System Security

Assignment 1

Unit 07

George Hotten

Task 1

What malicious threats are there to an organisation?

There are many different malicious threats to an organisation, here is a list of some of the threats an organisation can face and what they mean.

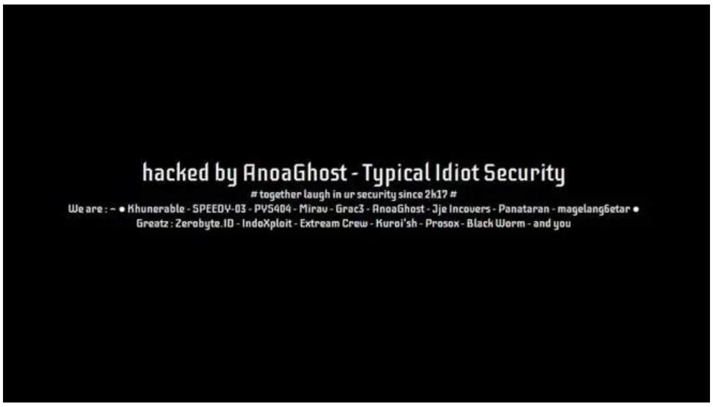
Term	Definition
Trojan Horse	A trojan is a type of malware that disguises itself as another application and, once executed, causes havoc on the system. It can often provide a 'back door' into the system for hackers to use later to steal data or do even more damage.
Virus Attacks	Viruses are self-replicating software that causes either damage to a computer system or steals data. It is often 'baked' into software such as pirated games, emails and downloaded files.
Worms	A virus that duplicates itself and spreads itself throughout a network using open network shares, email, or Internet Relay Chat.
Phishing	Phishing is where a criminal pretends to be a legitimate company (e.g., a bank) to try and lure somebody into giving them sensitive info. For example, login details, bank details, etc.
ID theft	Identity theft is when a fraudster has so much information on a person, they can impersonate them to the point where it is hard to tell the difference. People often do this to steal from a person or get benefits that person is entitled to.
Piggybacking	Piggybacking is when someone who is unauthorised to access a system uses someone who is authorised to access it. This can be both physical (e.g., holding the door open for someone unauthorised to enter a building) and digital (e.g., giving your username and password to someone unauthorised).
Tunnels	A tunnel is a secure encrypted connection between two devices. You are unable to crack it without a cryptographic key, meaning no one can access the data. This hides what users are doing and it makes it harder to be traced. This means hackers can use tunnels to invade a

	system and will have little chance of being caught.
Hacking	Hacking is when someone attempts to break into a computer network with malicious intent to damage the system or to access sensitive data. This is done by finding and exploiting a weakness or vulnerability in the network. Hackers usually do this to hold companies to ransom over sensitive data or as an act of protest.
Key Logging	Key logging is where someone installs a program that records every time they press a key on their keyboard. This data is then sent to hackers. This can reveal the user's passwords and other sensitive information they type out on their keyboard: for example, bank details.
Magic Disk Tactics	Magic Disks are devices that allow you to boot into a different operating system than the one installed on the device. This allows criminals to access data from the drive, and therefore install programs, steal data or erase data.
Man in the Middle Attacks	A Man in the Middle attack is where an attacker intercepts the data sent from computer A to computer B before it reaches computer B. As it hasn't yet reached computer B, the attacker could modify the data and then send it on to computer B. The attacker can do the same when data is being sent from B to A: intercept it before it reaches computer A. Instead of modifying the data, they could just steal it and relay it on, or steal it and drop the packet all together.

What threats are there to an e-commerce platform?

Website Defacement

Website defacement is an attack where the appearance of the website is modified. This is done by hacking into a webserver and editing the files of the web server to change its appearance. This can include replacing the site's official homepage to a message, such as the following:



hacked by AnoaGhost - Typical Idiot Security

together laugh in ur security since 2k17

We are : ~ ● Khunerable - SPEEDY-03 - PYS404 - Mirav - Grac3 - AnoaGhost - Jje Incovers - Panataran - magelang6etar ●

Greatz : Zerobyte.ID - IndoXploit - Extream Crew - Kuroi'sh - Prosox - Black Worm - and you

This was seen on the NHS website in 2018.

