Attempt all questions

43 marks

1. A software development company wants to protect their computer systems and data from unauthorised access.

(a) Identify two methods of physical security that the company could use to protect their computer systems.

1. Biometric access controls can be used, these can be fingerprint scanners or facial recognition
2. CCTV cameras can be used for any potential breakins into the company and monitor the use of the computer [2]

2 marks

(b) Identify and describe two software-based security methods that the company can use to protect their computer systems and data.

Method 1. Antivirus software

Description. Program that is designed to detect, prevent and remove any harmful softwares. The regular updates that it goes through makes sure that the computer system can fight off a variety of threats.

Method 2. Firewalls

Description. Monitor and control the incoming and outgoing data, preventing any unauthorised access and protecting the network from any attackers. They filter out any harmful data. [6]

5 marks

what does filter out mean? needs more clarity

2. A university wants to protect their data against threats when connected to the Internet.

(a) Describe the threat malware can pose to the university's network and give a prevention method that the university can use.

both data breach and sensitve data are related

Description Malware can be a significant threat to a university's network by potentially compromising sensitive data. Malware can also disrupt operations making the university harder to run due to the data breach

Prevention Antivirus and Anti-malware software can be used to avoid malicious software from being transferred into the network. [3]

2 marks

(b) Describe the threat a brute force attack can pose to the university's network and give a prevention method that the university can use.

Description Brute force attack is attempting to gain unauthorised access to accounts or systems through trialing of various usernames and passwords that are relevant to the University

Prevention Limiting the amount of times a user can enter a password after the attempts then they will be locked out [3]

3 marks

3. Data in computer systems is valuable and at risk of loss, damage or being stolen.

(a) The table has four potential threats to data.

Write one prevention method for each threat in the table. Each prevention method must be different.

Threat	Prevention method
Unauthorised access to computer	Passwords
Virus	Antivirus software

Phishing	Firewalls
Data interception	Encryption

4 marks [4]

(b) Name two other threats to the data in a computer system and give a method of preventing each.

Threat 1 Malware need to specify what kind of malware

Prevention 1 Use antimalware software to avoid the malware from affecting the computer

Threat 2 Hacking

Prevention 2 Use strong passwords so that hackers will not be able to have access to sensitive information [4]

3 marks

4. Hamish stores confidential documents on his laptop.

(a) Hamish needs his computer to be secure from unauthorised access when connected to a network.

(i) Describe the problems that can arise from unauthorised access to his laptop and confidential documents.

Attackers can steal and have access to sensitive information. These can be sold to companies making it a problem for the user. Unauthorised access can result in financial consequences as attaches and make transactions using the laptop of the user.

3 marks [3]

(ii) Describe two ways Hamish can help prevent unauthorised access to his laptop.

1. Hamish can use passwords in order to prevent

in 2nd point use firewall/biometrics or physical security

unauthorised access. A long and unique password will make it harder for the attacher to use brute force as there are more characters.

2. Log out the device after a few minutes if the laptop has been left unattended. This makes sure that other people do not have access to the laptop and have access to sensitive data [4]

2 marks

(b) If unauthorised access does occur, Hamish would like to use encryption to add another layer of protection to his documents.

(i) Explain how encryption helps to protect Hamish's documents.

Encryption allows Hamish to control who has access to those documents. Only those with the decryption key can have access to this information making it secure. Encryption also allows for secure transmission of the document, so if the document does get intercepted by someone else, they will not be able to view it. [2]

2 marks

5. A house has computers in each room and a central router. Every room allows both Ethernet and WiFi connections to the router.

(a) The house owner is concerned about potential threats to the network from being connected to the Internet.

(i) Identify three possible threats to the computers connected to the network.

Threat 1 Denial of Service Attacks can take place. These attacks disrupt the usual functioning of the computer by overwhelming the computer with

with useless information, this can lead to the computer to crash

Threat 2 Data interception can take place. Attackers can attempt to intercept the transfer of data being passed from one person to another. If this data is sensitive they can threaten the sender.

Threat 3 Phishing attacks involves people having access to people's sensitive information by looking like a trustworthy resource. This information can be used by the person in very malicious ways. [6]

6 marks

(ii) Give one way in which each threat identified above can be reduced or prevented.

Prevention 1 Biometric access controls

not related to DoS (use traffic monitoring or analyzing traffic)

Prevention 2 Encryption software

Prevention 3 Use firewalls [3]

2 marks

6. An online supermarket stores customer account information in a database.

The supermarket recently suffered a security breach where customer information was stolen.

(a) A common way for databases to be breached is through SQL injection. Explain how SQL injection works.

Involves inserting malicious SQL code into the network giving access to the database to the unauthorised person. Attackers can use this data against the online supermarket. [2]

2nd point tells the loss it will incur not how the method works

1 mark

(b) The supermarket believes the data was stolen through social engineering.

Describe an example of how the thieves could have used social engineering to steal the data.

Thieves can act as IT support who claim to help the client. However when the data gets sent from the client to the thiefs, the thiefs will have access to the data which can put the client in a tricky situation [2]

2 marks

7. A company uses a firewall to protect its network.

(a) Explain how firewalls enhance data security on the network.

Firewalls act as a barrier between the user and external networks and data that is being transferred to the user. They filter unauthorised data and those who are trying to access the network. Firewalls allow trusted and secure data to be transferred to the user keeping the network safe. [3]

3 marks

(b) Devices on the network are automatically logged out if they are inactive for more than 5 minutes.

Explain how this helps protect the network.

Automatic logout ensures that if a user leaves their device unattended, there will be no unauthorised individuals who gain physical or remote access to a device. This avoids any insider threats if the person trying to access the network happens to be in the same geographical area as the user. [3]

3 marks