Why Systems are Attacked

Any system holds some form of value (financial value, functional value, and in some cases, personal value). This is because organisations use digital systems every day to carry out tasks, store data, and manage operations vital to the company. This value provides a key reason for malicious users to attack a business's systems.

To better understand why systems are the target of attacks, and the impact that these attacks have on the organisation as a whole, we must learn some of the most.

1. Reasons Why Systems are Attacked

There are many reasons why systems are attacked, and they are not always for financial gain. Sometimes attacks are purely for making mischief or due to a personal vendetta.

When we look at the reason why a system has been attacked, the most common factors are included below.

- **Fun/challenge** – Some attackers gain unauthorised access to systems for the purpose of amusement or challenge. Attacking a system for this purpose can allow individuals to gain experience for future cyber-attacks, overcome personal goals of 'beating' an organisation's cybersecurity measures, or in some cases, allow them to gain kudos from their peers or a community.
- **Industrial espionage** – Cyber-attacks may be perpetrated on specific targets for stealing unique sensitive information from a rival business (quite often intellectual property). This data can then be used to aid those carrying out the attack to be one step ahead of the rival, such as releasing a proprietary product before the original organisation can.
- **Financial gain** – More often than not, an attack will be motivated by money as the end goal, even if it is not immediately obvious. This could be through:
    - *Direct gain*, where the attacker directly steals money/information during the attack which will lead to profit.
    - *Indirect gain,* for example, extortion, where attackers may use ransomware, or denial of service attacks in order to threaten an organisation into paying them to end the attack.
- **Personal attack** – On occasion, the motivation for attacks can be personal, for example, an individual may be targeted based on their beliefs/opinions, or organisations may receive attacks from employees who feel they have been mistreated.

- **Disruption** – Attacks may occur with the primary purpose of disrupting an organisation's service. This may be to benefit financially, or in business, but is often for personal, political, or social reasons. Common forms of attacks that cause disruption include denial of service attacks and website defacement.
- **Data/information theft** – Attacks may occur for the purpose of stealing data. More often than not, this is customer, personal or financial data stored by the company. Stolen data can then be used by the attackers for identity and bank fraud purposes, such as purchasing items using the customer's credit card details.

Further Thought

Cyber-attacks quite commonly appear in the news. Find some news articles online about a cyber-attack and see if you can discover the reason for the attack.

2. The Impact of a Security Breach

Most attacks are perpetrated with a specific impact on the business in mind. It is important to understand the impact that a security breach can have, so we are aware of how best to reduce the effect of the breach.

- **Data loss** – This could either be due to data theft, or data which has been deleted/corrupted as a result of a malicious payload (e.g. virus).
- **Damage to public image** – Attacks may cause customers to view an organisation more negatively, and indirectly cause loss of customers, public panic, or create a political statement.
- **Financial loss** – Business may lose money such as from the theft of banking details, a loss in profit after the attack as a result of damage to the public image, data loss, and industrial espionage to name a few examples.
- **Reduction in productivity** – Attacks such as data theft (so employees cannot access the data they need to carry out their job), and denial of service attacks, prevent a business from performing their daily operations.
- **Downtime** – An attack may cause the system to fail, and go down completely, often as a result of a malicious payload being so disruptive that the service must be shut down manually, or due to an attack which takes the servers offline directly.
- **Legal action** – Organisations are legally obliged to ensure that individuals' data is secure and not misused. If data is harmed during an attack, then the organisation may be liable to huge fines under the Data Protection Act (2018).

Further Thought

Did you know you can visit https://haveibeenpwned.com/ to find out if your email address has been compromised in a data breach?