**Information Security and Threat Management**

Computer systems can be large and complex webs of interconnected subsystems. Each of these subsystems is made up of many smaller components, and each of these components is made up of increasingly smaller modules until we reach the levels of 1s and 0s in a network of transistors.

Consequently there are thousands of methods available to break into computer systems, since there are thousands (if not more) of different components involved in even simple configurations. In this session we will cover the general classes of attack and mitigation, find out more about how attacks are carried out and discover how IT security professionals use methods to detect and prevent these attacks.

Glossary

First we need to define some terms:

* **Attack surface –** All aspects of a particular IT system that are subject to **threats**
* **Threat –** a specific technique or method of mounting an **attack**
* **Attack –** An undesirable event initiated by a **malicious actor** with the intent to breach the **confidentiality** of the system, disrupt the **integrity** of a system or affect the **availability** of a system.
* **Malicious actor** – a person or organisation that carries out, or attempts to carry out, an **attack**
* **Confidentiality –** The ability to keep secret information about an organisation’s IT assets, or the data contained within their IT assets
* **Integrity** – The ability to have trust in the accuracy, validity and reliability of an organisation’s IT assets
* **Availability –** The ability for IT systems to be available for use
* **Risk** – Normally defined as a function of **likelihood** and **impact** with respect to the probability of an attack and the damage such an attack could cause.
* **Likelihood** – The probability that an attack could occur
* **Impact –** A measure of disruption to the organisation should an attack occur. This can be measured in financial terms, or as a measure of time, or other ways such as whether the organisation can continue.
* **Vulnerability –** Something about the IT system that enables an **attack.** Not the same as a threat – a threat is something that could happen, a more general class of attack. A vulnerability is the thing that enables a threat, or allows an attack to happen.

Exercise

Read the following information.

*“Heavy Metal Industries Ltd. is a company based in Sheffield that employs 20 people across two sites. Their business is the supply of rare metals and elements to the manufacturing sector, to produce the components for items such as computers and mobile phones.*

*The company uses e-mail and Internet-connected telephone lines to communicate between sites. Their IT equipment, including e-mail server, is all located on one site in a locked communications cabinet. Bob, the site manager, has the only key. The company has a server running their stock and inventory tracking system which is accessible by staff offsite via an Internet portal.*

*The company also has a website,* [*http://heavymetal.info*](http://heavymetal.info)*. Using this website, customers can log in, upload their design specifications and communicate with the company about their orders. There is an order tracker available and customers are able to change their details online.*

1. Estimate the likelihood and impact of the threats on a scale of 1-5 (1 is low). Talk through your reasoning – what **vulnerabilities** are present?

For each threat, multiply your two figures together. To obtain a risk score in the range 0-10 we can normalise the result. This is easiest done by multiplying your result by (1/25), or 0.04.

|  |  |  |  |
| --- | --- | --- | --- |
| **Threat** | **Likelihood (L)** | **Impact (I)** | **Risk Score (L x I x 0.04)** |
| Unauthorised access to comms cabinet |  |  |  |
| Interception of website traffic |  |  |  |
| Impersonation of customers |  |  |  |
| Unauthorised access to email system |  |  |  |
| Theft of data about stock levels and movements |  |  |  |

2) Can you think of any other threats? How would you categorise their risk?

3) If you were assessing security for this company, what other questions would you want to ask?

**Types of Threat**

Some common classes of threat:

* **Malware** – This is software created specifically to enact a threat. Things that malware can do – theft of data, enable blackmail, disrupt a computer system or spread false information.  
    
  Watch this short video about Stuxnet - <https://www.youtube.com/watch?v=7g0pi4J8auQ>
* **Phishing** – This is an attack normally carried out by email. In this attack, a malicious actor tries to persuade, trick or coerce a victim into parting with money for a non-existent service, or under false pretences. For example, an email might try to persuade a victim that in exchange for a small money transfer fee, they can take receipt of a larger amount of cash that needs exfiltration from a hostile country. These are always scams and many hundreds of people fall victim every year.
* **Social Engineering** – In this type of attack, the person is the target, and is the vulnerability in the system. Social engineering can quite often not involve technology at all – for example, persuading a receptionist to allow access to a secure area, using disguises or false documentation; or using the telephone to persuade someone to hand over sensitive information.

Watch this video showing a live attack by Kevin Mitnick, a noted social engineer: <https://www.youtube.com/watch?v=DB6ywr9fngU>

* **Brute Force Attacks** – These are automated attacks that can try many thousands or millions of password attempts to try and break into an account. Within this type is a **dictionary** attack, where permutations of dictionary words are tried at high speed until a match is found, and attacks using **rainbow tables**, a slightly more advanced technique that compares password **hashes** to obtain commonly-used passwords.