UTS KEAMAN INFORMASI

Name : Vanessa Dangremont

Nim : 20230801025

Essay:

1. Explain what information security is, according to you.

To me, information security means protecting vital information and digital platforms from threats, whether it come from outside hackers or internal mistakes. It includes putting in place protocols to safeguard sensitive information, like our personal data, financial records, or business information, from unauthorized disclosure, loss, or accidental alteration.
It's not just about technology in information security; policies, awareness, and healthy habits are also essential to ensure data is protected, trustworthy, and readily available. This involves employing tools such as firewalls, antivirus programs, and encryption to protect systems. For reduce human errors, which are among the biggest risks, employees must undergo continuous training.
The goal of information security ultimately revolves around maintaining trust, ensuring compliance, and aiding the overall success of an organization.

2. Explain what Confidentiality, Integrity, and Availability mean, according to you.

For me Confidentiality, Integrity, and Availability, collectively called the “CIA Triad,” serve as the essential principles underlying information security.

For me the concept of confidentiality refers to safeguarding information so that only permitted individuals can view it. For example, only you should have access to your personal messages or bank account information because it’s privacy.

For me the concept of integrity pertains to preserving the correctness and unaltered state of data unless changes are authorized by permitted users. This is about protecting data from unauthorized changes or accidental corruption.

For me the concept of availability implies that data and systems must always be accessible to users they need them. If users are unable to access the information, they need due to a system crash or attack, it indicates a failure in system availability. The security of systems depends on these three concepts working together seamlessly. If one of them is compromised, the entire system can be at risk. Many organizations develop their security policies around these three.

3. Mention types of security vulnerabilities you know!

It has a lot of different type of security vulnerabilities that's I know but the three type of vulnerabilities that's I choice is the one for ma that's the most dangerous and common to happen in the life in general.

The first one will be Weak password, Weak passwords are those that are simple to guess, short in length, or commonly used, including examples like birthday date, or a person's name. Accounts are vulnerable to hacking through simple brute-force or dictionary attacks when passwords are not sufficiently strong. This weakness is very common because many users prefer passwords that are easy to remember, even if that means sacrificing security unfortunately. A strong password should include a mix of uppercase and lowercase letters, numbers, and special characters for be harder to guess. Using strong passwords make it safer and give an extra layer of protection.

The second for me will be Phishing, In a phishing attack, cybercriminals impersonate trusted institutions such as banks, companies, famous person or government agencies or even someone that's we can know such as a friend or member of family to trick users into giving away personal information through social engineering techniques. Phishing attacks typically arrive as emails or messages with malicious links or fake attachments. After a user interacts with a fake site by clicking a link or submitting their personal information such as bank code, the attacker may steal credentials, install malware, or infiltrate accounts. Preventing phishing involves educating users to detect suspicious emails and websites, as well as employing email filtering solutions, also to always remember to never click on a APK file because it's not a normal file.

The third for me will be SQL Injection , The insertion of malicious SQL code into input fields on websites, such as those found in login forms or search bars, can lead to SQL Injection attacks, which enable cybercriminals to gain unauthorized access to or alter the database. When an application fails to adequately validate or filter user input, it becomes vulnerable to exploitation, allowing attackers to potentially access, modify, or erase sensitive information, including usernames, passwords, and credit card details. Furthermore, such attacks can be employed to circumvent authentication processes without requiring a password. To give a protection applications from SQL Injection vulnerabilities, it is important to implement secure coding practices, such as the use of prepared statements or parameterized queries, in conjunction with regular security evaluations.

4. Data security can use hash and encryption. Explain what you know about hash and encryption!

Both hashing and encryption are important techniques used to protect data, but they serve different purposes.

Hashing can be likened to the generation of a unique fingerprint for data. It transforms any input, such as a file or password, into a string of characters of fixed length. This process is unidirectional, indicating that it is not possible to revert the hash to retrieve the original data. Hashing is frequently employed for the secure storage of passwords; when a user inputs their password, it is hashed and subsequently compared to the stored hash. Access is granted if the two hashes correspond.

Conversely, encryption serves to safeguard data by converting it into a format that is not easily interpretable. This transformation can be reversed using a key, allowing authorized individuals to decrypt and access the original information. Encryption is commonly utilized to secure emails, files, and online communications. While hashing verifies that data remains unaltered, encryption ensures that only authorized users can access the information. Collectively, these mechanisms contribute to the preservation of both data privacy and integrity.

5. Explain what session and authentication mean, according to you!

A session can be defined as a transient interaction between a user and a website or application. Upon logging into a website, a session is initiated, allowing the system to recognize the user as they navigate through various pages. This session remains active until the user logs out or the session expires. It facilitates the tracking of user activity without the need for repeated logins.

Authentication refers to the process of verifying an individual's identity within a system. This process typically begins with the input of a username and password; however, alternative methods exist, such as biometric identifiers like fingerprints and facial recognition, or even verification codes sent to mobile devices. The primary objective of authentication is to ensure that access to specific information or functionalities is granted solely to authorized individuals.

Effective authentication mechanisms are essential in preventing unauthorized access to sensitive data. Sessions contribute to a secure and seamless user experience following login. Collectively, these elements are crucial in the management of user identity and the regulation of system access.

6. Explain what privacy and ISO mean, according to you!

Privacy involves managing who can access your personal information, how it is utilized, and with whom it is shared. In today's digital age, we often unknowingly share a great deal of data, including our whereabouts and shopping preferences. Effective privacy practices make sure that this data is kept secure and not exposed or misused without our approval.

Safeguarding privacy is both an ethical obligation and a legal requirement in numerous nations. European laws like GDPR set the rules for processing personal information. Maintaining privacy is essential for companies to build trust and steer clear of legal repercussions.

The International Organization for Standardization (ISO) is tasked with creating international standards to maintain quality, safety, and efficiency worldwide. Among the various standards in information security, ISO/IEC 27001 is considered one of the most crucial. It provides organizations with a well-defined structure for handling and safeguarding sensitive data. Using ISO standards helps companies follow best practices and build customer confidence. It also provides guidelines for risk management and security controls. Numerous organizations aim for ISO certification to validate their commitment to safety and reliability.