IJEMD-S, 1 (1) (2023), 1 –9 https://doi.org/10.54938/ijemds.2023.01.1.232

International Journal of Emerging Multidisciplinaries: Security

Research Paper
Journal Homepage: www.ojs.ijemd.com
ISSN (print): 3005-4265

Fundamentals of Cyber Security

Hammam Almonajid
Department of Information Technology, College of Computer Engineering & Sciences
Prince Mohammed Bin Fahd University (PMU), Al Khobar, Saudi Arabia

Abstract

This study highlighted the importance of cybersecurity for organizations that hold databases, emphasizing the increasing need to secure sensitive data from all types of online attacks. Given the rate and complexity of attacks, organizations must recognize that data breaches can have major consequences, including financial losses, damage to reputation, and legal responsibility. Companies may better prepare to recognize and manage these risks if they are aware of the most frequent cyber-attacks, such as phishing, malware growth, and social engineering. Furthermore, the study analyzed several types of malware, such as viruses, adware, ransomware, and spyware, emphasizing the importance of effective security measures to prevent the assault and potential harm. as well as implementing strict access controls, encryption processes, and frequent data backups. By developing an effective cybersecurity plan, organizations may strengthen their resilience to cyberthreats and safeguard the confidentiality, integrity, and availability of their precious data assets.

Keywords: CIA; Cybersecurity basics; Data Protection; Hackers Types; Threats and vulnerabilities

1. Introduction

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It is now considered the basis for the security of any organization, company, association, or entity that has information stored in its database.

“Cybersecurity is a strategy that people as well as companies use for protecting against unwanted access to databases and other digital systems. A strong cybersecurity organize can offer a decent security posture against threatening attacks designed to gain access to, change, delete, destroy, or extort sensitive data and systems that belong to a business or user. Security measures are crucial in preventing attacks that try to take down or damage a system or device's functionality” (Shea, S., Gillis, A. S., & Clark, C, 2023).

Email address: **hammam.almonajid@gmail.com (H. Almonajid)**

To establish a secure system, it is important to know the security triangle (CIA) which consists of (C: Confidential: Protecting sensitive data from unauthorized access, I: Integrity: Maintaining data accuracy and preventing unauthorized modifications, A: Availability: Making sure the right people can access information when they need it).

In this paper, we will learn about the categories of security, and the most prominent modern attacks in society, how they work, and what techniques are required to protect our personal data, or the data of the company or organization in which we belong to.

Firstly, lets define the security categories:

1. Network security refers to the protection of computer networks and all of their components against intrusions, assaults, and data leaks. It includes setting up several types of protections and technologies to protect from and detect threats as well as to ensure the availability, confidentiality, and integrity of network resources. Network security uses firewalls, encryption, access restrictions, detection of intrusions, and other security measures to protect network infrastructure, devices, and data.
2. Application security: Application security is about securing software programs against bugs and malicious penetration. In order to make sure that applications are created, developed, and launched with security in mind, it involves setting policies and best practices in action. Application security focuses on locating and eliminating threats such unauthorized access, code vulnerabilities, malware injection, and cross-site scripting. To ensure the confidentiality, integrity, and availability of the application and its data, it incorporates approaches like secure coding practices, input validation, session management, and routine application testing.
3. Information security: Information security is the process of preventing people who are not authorized from accessing, using, providing, harming altering, or destroying sensitive information. It includes maintaining the privacy, accuracy, and accessibility of data in any type, including digital and physical. To protect data and stop illegal activity, information security requires setting a variety of rules, processes, technology, and controls in spot. Encryption, access restrictions, authentication, regular backups, security awareness training, and incident response planning are a few examples of the protections that come under this category. Information security is designed to protect information from any kind of risks including cyberattacks, data breaches, and unauthorized access.
4. Operational security: is the protection of a company's regular business operations against potential threats and interruptions. It involves setting policies and procedures into place that ensure the dependability, continuity, and security of important systems, processes, and resources. Operational security includes a range of elements, such as physical security of buildings, access controls, security awareness training for employees, incident response preparation, and business continuity management. It tries to recognize and prevent threats and vulnerabilities such unauthorized access, insider threats, emergencies, and cyberattacks that might affect an organization's operational working properly.

Organizations may reduce risks, maintain productivity, and respond to security events in an effective way by maintaining a strong operational security architecture.

Secondly, there are many types of cyber-attacks which are “cyberterrorism: is intended to undermine electronic systems to cause panic or fear, cybercrime: includes single actors or groups targeting systems for financial gain or to cause disruption, cyber-attack: often involves politically motivated information gathering” (Kaspersky, 2023). Now let’s move to the most common threats and how it works:

- Man-in-the-middle (MITM): This type of cyberattack involves a hacker accessing and intercepting communication between two parties, such as a user and an application, a user and a network, or a user and a website. This attack's main goal is to collect all data and information that is accessible in the affected area and use it for illegal activities like spying, selling, or to target victims.

