacks. Security virtualization moves security features from hardware to software in security virtualization; segmentation and isolation are both terms used. As more apps run in the cloud and virtual networks continue to develop, therefore, security virtualization is likely to stick around.

References

[1]. Garba, A. A., Siraj, M. M., Othman, S. H., & Musa, M. A. A (2020) Study on Cyber security Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach.
[2]. Tikk-Ringas, E. (2015). Evolution of the Cyber Domain: The Implications for National and Global Security. IISS Publications.
[3]. Dunn Cavelty, M. (2012). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. (ND). Science and Engineering Ethics, 20(3), 701-715.
[4]. Rueter, N. (2011). The Cyber security Dilemma. MA Thesis. Duke University
[5]. Taylor, R. W., Fritsch, E. J., &Liederbach, J. (2014). Digital Crime and Digital Terrorism. Prentice-Hall Press.
[6]. Moody, G. D., Siponen, M., &Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. MIS Quarterly, 42(1), 285-A22.
[7]. Weishaupl, E., Yasasin, E., &Schryen, G. (2018). Information Security Investments: An Exploratory Multiple Case Study on Decision-Making, Evaluation, And Learning. Computers & Security.
[8]. Healey, J. &Grindal, K. (Eds.). (2013). A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Washington, DC: Cyber Conflict Studies Association. 77
[9]. Langer, S. (2017). Cyber-Security Issues in Healthcare Information Technology. Journal of Digital Imaging, 30(1), 117-125. DOI:10.1007/s10278-016-9913-x
[10]. Taylor, R. W., Fritsch, E. J., &Liederbach, J. (2014). Digital Crime and Digital Terrorism. Prentice-Hall Press.
[11]. Garba, A. A., Siraj, M. M., Othman, S. H., & Musa, M. A. A (2020) Study on Cyber security Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach.
[12]. Peppard, J. & Ward, J. (2016). The Strategic Management of Information Systems: Building a Digital Strategy, 4th Edition (ISBN: 978-0-470-03467-5) 54/504 pages.
[13]. Effendy, D. A., Kusrini, K., Sudarmawan, S. (2017). Classification of Intrusion Detection System (IDS) Based on Computer Network. International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE).
[14]. Jin, H., Xiang, G., Zou, D., Wu, S., Zhao, F., Li, M., & Zheng, W. (2013). A VMM-Based Intrusion Prevention System in Cloud Computing Environment. Journal of Supercomputing, 66(3), 1133-1151. DOI:10.1007/s11227-011-0608-2
[15]. Moody, G. D., Siponen, M., &Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. MIS Quarterly, 42(1), 285-A22
[16]. Tagarev, T., Sharkov, G., &Stoianov, N. (2017). Cyber Security and Resilience of Modern Societies: A Research Management Architecture. Information & Security, 38(1), 93-108.doi:10.11610/isij.3807
[17]. International Organization for Standardization (ISO (2012). ISO/IEC 27032:2012 – Information Technology – Security Techniques – Guidelines for Cyber Security.
[18]. Denardis, D. & Raymond, M. (2013). Thinking Clearly about Multistakeholder Internet Governance. Eighth Annual GigaNet Symposium.
[19]. Dunn, J. (2016) Computational learning of constructiongrammers. Language and Cognition, Available on CJO 2016 doi:10.1017/langcog.2016.7
[20]. Day, R. E. (2001). The Modern Invention of Information: Discourse, History, and Power. Carbondale: Southern Illinois University Press.
[21]. Deibert, R. J. &Rohozinski, R. (2010). Risking Security: Policies and Paradoxes of Cyberspace Security. International Political Sociology: 15-32.
[22]. Hansen, L. &Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and Copenhagen School. International Studies Quarterly: 1155–1175.
[23]. Mueller, M. & Klein, H. (2014). Sovereignty, National Security, and Internet Governance: Proceedings of a Workshop. Syracuse University: Georgia Institute of Technology School of Public Policy.
[24]. Global Cybersecurity Index, (2017) Global Cyber Ranking, retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
Johnson, K. N. (2016). Managing Cyber Risks. Georgia Law Review, 50(2), 547-592.
[25]. Makulilo, A. B. (2016). The Right to Privacy Relating to Credit Reporting: A Critical Review of the Emerging Africa's Credit Reference Market. Journal of Internet Law, 19(9), 3-17.
[26]. Ibikunle, F. &Eweniyi, O. (2013). Approach to Cyber Security Issues in Nigeria: Challenges and Solution. International Journal of Cognitive Research in Science, Engineering and Education:(IJCRSEE), 1(1), 100-110.
[27]. Andoh-Baidoo, F., Osatuyi, B., & Kunene, K. N. (2014). Architecture for Managing Knowledge on Cyber Security in Sub-Saharan Africa. Information Technology for Development, 20(2), 140-164.doi:10.1080/02681102.2013.832127
[28]. Orji, U. J. (2012). Cyber security Law and Regulation (pp. 398-400). Wolf Legal Publishers
[29]. Korte, J. (2017). Mitigating Cyber Risks Through Information Sharing. Journal of Payments Strategy & Systems, 11(3), 203-214.
[30]. Wueest, C. (2017). Financial Threats 2015. Retrieved from Symantec: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/financial-threats-2015. pdf.
[31]. Richardson, R. & North, M. (2017). Ransomware: Evolution, Mitigation, and Prevention. International Management Review, 13(1), 10-21.

