# PRSE6212 ASSIGNMENT SOLUTION

Question1

The information given to organizations is very important as this information this is sensitive such as home addresses phone numbers and identity numbers, this information can be used for things such as scams, identity theft and fraud. In the case of the banking sector, using a person's ID number, scammers could do fraudulent activity such as phishing by altering the HTML of their bank app using remote applications such as AnyDesk, this is a common method used by scammers to take money from unsuspecting people. People who have your information such as your phone number can contact you via e-mail or phone call and claim that they are the bank trying to assist you in an error within your account, it is important that this information is kept secure as this information could be used against the people if leaked, yeah thousands of people get scammed due to these Phishing schemes. This information needs to be protected using various encryption methods to ensure the prevention of data breaches and ensure the security of any user’s personal details.

Question2

Malware is harmful software that enters a computer system without the user consent or without their knowledge, causing damage to the device and leaving it vulnerable. There are different types of malwares that use different methods of attacks on devices, with different categories such as Imprison, Launch, Snoop and Deceive.

Imprison refers to the type of malware that take hostage of the device, not giving the user freedom to use their device as they please ransomware and crypto malware are malware that imprison. Ransomware prevents a user from using a device until a fee is paid, it embeds itself onto the computer in such a way that it cannot be bypassed, making it difficult to remove. Crypto ware does the same with the difference being that your files are encrypted until you pay a fee to recover the files. Both malwares imprison the device and prevent the user from using the device as desired, making both imprison malware.

Launch/Infection refers to malware is that which infects a device to launch attacks on other computers. Viruses and worms are malware in this category, viruses attach themselves to files or use vulnerabilities found on the software of a device and reproduce in favourable conditions. Worms also reproduce but they use the networks and vulnerability of a device’s OS to their advantage and spread to another device that has a similar vulnerability.

Snoop refers to malware that spies on the victims of the attack. Two common types of snooping malware are Spyware and Keyloggers. Spyware monitors and collects information from the user without their consent, including sensitive information and all programs downloaded on the device. A keylogger captures the keystrokes that a user has made on the device keyboard, using the keylogger attackers are able to obtain sensitive information such as passwords or personal information. These two malwares are snoop malware due to the surveillance they do without the consent of the user, and these can easily be used by attackers to obtain sensitive information.

Deceptive malware refers to malware that disguises itself as legitimate software, but it is malicious software. Trojans and PUPs (potentially unwanted programs) are examples. PUPs are malware disguised as programs pre-installed on devices or advertisements that interfere with web browsing. A trojan appears as a harmless program performing benign activities but is performing malicious activities without the knowledge of the user. Both malwares use deception to attack devices and gain access to sensitive information, making these the most common attacks users face on their devices.

Quesion3

Cybercriminals use various methods to attack web server applications, exploiting vulnerabilities to gain unauthorized access to sensitive information. Methods such as Cross sight scripting, SQL Injection, attacks on software using vulnerabilities, Cross Sight Request Forgery, Replay attacks.

Scripting: user input is accepted without validation and malicious scripts are injected into web pages viewed by other users. Attackers exploit vulnerabilities within the web application to inject JavaScript or other scripting code.

Injection: cybercriminals manipulate user input fields on web applications to inject malicious SQL commands into the backend database. Attackers can access the user’s input if it is not sanitized and validated.

Attacks on software: Attackers use the vulnerabilities found in software to access your personal information by exploiting memory vulnerabilities, improper exception and error handling, and external software components.

Request Forgery: authenticated users are tricked into unintentionally executing malicious actions on a web application they are logged into already.

Replay attacks: a type of cyberattack where an attacker intercepts and copies data exchanged between two parties then retransmits that data with slight altercations, to impersonate one of the legitimate parties (Ciampa,2022).

Question 4

It is important that operating systems are secure as they hold sensitive information that hackers could use for cyber crimes such as Identity theft or fraud. There are many methods that can be used to ensure the security of the operating systems and prevent any vulnerabilities from being exposed.

Regular software updates and patch management are a great way to keep secure, keeping operating systems and software applications up to date with the latest security patches, preventing cybercriminals from exploiting known vulnerabilities in outdated software in previous versions. Data encryption of sensitive data both in transit and at rest ensures the protection of data, even if it falls into the wrong hands. Implement Multi-Factor Authentication (MFA)for access to important systems and accounts, it adds an extra layer of security by requiring users to provide additional authentication factors beyond just a password. Collaboration with Cybersecurity Experts increases the security of the systems preventing future attacks from hackers and insight from professionals whenever problems are faced in security. Vendor Security is the most used option for protecting systems, assess the security of third-party vendors and service providers who have access to your systems and data and ensure they meet the desired security standards. Like the security firm mentioned in the case study, the security specialists you partner with and security products you choose to purchase can detect and rectify any vulnerabilities and prevent any threats from harming your systems.