The hacker starts the attack by secretly disrupting the user and connected system's communication. The hacker has the ability to access, find, and exploit sensitive data by decrypting the communication channels between the user and the system. The user is unaware of this and believes they are dealing with the system directly, but in reality, all of the data and inputs they provide including passwords, email addresses, and even web searches first go to the hacker and then to the system.

- Social Engineering: is a deceptive tactic used by hackers to get sensitive information from individuals or organizations. Passwords, financial information, personnel data, primary server domain names, and other data are included in this. Hackers use a variety of tactics to trick their victims. They may use fake phone numbers to deliver messages while posing as employees of appropriate government departments and financial organizations. In order to get sensitive information, they frequently send messages on email that contains links to fake offers, competitions, and rewards.

Another tactic used by hackers is to get users to click on search engine advertisements by hiding viruses designed to steal personal data inside of them. Additionally, in an effort to access and steal critical information, hackers may compromise the security of a person known to the target and send text messages with viruses. These social engineering techniques emphasize how important it is to be informed and have strong security measures in place to prevent such malicious activity.

- Ransomware: is a type of dangerous cyber-attack that aims to financially exploit victims by either locking their device or encrypting essential and important files, making it harder for the victims to access them. To unlock the device or decode the contents, the attacker wants a ransom payment.

The attacker installs a number of viruses at the beginning of the attack and distributes them in different ways. This can be done by sending false emails, text messages with tempting offers designed to get the reader to interact with the message, or by downloading data from the internet without checking its security and safety. As soon as the victim participates in these criminal behaviors, a virus is automatically installed on their device, allowing the attacker access, and enabling the encryption of crucial files or the locking of the victim's device. A ransom demand is then made, asking for money to unlock the device or decode the contents in return for their encryption.

- Phishing is a type of cyberattack where the attacker represents as official or governmental organizations, or as businesses such as shops, eateries, and logistics support companies that are connected to the targeted victim in order to obtain sensitive data such as passwords, banking information, and more.

The attacker uses persuasive techniques within the message content to persuade the victim to click on the link or download the file for a variety of reasons. The targeted victim receives emails that contain a link or file. One common situation is when the victim receives a mail from their bank asking them to update their information by logging in through a certain URL and changing their password. The attacker can collect and use the victim's financial information if they respond to the message without first checking where it came from and beginning entering it. This is one of the situations when a victim is taken in by a phishing scam.

- SQL injection: “is an internet security vulnerability that allows an attacker to make modifications with database queries made by an application. It typically enables an attacker to look at data that they would not otherwise be able to get. This might include data belonging to other users or any other data that the program has access to. An attacker can often edit or destroy this data, resulting in lasting changes to the application's content or behavior. An attacker may increase a SQL injection attack to breach the server that hosts the data or other back-end infrastructure, or launch a denial-of-service attack in specific circumstances” (PortSwigger, n.d).

- Distributed Denial-of-Service (DDoS): “is intentionally designed to overload a server, service, or network by overloading them with a high volume of Internet traffic. These attacks make use of botnets, networks of hijacked computers, and Internet of Things (IoT) devices that the attacker may remotely play with. The attacker organizes a flood of requests towards the target's IP address by sending remote commands to the infected devices, which denies service to authorized users” (Cloudflare, n.d).

“The difficulty in identifying malicious attack traffic from legitimate traffic makes DDoS attack prevention challenging. Filtering out harmful requests is difficult since the botnet's individual devices all seem like normal Internet-connected devices. Strong network infrastructure, early detection, and reduction methods, as well as the capacity to differentiate between legitimate and malicious traffic, are all essential components of effective DDoS attack protection measures” (Cloudflare, n.d).

Thirdly, “Malware, sometimes known as "malicious software," is risky code that enters computer systems, networks, and mobile devices and disrupts them or makes them unusable. It behaves aggressively, interrupting with regular processes and taking control of device operations. Malware can have a variety of goals, including monetary gain, making political comments, or gaining recognition. Without permission, it may steal data, interfere with computer operations, and keep track of user activities, with serious consequences including privacy violations and data breaches” (Malwarebytes, 2020).

“Individuals and businesses must prioritize cybersecurity measures in order to reduce the threats posed by malware. This involves using trustworthy antivirus software, secure passwords, routine software upgrades, and careful surfing techniques. User awareness and education are essential for identifying and avoiding

malware-infected files and programs. Users may guard against the detrimental effects of malware by being alert and taking preventive safety measures" (Malwarebytes, 2020). Here are some types of malwares:

I. Virus: is a malicious software program that may copy itself and send from one computer to another. It does this by poisoning authorized documents or applications, which damages the affected system and may spread the infection to other linked systems. Once a computer has been infected, the virus can carry out a number of damaging tasks including corrupting files, stealing data, or interfering with system operations. Viruses are frequently spread via email attachments, software downloads, or by taking advantage of vulnerabilities in software. Utilizing antivirus software, updating operating systems and applications, and following safe surfing practices are all aspects of virus protection that help keep computer systems secure and free of infection.

