**Task 1 – IT Security Systems and Encryption**

**Unit 7 - IT Security Systems and Encryption**

**Mohammed Mahin Ibnay Mamun (346584)**

**Type of Threats**

The financial and reputational outcomes of cyberattacks can be devastating for businesses. Security issues sometimes exist in businesses' systems which users are not aware of this information. It is quite common for organizations to be hacked internally, accidentally, intentionally, or maliciously.

**Internal Threat**

Internal threats are those that originate from within the company.

**Deliberate Internal Threats:**

**Employee Actions:**

A disgruntled employee might end up damaging or deleting documents maliciously as a form of revenge. In addition to destroying files and software, these threats can also compromise customer data. There are also instances where some employees who have access to important data threaten to post information about the company on the Internet.

**Data Theft:**

If an employee has access to data or is fired, or if an employee was dismissed from the organization, they can steal from the organization. The reason behind this attack is that most employees have direct access to this data with permission from the organization to edit, view, add data to it or remove it.

**Users overriding security controls:**

An employee is sometimes tempted to bypass the built-in security controls on the network, these security controls are often used to safeguard the information on the network. Those who breach these controls often do not consider the consequences of their actions, it is possible for malware to be installed on a network due to this.

**Accidental/Unintentional Internal Threats:**

**Accidental Loss:**

The most common cause of accidental data deletion and corruption is poor training and misunderstanding of procedures for employees who have access to important data. A lack of software design can also lead to data loss since some of the best ways to recover data, such as recycling bins built into operating systems, are not available on all systems.

**Unintentional disclosure or damage to data:**

Besides numbers, addresses, and card details, employees can also accidentally divulge confidential information. Also, corrupted data could be damaged by the employees. While not in use, some people leave their computers unlocked. It is also possible for employees to expose their own personal details since some staff members leave their passwords on display in the room.

**Unsafe Practices:**

Risky practices could include any practices that pose a threat to an individual or worker. By performing actions that leave the company's computer system vulnerable to external hackers, employees may expose the company to security threats. There are many ways to accomplish this, below is a list of unsafe practices:

**Employees using external storage devices:**

Connecting personal storage devices to work on computers and laptops is very risky for employees. This is primarily because malware or viruses on the storage device can spread to the work machine. Additionally, connecting an external storage device to your work computer is a risky move because other employees and hackers may copy or download your personal information and data, which may cause many problems. As a result, your personal information can be obtained, such as: name, address, date of birth, card information, and anything else you have stored on your device.

**Visiting untrusted websites:**

A website that is untrusted is susceptible to cyberthreats, including malware and cyberattacks. A cyberattack can affect your site's operation, prevent your visitors from accessing it, or compromise customer information.

**Downloading files from the internet from untrusted websites:**

Visiting websites, we cannot trust or unknown websites where we can download any files or share our login credentials should be avoided. Untrustworthy websites can silently deliver malware through downloaded files, potentially compromising your safety.

**Using file sharing software that is not trusted:**

The employee might inadvertently download and introduce malware from the file-sharing service if they select a risky file. This malware could include viruses, spyware, worms and many other cyberattacks leaving the company vulnerable.

**Employees bring their own devices to work and connect that device to the organization's network:**

Any malware on those devices is exposed to the network when employees connect their own devices from home to the network. It is not necessary for companies to provide employees with devices when they use their own. BYOD can be incorporated into the acceptable use policies of an organization as a result, which reduces the associated security threats.

**External Threats:**

There are a variety of sources of external threats to an organization. As a rule, cybercriminals aim to steal information or hold companies or individuals to ransom by encrypting data or blocking access to services. A method for protecting data is to encrypt it or block access to it. In some cases, competitors may want to target an organization to gain a competitive financial edge. Such behaviors are usually criminal in nature.

**Example of a cyberattack/cyberterrorism:**

Cyberattacks may also be used as a form of warfare when one country attacks another when there is a political motive, such as by protesters or groups of individuals targeting an organization with which they disagree politically, ethically, or based on religion.

When it was first found in 2010, Stuxnet was an infamous computer worm because it was used to attack Iranian nuclear facilities. Due to that attack, headlines were around the world.

Stuxnet was originally designed to attack programmable logic controllers (PLCs) that automate machine processes.

While Stuxnet is malicious software in the sense of a computer worm, it has also been used to attack electromechanical equipment.

