CYBER SECURITY

BISF 3103

ASSIGNMENT 2

EMMANUEL KIPKEMOI SIGEI

REG NO – 20/03807

CAMPUS: MAIN

FULL TIME

PRESENTED TO Mr. MARTIN LUTHER

QUESTION ONE: Types of Threats to Cyber Security and Points in the Network at which these threats are prevalent.

Cybersecurity threats are acts performed by individuals with harmful intent, whose goal is to steal data, and cause damage to or disrupt computing systems and can be classified into two main categories i.e. **internal threats** and **external threats**.

Internal Threats.

Internal threats are threats that originate from within the organization from people such as employees or contracted partners. These are usually either accidental or intentional. Some examples of Internal Threats include:

1. **Data Breaches –** This occurs when the insider mishandles sensitive information or becomes a victim of a social engineering attack which ends up giving unauthorised people access to the said sensitive information. These attacks are more prevalent at Network Endpoints such as the physical computers used to access sensitive information.
2. **Malware Distribution –** Employees can either knowingly or unknowingly be used to spread malware on the network thus compromising the network. This can happen through clicking malicious links or connecting infected drives into computers and it also is more prevalent at Network Endpoints like for data breaches.
3. **Sabotage –** Sabotage includes matters such as the deletion of data from the network or the reconfiguration of network systems which makes the network vulnerable to external cyber security attacks. These attacks are most prevalent on Network Servers since they can be considered to be the backbone of the Network.

External Threats.

External threats are threats that originate from outside the organization and are ordinarily carried out by malicious individuals or international gangs. Some examples of External Threats include:

1. Denial of Service Attacks where the attackers use botnets for example to try to flood the system with excessive amounts of spam traffic which in turn makes it inaccessible to the people who need to access the system thus disrupting operations.. DOS Attacks are most prevalent on Network Gateways
2. Advanced Persistent Threats (APTs), which are majorly installed on Servers, are very sophisticated attacks that are designed to evade detection and they can expand with time on the network posing major vulnerabilities to the Network.
3. Social Engineering Attacks such as Phishing are attacks where legitimate users are tricked into sharing sensitive information or performing actions that compromise Network Security and are most prevalent at Network Endpoints such as the physical Computers users use.
4. Malware attacks where malicious software is introduced into the Network through infected files or infected emails. Malware attacks are more prevalent on Network Endpoints which are used by the threat actors to introduce the malware into the Network.
5. Man-in-the-middle attacks where threat actors intercept communication while it is still en-route (eavesdropping), therefore gaining access to data that they can then change/alter before it reaches the intended recipient. These are more prevalent at Network Gateways so that the communication can be altered before it gets to the intended recipient.

QUESTION TWO: Reasons International Gangs use Cyberspace and why International Gangs are difficult to prosecute.

Reasons International Gangs Use Cyberspace.

1. Cyberspace gives these gangs a wider geographical reach thus giving them a wider pool of targets and potential victims to their activities.
2. Cyberspace brings forth the possibility of anonymity which makes them more discrete and therefore makes it more challenging for Law Enforcement to track them down.
3. It greatly reduces the physical risks such as physical injury or being captured that would otherwise be encountered by engaging in the traditional forms of "close contact" crimes.
4. There are generally higher incentives financially that are attached to cybercrimes eg through ransomware attacks and banking fraud which makes crimes conducted in cyberspace more appealing to these gangs.
5. It is easier to acquire tools to be used in conducting cybercrime such as hacking tools as opposed to obtaining the physical weapons used in most conventional forms of traditional crime.

Reasons why International Gangs are Hard to Prosecute.

1. Based on the fact that these gangs operate in multiple jurisdictions as facilitated by cyberspace, it is difficult to determine which courts have the mandate to hear and determine cases regarding these gangs.
2. As mentioned in the reasons for why they use cyberspace, these gangs enjoy anonymity in cyberspace which poses a major barrier in the tracking down of these criminals therefore making it hard to collect evidence of their criminal actions and afterwards prosecute them.
3. Law Enforcement agencies from different jurisdictions have different priorities based on the laws, legal frameworks and investigative procedures set out for them in their jurisdictions. This makes cooperation between them harder.
4. Law enforcement agencies (especially from less developed countries) are often unable to keep up with the international gangs and their activities due to the limited resources at their disposal, giving these gangs an advantage and making it more difficult for law enforcement agencies to track them down and prosecute them.
5. Due to limited resources including time and money, law enforcement agencies may be unable to successfully keep up with the constantly evolving cyberspace, making it more difficult to hunt down and prosecute these international gangs.

QUESTION THREE: Configuration Management – Key Areas in Network Configuration

Key Components of CM in relation to Network Configuration.

1. ***Asset Management*** – This area involves the identification of all hardware and software network components and keeping a record of them which provides a deeper understanding and greater insights on the network assets.
2. ***Change Management*** – This area involves documenting and tracking the changes implemented in the settings of the network such as updates and modifications made to assets on the network such as routers and switches.

3. ***Planning*** – This area involves the process of understanding the requirements needed for the Network and configuring the network based on these requirements. It also involves understanding the impacts the requirements will have on the network and allocating proper resources to the configuration of the network.
4. ***Quality Management*** – This area involves the continuous monitoring and assessment of the quality of the configuration of the network to ensure that the configuration meets Security Standards.
5. ***Risk Management*** – This area of configuration management involves the assessment and mitigation of risks involved with any changes implemented on the network configuration which in turn helps in the maintenance of security.