# Cyber Security Lesson 1 23/08/21

## Introduction

Cyber Security: The ability to protect or defend the use of Cyber-attacks,

* The prevention of damage, protection and restoration of communication and electrical services.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Availability** | **Integrity** | **Authentication** | **Confidentiality** | **Non-Repudiation** |
| Authorized users that can freely access the system, network and data needed to perform their daily task | To Ensure that a system, software, data has not been modified by unauthorized users or unauthorized means | Assurance and confirmation of a user’s identify | Ensures that sensitive information are accessed only by authorised person and kept away from unauthorized users | Ensures the inability to refute responsibility |

## Cyber Security Cube

* A model framework for establishing information security

|  |  |  |
| --- | --- | --- |
| **Desired Goals** | **Data States** | **Safeguards** |
| Confidentiality | Transmission | Human Factor |
| Integrity | Storage | Policy & Practice |
| Availability | Processing | Technology |

**Asset** – An Asset is what we are trying to protect (Data, Hardware, Software etc.)

**Vulnerability**: A weakness in our protection efforts

**Exploit**: How hackers take advantage of vulnerability’s

**Threat**: Potential negative action that results in a unwanted impact to a computer system or network.

**Risk**: Probability of exposure, loss of data or assets as a result of a cyber-attack

## Causes of Vulnerabilities

* Design & Development Errors
* Poor System configuration
* Human Error (Human Factors)
* Connectivity (using unsecure networks)
* Complexity (Adding too many layers of security = harder to maintain)
* Passwords
* User input (User input validation)
* Management
* Lack of Training Staff
* Communication

|  |  |
| --- | --- |
| **Cyber Threat Actors** | **Motivation** |
| Nation-states | Geopolitical |
| Cyber Criminals | Profit |
| Hacktivist | Ideological |
| Terrorist Groups | Ideological Violence |
| Thrill-Seeker/ Script kiddie | Satisfaction. |
| Insider Threat | Motivated by discounted. |

## Cyber Threat

|  |  |
| --- | --- |
| **Malware** | Software that does malicious tasks on a device or network. |
| **Spyware** | Is a form of malware that hides on a deceive providing real-time information. |
| **Phishing Attacks** | Is when a cyber-criminal attempts to lure individual into providing sensitive data. |
| **Ransomware** | Denies Access to a computer system or data until paid. |
| **Advanced Persistence Threat** | Unauthorised users have access and remains undetected inside the network. |
| **Trojan** | Misleads user of its true intent. |
| **Backdoor** | A way for unauthorised users to gain access to a system or network. |
| **Rogue Software** | Type of malware that misleads users into believing there is a virus on their system and aim to convince them to pay for a fake malware removal tool |
| **Data Destruction** | Is when a cyber-attacker attempts to delete data |
| **Drive-by-down Intellectual Property load** | Installing malware through a website visit |
| **Intellectual Property Theft** | Stealing the Intellectual Property of a organisation |
| **Unpatched Software** | Software that has weak security |
| **Zero-day attack** | Unknown vulnerabilities in a system |
| **Natural Disasters** | Earthquakes, Floods, Tsunami, Hurricanes |

### Cyber Threat Surface

* All the available endpoints that a threat actor may attempt to exploit a computer systems or data (Looking through windows, over the shoulder)
* Process that produces, deliver and reply on information systems connected to the internet are also a potential threat vector
* Services, Devices & Data can all be targeted
* System that connect physical entities with the internet

### Cyber Kill Chain

#### Steps to attacking the Target

Reconnaissance – Delivery – Weaponisation – Exploitation = Installation – Command & Control – Actions on Objectives

# Cyber Security Lesson 2 24/08/21

## Virtualisation

* Process of separating software form Hardware
* Hypervisor works as a interfaces between VM’s & the host
* Virtual Server exists digitally not physically
* When using multiple VM’s they are usually separate and can’t communicate with each other
* Host OS & Virtual OS can be different Operating systems

### Traditional Architecture

Application Operating System Physical Node

### Virtual Architecture

OS OS OS Virtual Layer Physical Node

#### Virtualisation Type

|  |  |
| --- | --- |
| Type 1 Hypervisor | Type 2 Hypervisor |
| * Hypervisor running straight from the hardware/Bare-metal | * Hypervisor running form and existing host operating system |

### Vulnerability with Type 1 and Type 2

|  |  |
| --- | --- |
| **Type 1** | * Better Security (Less Layers) * Performance (Due to no OS) |
| **Type 2** | * Better simplicity (Easy to set up) |

## Linux Architecture

**Inner Layer – *Hardware*** = Physical electrical device,

**Outer Layer 1 - *Kernel*** = The centre of a computer operating system, it’s the core that provides basic services

**Outer Layer 2 – *Shell*** – The interface between the user and the kernel, allowing the user to execute programs and commands

**Outer Layer 3 *– Application & Utilities*** = Software that performs specific tasks for the end user

## Linux Distributions

|  |  |  |
| --- | --- | --- |
|  | Linux |  |
| Debian | **Arch Linux** | **Fedora** |
| Ubuntu & Kali |  | **Red Hat & Centos** |

* Each distribution focuses on a different purpose, for example Ubuntu is commonly for general use, while Kali is designed for networking or cyber-security users.

## Linux File system

* A file system is the system that control how to store & retrieve data
* **Microsoft** == FAT, FAT32 & NTFS while **Linux** == EXT$, EXT£, BTRFS, XFS
* Windows FS uses letters for partitions, while Linus works on concepts that everything starts at the root, (A Tree Concept)