**Physical Threats:**

It is possible for computer equipment to be stolen or maliciously damaged, especially if it is valuable. Security is particularly at risk from theft or loss of portable equipment which may contain sensitive data since a hard disk is discarded by a computer once it is removed from the system.

**Social Engineering and software driven threats:**

A social engineer uses methods, such as hacking security or sending money, to persuade a victim to take some sort of action that may be questionable. The purpose of social engineering is to trick computer users into providing secure information to cybercriminals. The purpose of social engineering is to use software made with malicious intent.

**Shoulder Surfing:**

When a criminal watches over a victim's shoulder as they use electronic devices, such as ATMs, payment terminals at checkout, or even laptops or smartphones. They look over their victims' shoulders as they do this. Because it can lead to bank fraud and theft, this is extremely dangerous for the victims. If you type your pin on an ATM machine, cover it with your hand to avoid this happening.

**Spear phishing and whaling:**

Spear phishing: These are also forms of phishing that target a specific individual to obtain sensitive information about that person. Securing the target's click is accomplished by dressing up as a trusted individual and using a spoofed email to trick them.

Whaling: in whaling attack, the goal is to steal sensitive information from a company, habitually for malicious reasons, such as financial details or employee personal details.

**Dumpster Diving:**

The technique of dumpster diving is still used nowadays. With more advanced technology, it is still possible for people to dumpster dive. Dumpster diving does not require any technical skill which is why it is so easy for one to do. Information retrieval techniques can be used to launch attacks on computer networks. It is possible to find information that one could use against a victim using this method. For example, they might find a piece of paper with a victim's bank details or passwords.

Types of malwares

|  |  |  |
| --- | --- | --- |
| **Type of Malware:** | **What is it?** | **Solution:** |
| **Virus** | Typically, a computer program files itself as another program and inserts its own code when it is executed. | - Delete files  - Scan device for threats  - antivirus scans |
| **Worms** | Viruses replicate themselves to spread to other computers. | - antivirus scans  - remove software  - antivirus and antimalware software's |
| **Trojan Horse** | It is a program that appears innocent but is harmful when downloaded and installed on the computer | -disable function  -restart device  - control panel -> add and remove programs |
| **Ransomware** | Data, documents, and other important files are locked and encrypted and then the attacker demands payment to unlock and decrypt the data. | - backup data  - update software  -turn on ransomware protected files |
| **Spyware** | Using this software, the user can obtain data from another user's hard drive-in order to convert information on those activities. Also use keyloggers. | - backup data  -run spyware cleaners  - disable any keyloggers |
| **Adware** | When a user is online, it automatically displays or downloads marketing materials such as banners and pop-ups. | - do not click on them  -scan your device  - uninstall the adware |
| **Rootkit** | An unauthorized person can gain access to a computer system without being discovered by using software tools. | -remover tool  - add a pin to your files  -hide important files in other root files |
| **Backdoor** | Using this method, an unauthorized remote user can access a computer without going through normal authentication procedures | -use antimalware tools which are reliable  -change your password and make it strong |
| **Logic Bomb** | Secret instructions that are embedded in a program to execute when a specific condition is met, usually with adverse consequences. | - use strong antivirus  - avoid pirate software's  -keep antivirus updated |

Example of a type of malware: (Ransomware)

A 2048-bit RSA key is used by Crypto Locker to encrypt files, which are renamed with an extension, such as cryptolocker, to reveal the keys. There is also ransomware that simply freezes your computer and asks you to pay a fee.

**Passive and active threats**

Threats can be passive or active, as shown in the following examples:

Wiretapping: A device that listens to telephone conversations secretly by connecting it to the line.

Port scanning: Port scanning can also be used to determine if a system's ports are accessible or visible over a network.

Idle scanning: Spoofing packets to determine what services are available on a computer by sending spoofed ones.

**Most common threats to computer systems:**

**Injection/SQL Injection:**

This technique consists of inserting malicious SQL statements into entry fields to execute in data-driven applications, it allows criminals to access sensitive information on you, Information about customers, personal information, trade secrets, and intellectual property is included in this category.

**Unprotected sensitive data:**

Identity theft, fraud, and theft of financial resources from employees and customers occur because of unprotected sensitive data. In the public and private sectors, data breaches affect large and small businesses alike. The reason hackers target small and midsized businesses today is that these networks are less secure because of their nature.

**Broken authentication:**

Specifically, session management and credential management are weak points. Using either method to hijack session IDs or steal login credentials, attackers can create either effect.

In addition to credential stuffing attacks, attackers also use highly targeted schemes aimed at accessing specific users' credentials to exploit these weaknesses.