II. Spyware: is malicious software that acts secretly and gathers private data from a computer or other device without the user's knowledge or agreement. It secretly keeps track of user activities, collecting sensitive information including login passwords, financial data, and browsing habits that can be exploited for identity theft, financial crime, or unlawful spying. Spyware may be used via tricks and vulnerabilities, and once activated, it runs in the background while sending the data it has stolen to outside attackers. Strong cybersecurity measures, such as the use of reliable antivirus software, routine software and system updates, and the introduction of safe browsing habits, are essential to defend against spyware. These activities reduce the chance of outbreaks and maintain user privacy and data.

III. Trojans, commonly referred to as Trojan horses in cybersecurity, are sneaky malware that acts as trustworthy files or applications to trick users. Trojans, in contrast to viruses, rely on social engineering to enter systems rather than self-replicating like viruses do. Once inside, they can engage in a variety of damaging actions, such as data theft, illegal access, or giving attackers remote control. Trojans are frequently spread via email attachments, questionable downloads, or by taking advantage of vulnerabilities in software. Trojans must be treated with using a complex strategy. This involves employing reliable antivirus software, upgrading computers often, and being careful when utilizing suspicious files or links. The misleading risks offered by Trojans must be avoided in order to preserve system security, which calls for attention and strong cybersecurity procedures.

IV. Adware is a term used to describe unwanted software that shows annoying advertising on a user's device. Adware, which is frequently installed without complete agreement, makes money by displaying customized ads or gathering user data for marketing purposes. With pop-ups, advertisements, and browser redirection, it spoils the user experience while also possibly violating privacy by monitoring activity and gathering sensitive information. Use reliable antivirus or anti-malware software, be cautious when installing software, and read any agreements and rules to protect yourself against adware. The likelihood of adware

outbreaks is further reduced by routine system upgrades and safe surfing techniques, such avoiding unsafe websites and links, which help to maintain a secure digital environment.

V. Botnet: is a collection of computers with malware or (bots) that are managed by a central server. By installing malware on vulnerable computers, cybercriminals build botnets that allow for remote coordination and control. Botnets offer serious risks because they may carry out coordinated cyberattacks, send out spam emails, steal data, and launch massive DDoS attacks. Compromised systems provide strong tools for thieves due to their combined computational strength. Strong cybersecurity measures are needed to combat botnets, including current antivirus software, vulnerability patches, and network security controls to identify and stop botnet traffic. User awareness is essential, with a focus on care with suspect connections, avoiding unreliable sources, and maintaining good cybersecurity habits to avoid joining botnets. Organizations and individuals may reduce the risk of botnets and help create a safer digital environment by adopting proactive actions.

Additionally, not all the hackers are bad, there are some categories that can define who is the good hacker and who is the bad:

- Black Hat Hackers: “Black hat hackers are malicious users who purposefully attack networks without authorization. Black hat hacking is defined as trying to obtain unauthorized access to computer systems. Once a black hat hacker discovers a security vulnerability, they attempt to exploit it, frequently by inserting malware such as a trojan or a virus. Black hat hackers frequently use ransomware attacks as an additional tactic to extract money or compromise data systems” (Buxton, O. (2023).
- White Hat Hackers: “White hat hackers are ethical security hackers who find and patch vulnerabilities. White hat hackers work to find system vulnerabilities so they may be fixed, and assist increase a system's overall security. They hack into systems with the authorization of the businesses they hack into” (Buxton, O. (2023).
- Gray Hat Hackers: “Gray hat hackers have the illegal or malicious purpose of black hat hackers, but they also don't have the previous knowledge or approval of people whose systems they hack into. However, when gray hat hackers discover vulnerabilities such as zero-day vulnerabilities, they provide them rather than exploiting them fully. However, gray hat hackers can ask for money in return for a full account of what they discovered” (Buxton, O. (2023).
- Green Hat Hackers: “Green hat hackers are "green" in the sense that they lack the technical capabilities of more experienced hackers. To bypass security measures, green hats may use phishing and other social engineering tactics” (Buxton, O. (2023).
- Blue Hat Hackers: “Blue hat hackers are white hat hackers that are hired by a company to do penetration testing to assist improve its security systems” (Buxton, O. (2023).
- Red Hat Hackers: “Red hat hackers, also known as heroic hackers, are motivated by a desire to combat black hat hackers, but they do it by entering black hat groups on the dark web and executing cyber assaults against their networks and devices” (Buxton, O. (2023).

