Sun Mon Tue Wed Thu Fri Sat

Information Security

Assigment # 1

Group Members

Zuia Tahir 211980052

Mahnoor Amir 211980063

Ayesha BiBi 211980004

Maryam Mustafa 211980068

Question no 1

Imagin you are - - - -

1- Identify three potential vulnerabilities in the company's current security setup

⟹ Security vulnerability

A security vulnerability is an unintended characteristic of a computing component that multiplies risk of an adverse event or loss occurring either due to accidental exposure, deliberate attack or conflict with new system components

Date:.....

Sun Mon Tue Wed Thu Fri Sat

There are numerous ways security vulnerabilities could enter your system.

Following are three Vulnerabilities

1-

Security Misconfiguration

A security misconfiguration arises when essential security settings are either not implemented or implemented with erross. Such error create dangerous security gaps that leave the application and its data (and thus the organization itself) open to a cyber attack or breach.

2-

Sensitive Data Exposure

Sensitive data is anything that should not be accessible to unauthorized access.

Date:

Sun Mon Tue Wed Thu Fri Sat

Sensitive data exposure occurs when an organization unknowingly exposes sensitive data. Such data exposure may occur as a result of inadequate protection of database. Sensitive data exposure can happen in several ways human negligence can cause data to be uploaded to public website Inappropriate access controls might lead to a single employee owning control over a huge database of sensitive information

3. Indequate Authentication

Authentication vulnerabilities arise when there are not enough checks and balances to reset passwords and credentials. This means that a hacker might exploit the "forget password"

option present in every login system to hack your account and find a backdoor to initiate an account.

Preventing Measures

1- For Security Misconfiguration

⟹ Configuration errors usually create warning signals that admins and developers should watch for. Red flags include notification of multiple login attempts, devices that self install software and user's web searches being redirected to unexpected websites.

⟹ A lack of cybersecurity knowledge results in insecure practices and human errors which increase

the risk of breaches- Employees must be trained about the need of strong passwords and rules for handling sensitive data

⇒ Secure coding practices are essential to prevent misconfiguration issues - Developers must assure proper input/output data validation in the code

For Sensitive Exposure

⇒ Catalog Data

In order to protect their consumers data, organization need to make sure they keep track of all the data stored within their system and perform an audit (analysis)

Date:.....

Sun Mon Tue Wed Thu Fri Sat

⇒ **Appropriate Security controls**

Organization must have appropriate security controls in place to avoid the sensitive data exposures as well as to limit their impacts on data subjects

⇒ **Assess Risks Associated to Data**

In order to protect data, organization need to have clear understanding of the data risk. The more sensitive the date is, the heigher the risk of harm will be.

Organization must have an effecient breach response mechanism in place to sudden ~~respond~~ to sensitive data exposure

Date:.....

Sun Mon Tue Wed Thu Fri Sat

For Indequate Authentication

⇒ Keep your systems, software, applications, networks and

⇒ operating systems up-to-date to protect from authentication bypass vulnerability

⇒ It is recommended to install a good antivirus program and patch all vulnerabilities

⇒ Ensure that all your systems, applications and folders are password protected

⇒ Security experts recommend having a unique and strong password than default passwords