Question 5

By utilizing network segmentation and security zones, African businesses can be protected against any threats. When using security zones first identify all the security zones within your network as they all serve a purpose and have varying security requirements, businesses can create security zones or segments within their network architecture. Each zone should have its own set of security policies and access controls. Network segregation refers to logical separation of the network into these defined security zones, it can be used to secure network architectures by creating separate network segments with different trust levels and access controls. It also helps to reduce the attack surface by limiting the exposure of critical assets to potential threats. Performing regular patches and updates ensure that there are no vulnerabilities attackers can exploit (Techslang ,2021).

Question 6

Some applications have different security have different security requirements; it is important they all adhere to the set protocols to ensure the safety of the data. African businesses must adopt methods such as network segmentation to protect the critical assets, with only authorized members being able to access sensitive information. Regular security patches and updates can be done to increase the security and removes known vulnerabilities, protecting the network from exploits. Firewalls could also be used to monitor and control traffic to and from the applications and platforms in African businesses. Any suspicious activity is blocked when a firewall is used, preventing any attacks. Strong authentication methods must also be applied such as such as multi-factor authentication where a further verification is done to ensure that the person is authorized to perform certain functions or is able to access certain information.

Question 7

Cryptography is the process by which information is transformed into a secure form so that unauthorized persons have no access to it. It can be applied through hardware or software. Two of the most common types of attacks on cryptography are algorithm attacks and collision attacks. Algorithm attacks target the encryption algorithm focusing on the vulnerabilities or weaknesses in the implementation, or selection of the encryption algorithm. The weaknesses are exploited intercepting and collecting ciphertext.

Collision attacks focus on cryptographic hash functions. They aim to find two different inputs that produce the same hash value, finding a vulnerability in the hash function. These attacks exploit the finite size of the output space of a hash function, generating inputs that lead to hash collisions. This can be used to manipulate data integrity checks or gain unauthorized access by exploiting the collision. (Lake,2023).

Question 8

Cryptography can be used to secure the information communicated and ensure none of the information can be accessed by any unauthorized individuals. It can be implemented by:

Strengthening encryption algorithms: Strong encryption algorithms are crucial for ensuring data confidentiality, even if intercepted by unauthorized parties. The length you choose for encryption keys should be longer to increase security. The keys must be protected by rotation ensuring they do not fall into the wrong hands.

Secure hash functions: Implement secure cryptographic hash functions to ensure data integrity, the functions convert data into fixed-length hash values used to verify data integrity during transmission and protect passwords. Comparing the hash of received data with the expected hash enables you to detect any unauthorized alterations. Secure Key Management Practices: Practicing effective key management practices to safeguard encryption keys and ensure their secure generation, storage, distribution, and retirement. Use cryptographically secure random Implement access controls and policies to restrict access to encryption keys to authorized personnel only (Freeman, 2022).

# REFERNCES

Auda, Y. (2020) Zone Based Firewall Part 1, Cisco Learning Network. Available at: https://learningnetwork.cisco.com/s/article/zone-based-firewall-part-1#:~:text=Zone%2DBased%20Policy%20Firewall%20(ZBPF,the%20same%20level%20of%20trust. (Accessed: 17 October 2023).

What is a security zone? - definition by Techslang, Techslang. Available at: https://www.techslang.com/definition/what-is-a-security-zone/ (Accessed: 17 October 2023).

Use cryptography correctly (2015) IEEE Cybersecurity. Available at: https://cybersecurity.ieee.org/blog/2015/11/13/use-cryptography-correctly/ (Accessed: 17 October 2023).

Russel, D. and Gangemi, G.T. (1991). Computer Security Basics. Sebastopol, CA: O'Reilly & Associates. (Accessed: 17 October 2023).

Strang, D. and Moon, S. (1993). Network Security Secrets. San Mateo, CA: IDG Books Worldwide, Inc. (Accessed: 17 October 2023).

Freeman, C. (2022) Five cryptography best practices for developers: Synopsys Blog, Five Cryptography Best Practices for Developers | Synopsys Blog. Available at: https://www.synopsys.com/blogs/software-security/cryptography-best-practices.html (Accessed: 17 October 2023).

Rosencrance, L. (2020) What is ciphertext?Whatis.com. Available at: https://www.techtarget.com/whatis/definition/ciphertext (Accessed: 17 October 2023).

Lake, J. (2023) What is a collision attack?, Comparitech. Available at: https://www.comparitech.com/blog/information-security/what-is-a-collision-attack/ (Accessed: 17 October 2023).

Ciampa, M. 2022. Security+ Guide to Network Security Fundamentals. 7th ed. Cengage Learning, Boston, MA. Cengage (Accessed: 22 August 2023).