**Availability/Data Integrity:**

**Server Redundancy:**

When it comes to redundancy, having a backup server ready and waiting in case your primary one fails is the goal. Many people, especially those who are employed by a company or business, will have this. In the event of a disaster and a live server becoming unavailable, redundant servers can provide businesses with a cost-effective backup to access vital data.

**Data Redundancy:**

Redundancy of data is the practice of keeping data in multiple places in a database or data storage system so that, if the data is lost, the organization can continue its operations. A complex process or ineffective coding can result in accidental data redundancy, while intentional redundancy results from intentional factors.

RAID:

A redundant array of independent disks Provides data redundancy in the event of a failed drive by storing the same data in multiple locations on one hard disk or solid-state drive (SSD).

The RAID system works by storing data on multiple disks and delaying input/output (I/O) operations to improve performance. The increased mean time between failures during this process is a result of storing data redundantly on multiple disks in addition to improving performance.

**Legal requirements and criminal acts**

Copyright, design, and privacy laws require all organization data to meet the requirements of the law as well as the data protection act. The data protection act requires that all information organizations collect about consumers be accurate and protected. In criminal acts, it is stated that any attempt to attach malicious code or modify files or to gain unauthorized access to computers will be illegal. Examples include the Computer Misuse Act and the Fraud Act. Phishing is also a violation of the fraud act because it is an attempt to deceive.

Copyright laws help organizations because the products or services that they create are protected, which means that other companies or individuals cannot copy or use what an organization has created.

When an organization discovers that their data has been revealed or used against them, they can use the computer misuse act to prosecute the attacker since the attacker has access to their systems and data unauthorized by them.

**Consequences of Security Breaches**

**Operational Impact on an organization of the loss of data or service:**

A company that discovers that their data has been exposed or misused may be able to prosecute the attacker under the computer misuse act since the attacker is gaining access to their systems and data without authorization. This can have adverse effects on an organization's ability to do business. A loss of data or financial impact can result, of this can limit an organization's ability to do business in the future.

An attack of this degree can produce devastating results for an organization, especially if any data is lost, encrypted, corrupted, or copied. If this occurs, then the effects could last a long time and be very damaging.

**Financial Impact of loss of service, such as an e-commerce website:**

The way in which organizations function and their financial performance may be impacted significantly, including e-commerce websites/businesses. The costs of investigating security breaches will not only be incurred by businesses, but they will also suffer a revenue loss while the services are down. Businesses will have to pay for the cost of investigating the security breach as well as the loss of revenue while the services are down.

**Damage to reputation:**

It has been reported that security breaches cause many users to have their personal details stolen or made public after a breach has been detected, even after a security breach has been stopped. Therefore, a lot of users depend on their organization to maintain adequate security and access to their data.

An organization that has been breached can damage its reputation as being secure, causing users to stop using that service even if they were not affected, as they may no longer trust them to protect their data moving forward.