Finally, after we knew about the attacks and how it runs, we should know how to protect our personal information, private data, etc.…

1- “Use strong, unique passwords: Create complex passwords that are difficult to guess and avoid using the same password for multiple accounts” (Eitel. B, 2023). There are some standards for a good password that are recommended to follow: (Make your password consist of 14-16 characters minimum, do not use any words that related to you, or your habits, use lower and upper case, use numbers, and use symbols).
2- “Enable two-factor authentication (2FA): Set up 2FA whenever available for your online accounts. This adds an extra layer of security by requiring a second form of verification, such as a text message or an authentication app (Federal Trade Commission, 2021)”.
3- “Use secure Wi-Fi networks: When connecting to Wi-Fi networks, especially public ones, ensure they are encrypted, and password protected. Avoid accessing sensitive information on unsecured networks” (Federal Trade Commission, 2021).
4- “Use reputable antivirus and anti-malware software: Install and regularly update antivirus and anti-malware software to detect and remove malicious software from your devices” (Federal Trade Commission, 2021).
5- “Regularly back up your data: Create backups of important files and store them securely. This helps protect against data loss due to malware, hardware failure, or other incidents” (CISA, 2022).
6- Use a VPN to privatize your connections: “Use a virtual private network (VPN) for a more secure and private network. Your connection will be encrypted, and your private information is protected even from your internet service provider” (Chen. S, 2023).
7- Double-check for HTTPS on websites: “When you visit a website that does not use HTTPS, there is no assurance that the information transferred between you and the site's server is safe. Make sure a website is HTTPS-encrypted before providing any confidential or personal information” (Chen. S, 2023).
8- Scan external storage devices for viruses: “Both internal and external storage devices are vulnerable to a virus. The malware infection might spread if a malicious external device is connected to your computer. Before using external devices, always check them for the spread of infection” (Chen. S, 2023).
9- Employ a “White Hat” hacker: “Not all hackers are bad. Some hackers publish vulnerabilities so that others might increase their cybersecurity by being informed of them and repairing them. "White hat" hackers are those who use these techniques. Hiring one might assist you identify threats you weren't aware of” (Chen. S, 2023).

2. Conclusion

In the end, this study has emphasized the importance of cybersecurity for businesses that own databases, highlighting the increasing needed of protecting sensitive data from many kinds of online threats. Organizations must understand that data leaks can have serious effects, including financial losses, damage to reputation, and legal responsibility, given the frequency and complexity of attacks. Companies may better prepare themselves to identify and manage these risks by knowing about the most common cyber-attacks, such as phishing, spread of malware, and social engineering. Furthermore, the study looked at several kinds of malware, such as viruses, adware, ransomware, and spyware, highlighting the need for strong security measures to stop the attack and possible damage. The study also covered the need to take proactive steps to protect personal data, such as setting up strong access restrictions, encryption methods, and regular data backups. Organizations may increase their resilience to cyberthreats and protect the confidentiality, integrity, and availability of their valuable data assets by implementing an effective cybersecurity strategy.

3. References

[1] Kaspersky. (June 30). *What is cyber security?* www.kaspersky.com. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security (2023).

[2] *What is a distributed denial-of-service (DDoS) attack? | Cloudflare*. (n.d.). Cloudflare. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

[3] *Virus vs Malware*. [Video]. Malwarebytes. https://www.malwarebytes.com/malware (2020).

[4] Eitel, B. 7 Tips to Manage Your Identity and Protect Your Privacy Online. *National Cybersecurity Alliance*. https://staysafeonline.org/resources/7-tips-to-manage-your-identity/ (2023).

[5] *Identity Theft and Online Security*. (November 10). Consumer Advice https://consumer.ftc.gov/identity-theft-and-online-security (2021).

[6] *4 Things You Can Do To Keep Yourself Cyber Safe | CISA*. (December 18). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-cyber-safe (2022).

[7] Buxton, O. Hacker Types: Black Hat, White Hat, and Gray Hat Hackers. *Hacker Types: Black Hat, White Hat, and Gray Hat Hackers*. https://www.avast.com/c-hacker-types (2023).

[8] Chen, S. 21 Cybersecurity Tips and Best Practices for Your Business [Infographic]. *TitanFile*. https://www.titanfile.com/blog/cyber-security-tips-best-practices/ (2023).

[9] Shea, S., Gillis, A. S., & Clark, C. What is cybersecurity? *Security*. https://www.techtarget.com/searchsecurity/definition/cybersecurity (2023).

[10] *What is SQL Injection? Tutorial & Examples | Web Security Academy*. (n.d.). https://portswigger.net/web-security/sql-injection