Control of Access to Data

Control of access to data ensures that only people who need to see specific data can see it. For example, sellers on e-bay don't need to know the card information someone paid with, or their purchase history with other sellers. They just need to know the data required to fulfil the sale – for example what they ordered, how much and where they want the product shipped to.

If someone has too much access to data they don't need, it could put people at risk of being hacked. If sellers know the bank details a person paid with, they could use that to steal money from their account.

Denial of Service Attacks (DoS)

A DoS attack is where a web server is flooded with requests causing it to become slow and unresponsive and may eventually crash. This is a threat to e-commerce platforms. If customers are unable to access their website to buy items, the company will lose money and potentially los customers.

What are counterfeit goods and how can they affect a company's sales?

Counterfeit goods are fake versions of something a company makes. For example, someone could sell fake designer shoes or a fake version of a game. This means the person who is buying it is getting intentionally misled and loosing money on something that isn't the genuine. This also means the genuine company that sells the product is losing money as the customers aren't buying from them. If the counterfeit goods aren't good quality, and the person who bought them doesn't realise they're fake, it could mean the genuine company could lose the customer as the customer may think all their products are low quality.

Conclusion: what happens if any of these happen?

If these threats occur, the organisation is going to lose out on money and may start to gain a bad reputation as people would think the seller sells low quality items, aren't secure with their data or doesn't offer a reliable service. This means less people will buy from them and the company may eventually go out of business as they are not earning enough money to be sustainable. This would put many people out of work too, causing financial issues for them.

Task 2

Key Locks

Locks can keep systems secure as they can prevent unauthorized people from entering certain rooms, for example where servers are. They must have the correct key to open the door to access the room. Only people who are authorized to interact with the servers should have a key. If one gets lost: all keys should be revoked, the locks changed, and new keys given.

Pros:

- Doesn't require any technology
- Simple to setup and maintain

Cons:

- People can lose the keys easily
- Locks can be picked
- The keys can be copied and redistributed

RFID Locks

RFID (**R**adio **F**requency **Id**entification) Locks uses cards or fobs with specific data encoded onto them as verification. This is read by a card reader using electromagnetic fields that is connected to a (usually) magnetic lock. If the card is valid, the door will unlock. Similarly, to key locks, they can be given out to people who need them. Only people allowed in the area the lock is protecting should have them. Unlike keys, the cards don't need to be handed back in to be revoked.

Pros:

- Much harder to copy
- Securer than regular keys
- More convenient

Cons:

- Requires electricity
- More expensive

Visitor Passes

Visitor Passes can help identify people on the site so other staff members know they are authorized to be in the facility. If someone is seen not wearing / having a visitor pass, they should be reported to the site's security as there may be a security breach as someone has entered the site without authorization.

Pros:

- Identifies people in a secure facility
- Provides a way to ensure everyone is authorized to be where they are

Cons:

- Could be forged
- People could leave their badge somewhere in the facility
- It is up to other members of staff to challenge anyone without an ID

Sign in / out

All staff must sign in when they enter a facility and sign out when leaving. This keeps a log of when staff have been in the facility and if someone is noted to have not left the facility by the time it should close or after a certain amount of time has elapsed, there may have been a security breach.

Pros:

- Shows how long, what time and when staff members have been on site
- Shows if someone is taking a long time to do a short task

Cons:

- People may forget to sign in or out

Biometrics

Biometrics is using part of your body to authenticate you are really who you say you are. This could be done by verifying a staff member's fingerprint, face, voice, retina, etc. This adds an extra layer of security to prevent any impersonation or attempts of trying to access someone else's data or access data only they can see.