[32]. Aliyu, A., Danjuma, S., Dai, B., Waziri, U., & Ado, A (2014). An Integrated Framework for Detecting and Prevention of Trojan Horse (BINGHE) in a Client-Server Network. 3(1), 2319-8753.
[33]. Miedema, T. E. (2018). Engaging Consumers in Cyber Security. Journal of Internet Law, 21(8), 3-15.
[34]. Bernardo, L., Oliveira, R., Pereira, M., Macedo, M., and Pinto, P., (2007). A Wireless Sensor MAC Protocol for bursty data traffic. In IEEE PIMRC'07, 18th IEEE Annual International Symposium on Personal Indoor and Mobile Radio Communications, Sep. 2007.
[35]. Cerpa, A., Elson, J., Estrin, D., Girod, L., Hamilton, M., and Zhao, J., (2001). Habitat Monitoring: Application Driver for Wireless Communications Technology. In 1st ACM SIGCOMM workshop on Data Communication. In Latin America and the Caribbean, ACM Press.
[36]. Luis corrons – Panda Labs. (2012). A Look back on Cyber Security – Trends and Challenges. IJCSMC, VOL. 3, Issue. 2, pg. 549-555
[37]. Gabra, A. A., Sirat, M. B., Hajar, S., & Dauda, I. B. (2020). Cyber Security Awareness among University Students: A Case Study.
[38]. Chawathe, et al., (2003). Making Gnutella-like P2P Systems Scalable. In SIGCOMM'03, the 2003 conference on Applications, technologies, architectures, and protocols for computer communications, ACM Press.
[39]. Greenstein, B., Estrin, D., Govindan, R., Ratnasamy, S., and Shenker, S., (2003). DIFS: A Distributed Index for Features in Sensor Networks. In SNPA'03, 1st IEEE Workshop on Sensor Networks Protocols and Applications, IEEE.
[40]. Bernardo, L., and Pinto, P., (2004). A decentralized location service Applying P2P technology for picking replicas on replicated services. In ICETE'04, 1st Int. Conf. on E-Business and Telecommunication Networks, Vol.1 pp.39-47, INSTICC Press.
[41]. Vidhya P.M. (2014). Cyber Security – Trends and Challenges. IJCSMC, VOL. 3, Issue. 2, pg. 586-590 (ISSN 2320-088X)
[42]. Aman singh and Aniket Gupta, (2020). Cyber Security Roles, Processes and Operating System Security. Retrieved from; https://WWW.researchgate.net/publication/346623641
[43]. Sunit, B. & Nina, G. (2011), Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives. (ISBN: 10-9788126521791)
[44]. *Luis corrons – Panda Labs. (2012). A Look back on Cyber Security – Trends and Challenges. IJCSMC, VOL. 3, Issue. 2, pg. 549-555*
[45]. 46. Nikhita, G.R. &Ugander, G.J.R. (2012) Study of Cloud Computing in HealthCare Industry. International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518.
[46]. 47. Hartung, C., Han, R., Seielstad, C., and Holbrook, S., 2006. FireWxNet: A Multi-Tiered Portable Wireless System for Monitoring Weather Conditions in Wildland Fire Environments. In MobiSys'06, 4th Int. Conf. on Mobile Systems, Applications, and Services, pp.28-41, ACM Press. (Hartung et al., 2006)