In this time of technology, security is a strong necessity for businesses across industries. With every organization now depending on IT infrastructure to carry out their daily business operations, securing their networks makes practical sense.

And because of the evolving landscape of digital infrastructure, it’s natural for businesses to protect IT assets, especially with newer, more sophisticated attacks springing up.

These protection does not come in digital form alone but with physical security systems as well. Physical security is not a new concept, but it must evolve with the technical or cyber security measures.

A drawing of a wall

Description automatically generated

Figure 1 above is the on-site premises of the information technology unit I designed.

At the drive-in entrance to the site is an access control security barrier that allows only registered cars to have access to the parking lot. A security guard mans the driveway to prevent deterrence or any unwanted moving object to cause trouble at the entrance or the parking lot. From the parking lot is another access-controlled entrance where only an authorized and authenticated employee or contractor can pass through. Two security guards man both sides of the main entrance to the technical area where all the information technology facilities are located. The security guards aim to detect any potential intruder with the help of two CCTV cameras at the fence of the entrance gate. Other CCTV cameras are also around the site to help in capturing events. At the entrance to the facility is a door that serves as a physical security tool to cause delay if an intruder can beat the previous security protocols. The door only opens with the flash of an employee ID card with a fingerprint capture that must reconcile with a pre-stored facial image. The door also serves as a response strategy for any possible attack on the facility as it shuts down at any sound of an alarm from the SIEM. The SIEM is a technology that collects event log data from a range of sources, identifies activity that deviates from the norm with real-time analysis, and takes appropriate action. (Microsoft.com, n.d.)

From the technical aspect of the security architecture are various security measures and tools. There is the firewall that monitors and controls incoming and outgoing traffic based on a predefined set of security rules. The DMZ is a symbol that represents a network barrier between trusted and untrusted networks in an organization’s private and public networks. It acts as a protection layer through which outside users cannot access the company’s data while the VPN is a technology that makes a public network behave like a private network. It allows for privacy and security and can make a user to be part of a local network from a remote location.

Inside the facility is a small room with the gateway router that facilitates communication between different networks and can be used for connecting devices and networks together with an internet-facing computer that has an antivirus installed which scan, prevent/detect and remove viruses from the computer. In another room is the server with data backup devices. A server is a device or a software that processes requests sent over a network, responds to them and transmits back to the requestor known as ‘Client’. The server room is equipped with an Intrusion Prevention System (IPS) which is a network security technology that monitors network traffic to prevent and/or detect potential threats and unauthorized access using defined security rules and Security Information and Event Management (SIEM) which is a security solution that helps organizations detect threats before they disrupt business operations. (GeeksforGeeks.com, 2024).

Cyber defense is protecting systems and networks from attacks and threats using a set of tools, methods and components to ensure this.

The components used in cyber defense can be categorized into hardware, software, users and policies. Examples of the hardware components are servers and routers while software components can be encryption, antivirus and VPN. Examples of users are the employees that are trained & given regular awareness and security practitioners who implement policies and regulations.

The defense tools are:

A firewall which is a security device which monitors and controls incoming and outgoing traffic based on a predefined set of security rules.

Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) are network security technologies that monitor network traffic to prevent and detect potential threats and unauthorized access using defined security rules.

An antivirus is a computer protection software that scan, prevent/detect and remove viruses from the computer.

Security Information and Event Management (SIEM) is a security solution that helps organizations detect threats before they disrupt business operations. (Microsoft.com, n.d.)

Encryption protects communication by converting data into an unreadable format and ensures it can only be decrypted and read by authorized persons.

Kali Linux is like a toolbox for cybersecurity tasks. (GeeksforGeeks.com, 2024).

The methods that might be used in cyber defense are network segmentation which divides a network and isolates applications from each other, access control which allows only authorized and authenticated users to have access to a system, Penetration Testing which is a method where an attack is imitated to see vulnerabilities and fix it before it can be utilized, educating employees and system users on best practices, regularly planning incident response and ensuring information systems are frequently updated and have latest patches.

To apply these methods, it requires security practitioners and professionals to understand the architecture of their information system, then conduct risk assessments to identify vulnerabilities and potential attack types. From risk assessment, necessary defense tools and methods are deployed and utilized. Once the risks are mitigated, regular updates and latest patches are used to strengthen the defense after which frequent penetration tests are carried out to be ahead of any potential attack and ensure policies and regulations are implemented and enforced.