Pros:

- Ensures people are really who they say they are and makes them prove it

Cons:

- Can sometimes be unreliable and doesn't work 100% of the time (more likely for false negatives than false positives, however)

Cable Shielding

Data traveling using electromagnetic, or radio transmission is at risk of being intercepted by analyzing the magnetic field around a cable. Cable shielding is used to protect the data from being intercepted and to protect the cable from magnetic interference. This is done by protecting the cable around dielectric insulator and a metallic shield.

Pros:

- Helps protect from data interception
- Prevents interference during the transmission of data
- Helps the robustness of the cable

Cons:

- More expensive to produce
- Makes the cables heavier

Task 3

The consultancy has asked me to create a form of FAQs for employees to use. Here are the answers to the following questions

What is meant by encryption?

Encryption is securing data via mathematical techniques. It takes plain text and uses an algorithm to scramble the data to make it unreadable. This is done through the public key. A private key is then needed to decrypt the data to turn it back into a readable form again.

What is meant by handshaking?

To help ensure the two devices communicating with each other over a WAN are trustworthy (e.g., not mimicking legitimate requests), both devices before a **C**hallenge **H**andshake **A**uthentication **P**rotocol (CHAP). When performing a CHAP, the server sends a challenge message to the requestor, if the requestor responds with a value obtained by using an irreversible MD5 hash, the authentication is accepted. If not, the connection is terminated.

Why do you recommend the use of diskless networks to improve security?

A diskless network is where workstations do not have ports for storage mediums such as USB, CDs, floppy disks, etc. I recommend this as people are unable to plug in any malicious devices into the companies' machines which could steal data or infect the system. It also prevents unauthorized copying of company files.

Why should data be backed up?

Data should be backed up in case of a disaster where a device has a drive failure and loses all its data. A backup is where all data from a drive is copied and stored in a safe location in case of a data loss. This location is often stored off site and can take a long time based on how large the backup is and where the data is being transferred to.

Why should employees change their password frequently?

Employees should change their password regularly as it can keep their account safe and secure. If the password is guessed and the employee isn't aware, the regular changing of passwords will lock them out.

Why does a network need various levels of access?

Different levels of network access are needed to ensure that people can only access what they need to on a network. For an example, a regular user shouldn't be able to see finance documents for the company they work for, only the accountants should. This is often managed by the central server.

What is an intruder detection system and why should networks consider having one?

An intruder detection system (IDS) are methods used to detect when someone not authorised has entered a system. Some systems just record the attempt, others use a firewall to block the request. Traffic control can also be used through Access-control lists which create traffic-based rules for all devices connected to it. Networks should consider having an IDS in place to prevent any data loss, leak, or outage time when someone breaks into its system as it should attempt to stop them from getting access.

Task 4

A client has asked me to join a discussion about the security of information. Here are some notes I have written up about the topic and how they are related to organisational threats.

Data Confidentially

Confidential data collected must be used lawfully and fairly, for explicit purposes that the user knows about, it is only used for what is necessary, it must be up to date, not kept longer than needed and held securely with protection against unauthorized access. If a server is breached and the data leaked, the company will be liable under the Data Protection Act and could be sued by their customers. This breach could also make the company lose customers as customers may not trust the service to hold their information securely. However, customers do have the right to view the information the company has on them through the same Data Protection Act.

Data Integrity

Data integrity is maintaining data to ensure that it is accurate, consistent and in context. This makes the data useful to the owner. Data integrity also includes data integration, data quality, location intelligence and data enrichment. Data integrity is important because, especially for advertising, accurate data is very important as inaccurate data can cause incorrect insights, and misleading analytics. If data is incorrect, the company could lose out on revenue as they could be targeting the wrong people for their advertising.

Data Completeness

Data completeness is the wholeness of your data and its comprehensiveness. For the data to be referred to as complete it mustn't have any gaps or missing information. This is important as if data is incomplete, it can cost the company money as it could lead them to target people who aren't in their target audience. It is also important as if it is incomplete consistency and accuracy errors may come up making the data less reliable.