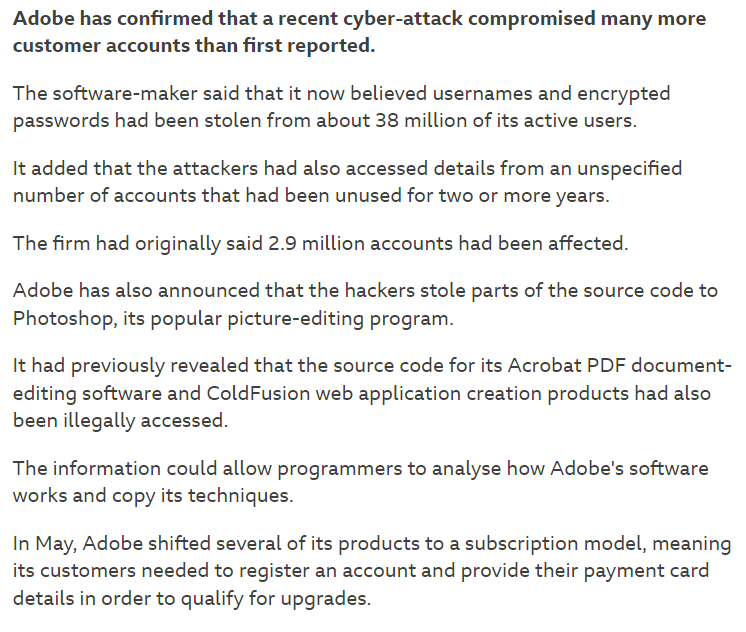
**Legal consequences:**

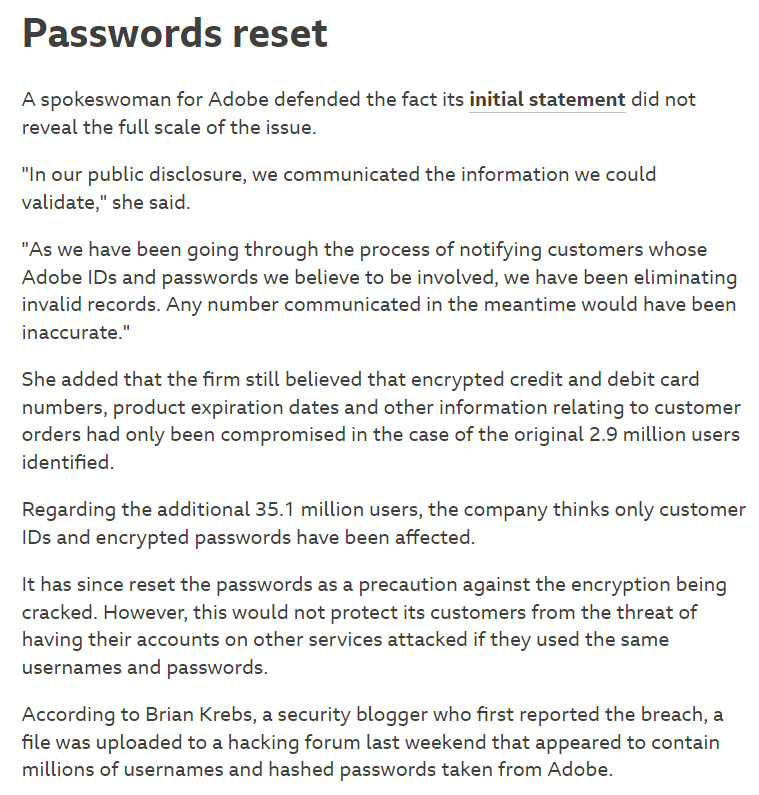
It is the legal obligation of most organizations to protect their users' data since many of these organizations hold very private and sensitive information that could adversely affect users if that information is revealed. The data protection act says that all data must be kept as secure as possible, so an organization experiencing a security breach may be deemed neglectful. This can be used legally.

**Case study: Adobe**

Several sources on the internet have still written about this huge cyber-attack on Adobe. For example, I found a headline on BBC news which mentions it.







**About Adobe**

Founded in 1982, Adobe is a California-based company. Adobe Systems, also known as Adobe, is a software company that develops multimedia and creative software. Its most popular products are Photoshop, Acrobat Reader, and Adobe Creative Cloud.

**What happened**

In 2013, Adobe unfortunately was the victim of a large cyber security breach of which the passwords, usernames, and credit card details of over 30 million Adobe accounts were leaked to the public. Innocent Adobe users were fortunate that some of their credit card information was encrypted and hashed, which prevented their information from being exposed. The attackers had access to Adobe programs such as Photoshop and Acrobat.

**What led to its discovery?**

Before the breach took place, about a week had passed until the owner of hold security, Alex Holden and Brian Krebs who is well known for hunting cybercriminals came across 40GB of data was transferred from Adobe to a criminal server. Prior a few days, the world found out about this case Aswell as Adobe.

**Are IT professionals responsible?**

The hackers gained access to it after exploiting three mistakes made by Adobe's IT department. All three of these steps involved encryption.

* They made an obvious mistake: The same key is used to encrypt all their passwords. That is something that every IT professional with a sense of responsibility should avoid.
* In addition, the company used a dangerous encryption method called ECB mode. By using this method, equal passwords end up looking identical when encrypted. Therefore, criminals will be able to break them much more easily.
* Finally, they failed to encrypt password hint points.

**How can Adobe make their system safer and prevent these attacks**

Adobe can prevent similar attacks in the future by focusing on three main areas. These 3 specific areas were mentioned before, and they all consist of encryption. Overall, the staff at Adobe need to upgrade their encryption techniques so further attacks don’t take place. The company should

* Strengthen passwords
* Use different keys within encryption
* Switch from ECB or test the method thoroughly before using it.

**Is There Anything to Learn from This? (customers)**

* It is very important to reinforce the importance of not using the same password twice.
* Additionally, customers should be forced to select long and complex passwords.