BOOK CHAPTER | Cyber Security Concepts

Cyber Security Terminologies and Concepts

Osa Edosa
Department of Electrical/Electronic Engineering
University of Benin
Benin City, Nigeria
Email: edosa.osa@uniben.edu
Phone No: +2348168307508

Abstract

In our digitized world today, threats and attacks can come to systems and networks from various sources. It is often said that the most secure computer is the one that is not turned on. However, many a human institution cannot but rely on computers and more so the internet for their daily operations. Hence it is highly imperative to understand these threats to computer systems and networks with a view to mitigate or at least limit their impacts on systems while they are in operation. Understanding networking concepts helps a security professional to better grasp fundamental knowledge of the operations of threat actors. Such understanding serves to inform cyber security professionals as to how hackers are able to discover flaws in application software, operating system software and networking protocols. This chapter serves to introduce certain terminologies and concepts related to cybersecurity.

Keywords: Cybersecurity, Threat, Confidentiality, Data.

Introduction

Network security in general encompasses detection and prevention of unauthorized access or intrusion into both network elements and devices connected to networks. This definition can be applied to the cyberspace in particular. Therefore, cybersecurity could be viewed as encompassing the detection and prevention of unauthorized access or intrusion into the cyberspace and associated devices and systems. Cybersecurity is a worthwhile and complex business. It is important to have a broad range of experience in and an in-depth understanding of the cyberspace before one can begin to apply security checks. In this era known loosely as the *information age*, the commodity is information of various types and categories. The *data* so generated is considered private property by many organizations or institutions and can thus be extremely valuable, or to a considerable extent, the release of such information to unintended persons can be costly to such organizations or institutions. For this reason, cybersecurity is a priority within most organizations or institutions (Wilkins, 2011).

BOOK Chapter | Web of Deceit - June 2022 - Creative Research Publishers - Open Access — Distributed Free

Citation Osa, Edosa (2022). Cyber Security Terminologies and Concepts.
SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series
Book Chapter on Web of Deceit - African Multistakeholders' Perspective on
Online Safety and Associated Correlates Using Multi-Throng Theoretical, Review, Empirical
and Design Approaches. Pp 247 -252. www.isteams.net/bookchapter2022.
DOI https://doi.org/ 10.22624/AIMS/BK2022-P41

Core Terminologies

There are three major objectives or pillars of Information (or Cyber) Security upon which a cyber safe system is based. They include:

- Confidentiality
- Integrity
- Availability

These three pillars are commonly referred to in the security community as the **CIA triad** with each pillar playing a vital role in providing information security to any institution.

Confidentiality

Confidentiality is an objective to ensure that messages and other relevant data to the organization are kept private from unauthorized persons or devices in the cyberspace. Confidentiality is implemented in the form of data encryption techniques.

Integrity

Integrity is an important character of human society. It serves to ensure that things go as they are intended. This same principle is required in a computer. In cyberspace, it is extremely important to ensure that data or messages are not altered during communication between source and destination. Cybersecurity professionals make use of hashing algorithms to validate whether a message was altered or not during transmission.

Availability

Many hackers use various types of cyber attacks to prevent legitimate users from accessing a resource. In other words, they try to disrupt the availability of data and resources. Within the field of cybersecurity, availability simply ensures that data and resources are always available to users and systems that are authorized to access these resources. An example of an attack that can disrupt availability is a Distributed Denial of Service (DDoS) attack. This attack usually originates from multiple geographic locations to target a system or network in cyberspace. The attacker's intent is to cause the target system or network to be rendered inaccessible or unusable by others.

Fig. 1: Cyber Security Components

Source: https://www.campussafetymagazine.com/technology/cybersecurity-basics-campus-safety/

Security Risk Terminologies

Threats, exploits and vulnerabilities

A threat could be defined as anything that can potentially cause harm or danger to an asset in cyberspace. A good example of a threat is a disgruntled employee with the intention to disrupt the network of an organization upon departure from the company. The intention is primarily to disrupt availability of the network.

Threat actors

A threat actor refers to an individual or a group of individuals who use their skills to carry out malicious actions on an organization, system or person. Intention to compromise target systems varies from hacker to hacker; some hack for fun, while some others hack for financial gain. The following describes a list of some types of threat actors and their intent for hacking:

Hacktivists

Hacktivists are activists who use their skillset as hackers to promote political or social ideology.

Script kiddie

A script kiddie does not necessarily refer to a kid but one who uses ready-made scripts and tools built by professional hackers. Such persons lack the actual technical knowledge that real hackers possess but has the same intent to cause harm or damage to a system or network as hackers do.