Access to Data

People should only have access to the data they need to complete their job. For example, a customer service agent should not have access to someone's banking information, and a web designer shouldn't have access to anyone's data. If people have the wrong access levels, it could lead to people gaining access to everyone's data which could cause a data breach. If this data breach occurs, the company could lose the trust of customers. The data breach could affect the customers as their personal information could now be exposed to everyone on the internet.

Task 5

What is encryption?

Encryption is the method of securing data via mathematical techniques. The method usually needs a public key to encrypt the data and a private key to decrypt it. When data is encrypted, it is impossible to read and understand unless you have the private key which will make it readable again. For example, when unencrypted data is sent across a network, hackers can often intercept the packets being sent a read the data from inside them. However encrypted data being sent cannot be read as the data inside will just seem like gibberish.

How strong is encryption?

Some encryption methods are stronger than others. For example, weaker encryption such as a Caesar Cipher is easier to crack as there is less scrambling done to secure it, meaning it is very easy to reverse engineer the changes. However, a strong encryption such as AES uses many different methods of scrambling the data and therefore makes it very hard to decrypt without knowing how it was done (e.g., without the private key).

Caesar Cipher Example

The Caesar cypher works by shifting the alphabet down by a certain number of letters. It is weak as there is a limited number of combinations which can be easily cracked.

An example of a Caesar shift 4:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z – this is the original alphabet without any shifting

E F G H I J K L M N O P Q R S T U V W X Y Z A B C D – this is the shifted alphabet where A becomes E

I will perform a Caesar cipher on “This is a test of encryption”. To do this, I align the two alphabets and find each letter of the message on the top alphabet. Once found, I go down into the shifted alphabet to see what letter should be used. This means “This is a test of encryption” would be “Xlmw mw e xiwx sj irgvctxmsr”

Advanced Encryption Standard (AES) Example

The AES encryption is a strong method of encryption as it has a set pattern for shifting the characters in a message that is put into a table and it repeats this a certain number of times. The shift pattern and number of times it performs the shift depends on the key. This is strong as characters can be shifted both across and downwards. This is also dependent on the key. Here is an example of performing an AES on “Xlmw mw e xiwx sj irgvctxmsr” from the previous encryption using 1 round, 2 row shifts and 1 column shift. All spaces get replaced by a star.

First let’s put the sentence into a table, with 4 in a row and 7 rows and spaces replaced with a ‘*’:

[X, l, m, w]

[*, m, w, *]

[e, *, x, i]

[w, x, *, s]

[j, *, i, r]

[g, v, c, t]

[x, m, s, r]

Now I will shift each row down by 2, any rows at the bottom go up to the top

[g, v, c, t]

[x, m, s, r]

[X, l, m, w] ← this was at the top and it has moved down 2 rows

[*, m, w, *]

[e, *, x, i]

[w, x, *, s]

[j, *, i, r]

Now I will shift each letter in each column across by 1. If it reaches the end of the column, it will go to the first slot.

[t, g, v, c]

[r, x, m, s]

[w, X, l, m] ← the ‘X’ was at the start and is now the second character in the column. The ‘w’ which was at the end has gone to the start

[*, *, m, w]

[i, e, *, x]

[s, w, x, *]

[r, j, *, i]

Done! Now let’s take it out the table and message now says "tgvcrxmswXlm mwie xswx rj i"

[t, g, v, c]

[r, x, m, s]

[w, X, l, m]

[*, *, m, w]

[i, e, *, x]

[s, w, x, *]

[r, j, *, i]

Task 6

There are many ways companies can protect their data when disaster strikes to ensure they can keep operating with as little downtime as possible. In this report I will go over the different options companies have available to them if there is a disaster, and what they can do to prevent one from happening in the first place

Disaster Prevention & How it Will Help in a Disaster

Backup Systems

Backups is one best way to keep your data safe in a disaster as they are a direct copy of the data that could be at risk of being lost. Backups should be taken every 8 hours (around 2 a day) to a separate, local server for the fastest restore. The backups should also be sent off-site to another server. This ensures that if there is a physical disaster (e.g., fire or natural disaster), the off-site copy of the data is completely safe.

