**Learning Aim B – Cyber Security**

2. **Internal Threats and impact of Breaches**

1. Internal threats to digital systems and data security (insiders and trusted individuals)
2. Unintentional disclosure of data
3. Visiting untrustworthy websites and downloading files from the internet (drive-by-downloading, search engine poisoning)
4. Use of portable storage devices
5. Users overriding security controls
6. Intentional stealing or leaking of information
7. Impact of a security breach (data and financial loss; damage to public image; reduction in productivity and downtime; legal action)

3. **User Restrictions and finding weaknesses**

1. User access restrictions (physical measures)
2. Access control and authentication (access control systems, authentication)
3. Passwords
4. Two factor authentication and multi-factor authentication
5. Biometrics
6. Using correct settings and levels of permitted access (the principle of least privilege)
7. Finding weaknesses and improving system security (ethical hacking and penetration testing – white hat hackers, black hat hackers, grey hat hackers
8. System and behaviour analysis (who logs and when)
9. **System attacks and external threats**
10. Threats to digital systems and data
11. Why systems are attached? (fun, challenge, financial gains, industrial espionage, personal attacks and “hacktivists”)
12. External threats to digital systems and data security (unauthorised access – exploiting a security vulnerability, hacker, black hat hacker)
13. Malware (virus, worm, rootkit, ransomware, spyware, botnet, DoS)
14. Social engineering (phishing, spear phishing, blagging and shoulder surfing,
15. Pharming and man-in-the middle attacks

4. **Data Level Protection**

1. Data protection (defence in-depth)
2. Firewall (hardware firewall, software firewall)
3. Anti-virus Software (signature-based detection, quarantined or behaviour detection)
4. Device hardening
5. Software/ interface design
6. Encryption (symmetric encryption and asymmetric encryption

5**. Policy, Backups and data recovery**

1. The need for and nature of security policies
2. Roles and responsibilities (Information security manager, data protection officer)
3. Reporting (whistle blowing policies)
4. Defining security parameters
5. Password Policy
6. Acceptable use policy
7. Parameters for device hardening
8. Disaster recovery policy
9. Backup and recovery
10. Actions to take during and after an attack

**1. System attacks and external threats Questions**

1. **A malware attack can have serious consequences for an organisation**. Describe two types of disruption a malware attack can cause. [4]
2. **SmartThings is aUK-based company that develops Internet of Things (loT) solutions for the home. Since its set up in 2012, the company has been targeted several times by hackers.**
3. Explain what is meant by the term 'hacking'. [2]
4. Give four reasons why a hacker might attack the company's digital systems. [4]

1.

2.

3.

4.

1. The company found and repaired vulnerabilities that could lead to a ransomware attack. Describe how a ransomware attack works. [3]
2. **Social engineering works by manipulating people into voluntarily giving away information. Describe two techniques used in social engineering attacks.**
3. **ActivWear is an online clothing company which sends out printed catalogues to thousands of customers on its mailing list. It accepts orders online, by mail or by telephone. Discuss the external threats, both deliberate and accidental, to ActivWear's computer systems which may have serious consequences for the organisation.**

**2. Internet Threats and impact of Breaches Questions**

1**. ODS is a global mining company. It employs over 3000 people in sites all over the world. The company's digital systems and data are vulnerable to external and internal threats.**

1. Explain two ways in which an internal attack differs from an external attack. [4]
2. ODS has put in place a number of security controls to protect its digital systems and data. Explain two reasons why employees may be tempted to override these security controls. [4]
3. Explain two ways in which employees' use of portable storage devices, such as flash memory drives, poses a s'ecurity risk. [4]

2. **Credit2000 is a credit card company which has more than one million customers. Shoppers use their cards to pay for goods at tills in stores, or when ordering goods or services online. Discuss the impact that unauthorised access to personal data stored on company computers could have on Credit2000. [6]**

**3. System attacks and external threats Questions**

1. GreenLeisure Limited is a holiday company offering a range of activities.

(a) The company's network server is located at its head office. It is in a dedicated server room with secure access. Entry to the server room is currently controlled by an ID card system. The company wants to replace this with a biometric fingerprint scanning system. Explain two advantages of using a biometric access system rather than an ID card system. [4]

(b) The company employs a number of instructors to run outdoor activities for holiday makers. They log on to the company network to find out how many people are booked onto each activity. Office staff handle customer bookings and payments. Explain two ways in which file permissions can be used to control how instructors and office staff access customer data. [4]

2. Manjit is an ethical hacker. She works for a well-respected security company.

(a) Describe the role of an ethical hacker. [2]

(b) Explain the difference between a 'grey hat hacker' and a 'white hat hacker'. [2]

(c) One activity carried out by an ethical hacker is penetration testing. Describe what is meant by the term 'penetration testing'.

3. Lawrence University is a major provider of higher education. More than 20,000 students attend lectures and tutorials on its campus. The university is carrying out a review of security. Discuss the security measures the university should take to control access to its facilities, digital systems and data. You should consider: [6]

• physical security measures

• levels of permitted access

• system and behaviour analysis

1. **Data Level Protection Questions**

**1. Conor uses a laptop to carry out work-related activities.**

(a) Explain how anti-virus software will protect data stored on Conor's laptop. (4]

(b) The laptop has a software firewall installed. When Conor goes into the office he plugs his laptop into the company network. The network is protected by a hardware firewall. Explain how the hardware and software firewalls work together to enhance data security. [3]

**2. Installing a firewall is one device hardening technique.**

(a) State the purpose of device hardening. [1]

(b) Explain three other device hardening techniques. [6]

3. Explain how encrypting data during transmission protects it from being read by an unauthorised person who intercepts the transmission. [2]

**4. This table lists five tools used to protect and manage digital systems and data. Complete the table. The first row has been done for you. [6]**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Function** | **Firewall** | **Anti-virus software** | **Device hardening** | **Software/ interface design** | **Encryption** |
| Detects malware using a database of signatures |  | ✓ |  |  |  |
| Protects data from being read during transmission |  |  |  |  |  |
| Prevents a virus from spreading across a network by dividing the network into segments |  |  |  |  |  |
| A series of measures designed to make computers less vulnerable to attack |  |  |  |  |  |
| Prevents employees from visiting malicious websites |  |  |  |  |  |
| Quarantines suspicious files |  |  |  |  |  |
| Reduces the security risk posed by users |  |  |  |  |  |

**5. Policy, Backups and data recovery Questions**

1. **CleverTech develop Internet of Things (loT) devices for the home.**

(a) Describe two ways in which the company can make its staff more security-conscious. [4]

(b) Anya works in the marketing department. She has found a free image editor on a website and installed it on her company laptop. Describe how an organisation's security policies would prevent this sort of behaviour. [2]

(c) The company has a password policy. One rule of the policy is that passwords must be changed every three months. Explain two other rules that would increase the security of passwords. [4]

2. Mina is the Information Security Manager of a large hospital. Discuss the issues she should consider when deciding on procedures for backup and recovery. [2]

3. A secondary school has fallen victim to a ransomware attack. All the students' GCSE coursework has been encrypted. The malware found its way onto the school's network because a teacher failed to recognise a phishing email.

(a) Explain what is meant by the term 'phishing'. [2]

(b) Describe how an acceptable use policy might have prevented a successful phishing attack. [3]