State-sponsored

These hackers are hired by governments to both defend their nation from cyber attacks and to carry out information gathering (reconnaissance) on other nations. They are usually equipped with the best tools since they are sponsored by governments.

Organized crime

Sometimes, hackers work in groups in order to use their skills and resources for financial benefits. Each person within an organized crime group has a special skill and therefore plays an important role in the group.

Insider

Organizations usually perform a thorough screening of any potential employees during their interview process. However, there could be an *insider* who is a threat actor but poses as a trusted employee, a disgruntled employee who wants to take down the company's cyber infrastructure for personal reasons, or an innocent employee who accidentally clicks on a malicious link within a harmless email message.

Besides the above, there are also **black hat** hackers, who use their skills for malicious intentions, as well as **white hat** hackers, who use their skills to help secure organizations, they are the crime fighters within the cybersecurity industry. However, there are also **gray hat** hackers, that exist in between the black hat and white hat groups. Gray hat hackers can use their skills for both good and bad purposes, for example, they can work as a cybersecurity professional by day and a heinous hacker at night (Singh, 2021).

A **vulnerability** is a security weakness or design flaw in a cyber system. Hackers as well as cybersecurity professionals race against each other in discovering design flaws in cyber systems. While hackers are constantly searching for security weaknesses that enable them to compromise the system or network, cybersecurity professionals are constantly probing to discover these design flaws and fix them before hackers find them (Singh, 2021).

Exploits are employed by hackers to take advantage of a system or network vulnerability. An exploit is anything, such as malicious code or a tool, that can be used to leverage a security weakness in target systems or networks. They could either be local or remote. A local exploit needs to have been present in the target system, meaning the hacker would need to access the target and then execute the exploit on the system. A remote exploit is launched over the network by the hacker, so physical access to the target system is not required but simply network connectivity.

Attack surface and vulnerability

Cybersecurity professionals work round the clock to reduce the risk of organizations becoming victims of cyber attacks or experiencing threat outbreaks on their internal networks. One primary way of achieving this objective is by reducing the attack surface. With respect to cyberspace, **Attack surface** is defined as the total points on a system or network at which a threat actor can intrude and illegally access data.

Simply put, by reducing the attack surface within an organization, the number of security vulnerabilities are reduced and consequently the likelihood of a cyber attack. To reduce the attack surface, security professionals need continuously search for network and system vulnerabilities in order to implement remediation actions and security controls as needed. Security professionals use both free and commercial tools to help them achieve their objectives (Singh G. (2021).

Common Forms of Cyberattack

Ransomware

With this approach, hackers gain access to a system using malicious software, then encrypt sensitive data and hold it hostage until their demands are met. It could also involve scareware, a software that allows hackers to access an employee's computer, encrypt target sensitive data and thereafter demand some form of payment to decrypt it.

Spear Phishing

This is an email attack that requests information such as system access data or bank details in the hope that some innocent recipient of the mail will respond to the request.

Whaling

This method is the similar to spear phishing but C-level executives are the targets of attack.

Internet of Things

Another point of entry into cyberspace for hackers is the Internet of Things, or *IoT*. These are devices such as wireless HVAC controllers, smart watches, or even drug-infusion pumps that dispenses medication based on a patient's physiological alerts. These systems are particularly vulnerable because design of security elements is of little concern to their vendors (Adams, 2019).

Additional Cyber Security Terms

Source: https://www.campussafetymagazine.com/technology/cybersecurity-basics-campus-safety/

1. IP address: Each computer has a unique Internet Protocol (IP) address, which consists of a set of numbers. The set of numbers is a language that computers use to communicate with each other over a network. IP addresses allow any number of internet-connected computers to be distinguished from other computers. Blue Host compares it to calling someone on the phone — everyone has a unique phone number, and you have to dial that number to reach someone.
2. Domain: A group of computers, printers and devices that are interconnected and governed as a whole. In layman's terms, a domain name is the text that a user types into a browser window to reach a certain website.