Backups are needed in-case of events such as a hardware failure, accidental file deletion, security breach (e.g., the system gets hacked, and files are deleted) and many more. Once backups are done, make sure you check to ensure they have been done.

In the event of a disaster, the backup can be copied onto the primary machine to restore data with the most recent back up (which should be no more than 8 hours ago!).

Built-in Redundancy

On critical servers, you should make sure they are connected to back-up power in case of a site-wide power failure and should have at least 2 PSUs build-in to each server if one fails.

In the event of a disaster and power is lost, the UPS will be able to provide power to the servers while the disaster is resolved. In the event of a PSU failure, the secondary the PSU will keep the server online until a replacement is put in.

Mirrored Office

In the event of an outage where work cannot continue, the company could have a secondary office setup in-case of a disaster where employees can move to to continue working. This is also where off site backups can be stored so all employees have their data when moving.

Staff Training

All staff that have access to critical servers and files should be properly trained to take care whilst accessing them and should check all their actions before they perform them (e.g., check with another staff member who can verify their actions won't have any negative consequences or conflicts with existing data).

Regular Maintenance

Critical servers should be regularly maintained and checked to help minimize the risk of any disasters. For example, regular tests should be done on servers to ensure they are operating as expected and aren't using degraded / faulty hardware.

The Tiers of Recovery

In the event of a disaster, there are 7 tiers which shows how ready a company is if a disaster occurred.

Tier 0

This tier is for organisations that don't have a recovery plan or any forms of backup. Data recovery at this tier is mostly likely impossible.

Tier 1

This tier is for organisations that have scheduled backups of their data on an off-site facility. However, these organisations don't have any computer systems to download the information to during a disaster. It's possible the data backed up may be several days old.

Tier 2

This tier is for organisations that regularly back-up data which is sent off-site and to a 'hot site'. This means during a disaster; the organisation can access computer systems on the 'hot site' and continue working. However, the data backed up may be several days old.

Tier 3

This tier is for organisations that implement 'electric vaulting'. This means doing everything in tier 2 along with sending updates to critical servers / files are automatically backed up off-site once received. This means data is more up to date than the previous tiers.

Tier 4

This tier is for organisations that need their data backed up more regularly than identified in the previous tiers. This means, while a few hours of data may be lost in a disaster, most of it will be safe.

Tier 5

This tier is for organisations that need their data backed up instantly when its updated. This means very little data is lost during the disaster.

Tier 6

This tier is for organisations that need practically all their data and systems to be completely up to date in the case of a disaster.

Tier 7

This tier is very similar to tier 6, however the process of backing up data and restoring it to a separate network is fully automated in the event of a disaster. This means data and systems can be restored extremely fast.

Conclusion of Tiers

All companies should consider how critical data is and how quickly they need to be running again after a disaster strikes. They should then choose a tier readiness based off that. For example, a large company such as Google should be at tier 7, whilst a smaller business such as an independent newspaper should be around Tier 4-5 level.

For most businesses, I would recommend a Tier 6 as they would lose a minimal amount of data in the event of a disaster and would have fallbacks in place to get up-and-running immediately if a disaster occurred.

Disaster Recovery Plans

Using a combination of the Tiers of Recovery and some of what is mentioned in Disaster Prevention, a disaster recovery plan should be created by the businesses to ensure they are prepared if a disaster strikes. This should include identifying the issue, how service should be recovered (e.g., backup servers are booted and have data copied onto them or hire a new server if backups are damaged) and what should be done in the event of an unrecoverable event (e.g., it will take too long to get a backup server). In these cases, mirrored offices would be considered. These plans should include timeframes and should have information that would consider as many scenarios as possible. When considering differentscenarios, businesses should consider their office location – is it prone to natural disasters? They should also look at other types of disaster such as hackings, power loss, etc.