Common Security Breaches

Data Security

Has your data been compromised?

- Have I Been Pwned? (HIBP) is a website that allows internet users to check if their personal data has been compromised by data breaches.
- The service collects and analyses dozens of database dumps and pastes containing information about hundreds of millions of leaked accounts and allows users to search for their own information by entering their username or e-mail address.
- Go to the site and see if any of your accounts have been breached.
- URL: https://haveibeenpwned.com/

Common causes of data security breaches

- Data packets travel to and from numbered network ports associated with IP addresses and endpoints, using the TCP layer protocols.
- All ports are potentially at risk of attack. If a port is not configured properly, a hacker can gain access to a server that can contain valuable data.
- Any device and the associated user on that network is then at risk.
- There is 65,535 TCP ports; some of the more common ones are on the next page.

Common TCP ports

Port Number	Port Use
21	Connects FTP (File Transfer Protocol) servers to the internet
110	POP3 (Post Office Protocol version 3) - used for retrieving E-mails
80	HTTP traffic. Unencrypted web traffic
25	SMTP (Simple Mail Transport Protocol) - used for e-mail routing between mail servers
More…	Full List of TCP ports can be located here: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Reasons

A data security breach can happen for many reasons:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- ‘Blagging’ offences where information is obtained by deceiving the organisation that holds it.

Watch

- Watch this clip on the leading cause of cyber-attacks in business … CLICK HERE

- URL: https://www.youtube.com/watch?v=M7q6EH7u89k

Motives, tools and techniques

- The motive of cybercriminals directly influences which companies they target, and what data they want. Some hackers may want to get access to data for financial gain or fraud purposes. Others may want to gain access to data for revenge. Terrorists may want data that relates to critical infrastructure of a country, while hacktivists may want data that could embarrass officials in the Government, or people in authority. Different data will have different value depending on the type of data and what can be done with it. Although the site relates to American data breaches, it is still an insight into what happens to all that data and what we can do to protect ourselves.
- Where does all the stolen data go?
- URL: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/follow-the-data
- The tools and techniques at hackers' disposal to gain access to data is extensive. Causing a data breach or gaining access to unauthorised information is not as difficult as it appears to be.

Passwords

Weak and stolen passwords:

- Weak passwords are often a source of a data breach.
- An opportunist hacker may guess a password to a system, or the user has left clues about their password in a security question that leads the hacker to the password.
- Sometimes a password is a simple word from the dictionary that a hacker can do a dictionary attack or a brute force attack and gain access to an account.

Watch and Look

- Simple solution: Use a password manager or use complex passwords, and never share passwords, as this video shows
- URL: https://www.youtube.com/watch?v=UzvPP6_LRHc

- Have a look and see if your password is on this most common password list
- URL: https://www.passwordrandom.com/most-popular-passwords

Back door vulnerabilities

Back door and application vulnerabilities:

If a door is already open, there is no need to break it down.

Hackers love to exploit software that has been poorly written, or networks that are poorly designed and implemented.

Software that has not been updated may contain vulnerabilities that allow a hacker to exploit, thus giving them access to databases.

Simple solution:

Keep software and hardware up to date and fully patched.

Out of date software and data breaches – click here for more info

URL: https://digitalguardian.com/blog/behind-breaches-lots-outdated-software

Malware

Malware:

Malware is an umbrella term for viruses, Trojans and worms.

Malware is malicious software that can cause damage to a system and is loaded onto the system without intention; it can give a hacker access to the data.

If the system that contains the malware is connected to other networks, then that malware can spread allowing a hacker access to other areas of a network.

Difference between types of malware – click here for more …

Simple solution:

Be aware that accessing websites that promote free movies and software may contain malware.

Use anti malware protection and scan the system regularly. Do not open up e-mail attachments that look suspicious.

URL used:
https://www.wired.co.uk/article/ransomware-viruses-trojans-worms

Malicious Insider

Malicious insider:

A rogue employee, a disgruntled contractor, someone who may have even been placed in an organisation with the intent on causing a data breach, or even someone in the organisation who just does not know any better.

What stops people who already have access to a system from copying, altering or stealing data?

Simple solution:

Know whom you are dealing with and act fast if there is any hint of a problem.

Have good procedures in place and make sure all staff are trained

Security intelligence insider threats – click here for more info

URL used:

https://securityintelligence.com/news/insider-threats-account-for-nearly-75-percent-of-security-breach-incidents/

Unintended Disclosure

Unintended disclosure:

Human error can sometimes lead to a data breach.

Something as simple as sending an e-mail to the wrong person can be very serious if that e-mail contained sensitive data.

Posting too much information online can also lead to a data breach, if a hacker is able to use that information to gain access.

Examples of unintended disclosure on the next page …

Unintended Disclosure

- **Cloud access:** Data often is stored online in the Cloud. Services like Dropbox, iCloud, and OneDrive, if misconfigured, can allow public access to it, instead of access to only authorised people.
- **Phishing attacks:** This is an attempt to obtain sensitive information such as usernames, passwords and credit card details. An e-mail that looks like it is from a legitimate source such as Amazon or a bank will ask you to reset your username and password by getting you to log on to a fake website. The website may look just like the real site but will have subtle differences.
- **Keylogging:** This is the use of hardware or software to capture all the key strokes on a keyboard. A copy of all the keystrokes can be sent via e-mail to the hacker who set up the keylogger, and they would have access to all the credentials typed on that keyboard that day.
- **RAM scraping:** This is where malware is installed at a point-of-sale terminal and allows the details of debit and credit cards to be illegally collected. Target was hit by this type of attack in 2014
- **Physical loss of equipment:** Losing a USB flash drive, mobile phone, portable hard drive or laptop has been the cause of data breaches in the past. These devices, if not encrypted, can be easily accessed by someone not authorised, and all the data they contain can be stolen.

Information is Beautiful

The Information is Beautiful website has a very good visual resource on the world's biggest data breaches.

URL used: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Target attack in 2014 – click here for more information.

URL used: https://www.securityweek.com/target-confirms-point-sale-malware-was-used-attack

Task

- Now do Task 14