3. Domain Name System (DNS): Domain Name System (DNS) converts human-readable domain names, such as www.google.com, to machine-readable IP addresses. When you go to your web browser and type in a domain name, it will connect with the DNS. The DNS then searches through all of the registered IP addresses and connects that domain name with the IP address. Continuing with the phone analogy, Blue Host compares domain names to contacts in your phone — instead of typing in the full phone number to call someone, you click on the contact's name.
4. Virtual Private Network (VPN): A tool that allows users to remain anonymous while using the internet by masking the location and encrypting traffic. It allows private networks to send data across shared or public networks as if their devices were directly connected to a private network.
5. Firewall: A network security device that monitors incoming and outgoing network traffic and allows or blocks data packets based on a set of security rules. Its purpose is to block malicious traffic.
6. Spyware: Software that is installed on a device without the end user's knowledge and spies on their activity. It can invade the device, steal sensitive information and internet usage data, and relay it to advertisers, data firms or external users.
7. Trojan: A type of malicious software that downloads onto a computer disguised as a legitimate program. It is a type of malicious software that typically gets hidden as an attachment in an email or a downloadable file and then transfers onto the user's device. Unlike computer viruses or worms, a Trojan does not self-replicate, so it needs to be installed by a valid user.
8. Virus: A type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another.
9. Worm: A type of malicious software that spreads copies of itself from computer to computer. It can replicate itself without human interaction and does not need to attach itself to a software program in order to cause damage. The primary difference between a virus and a worm is that viruses must be triggered by the activation of their host while worms are stand-alone programs that can self-replicate.
10. Bot/Botnet: A type of software application that performs tasks on command, allowing an attacker to take complete remote control of an affected device.
11. Encryption: The process of converting human-readable plaintext to incomprehensible text to prevent theft. It is a way of scrambling data so only authorized parties can understand the information.
12. Penetration testing (pen testing): A practice that uses hacker tools and techniques as a way to discover and evaluate security flaws. It is essentially a simulated cyberattack to check for exploitable vulnerabilities.
13. Social engineering: A technique that uses psychological manipulation to trick users into making security mistakes or giving away sensitive information. When individuals are targeted, hackers are usually trying to trick people into giving them passwords or bank information. Examples include deceptive emails or text messages with the promise of a reward.
14. Threat actor: The person behind the event. This could be an external threat who launches a phishing campaign or an employee who accidentally leaves sensitive documents on their desk.
15. External threat: An external threat is an attack by a hacker not associated with the affected institution, where no trust or privilege previously existed. In the education sector, 80% of cybersecurity incidents were from external threats. In healthcare, 61% of threat actors are external.
16. Internal threat: An internal threat is a threat actor within the organization. In the education sector, 20% of cybersecurity incidents were from internal threats. In healthcare, that number is significantly higher at 39%.

Risk Mitigation Terminologies

Defense-in-Depth (DiD)

This represents a multilayered approach by which organizations defend their systems. The DiD strategy simply implies that a single layer of security should not be used alone to countermeasure cyber attacks. If this single layer fails to protect the network, then all organization assets are exposed to hackers. A multi-layered approach should therefore be employed to protect all assets from various forms of cyber attacks, if one layer of protection fails to safeguard an asset, another layer should already be in place to secure the company asset (Singh, 2021).

Classification of Data

One primary task that organizations need to carry out for adequate protection of their data is Data Classification. Levels of data classification could differ from one organization to another as described below:

Military Data Classification (Boyles, 2010)

Classification	Nature of Data
Unclassified	This form of Data has no Confidentiality, Integrity or Availability requirements
Sensitive but Unclassified (SBU)	This is data that has potential to embarrass the organization if made public but has no major restrictions imposed.
Confidential	This is data that has Confidentiality protection.
Secret	This refers to data that should be more restrictive than confidential but less than top secret.
Top Secret	Data here in this category must be secured with the most effort and at best cost. Only those with required clearance can access it.

However, some private organizations do not align with the above data classification. A common classification for private sector organizations is described below:

Private Organizations Data Classification (Boyles, 2010)

Classification	Nature of Data
Public	Data in public domain, no protection required.
Sensitive	This is similar to SBU in military classification model.
Private	Information about the organization not to be revealed to the outside world.
Confidential	This is the highest level of classification in the private sector. It is carried out with the highest level of security control and at the greatest expense. A good example is a trade secret.

REFERENCES

1. Adams, M. (2019). Cybersecurity: PROTECT THE VALUE OF YOUR COMPANY. Available at: http://mossadams.com/cybersecurity.
2. Boyles, T. (2010). CCNA Security Study Guide. Copyright©2010 Wiley Publishing, Inc., Indianapolis, Indiana.
3. Singh G. (2021). Cisco Certified CyberOps Associate 200-201 Certification Guide. Copyright © 2021 Packt Publishing.
4. Wilkins, S. and Smith III, F. H. (2011). CCNP Security SECURE 642-637 Official Certification Guide. Copyright© 2011 Cisco Systems, Inc.