Assignment 4

Deadline: Day 12/12/2017 @ 23:59

**Total Mark for this Assignment is [10]**

***IT Security & Policies***

***IT-409***

Student Details:

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **Name:** Mohammad Hazazi  **CRN:** |  | **ID:** 120003904 |
|  |  |  |

**Instructions:**

* This Assignment must be submitted on Blackboard via the allocated folder.
* Email submission will not be accepted.
* You are advised to make your work clear and well-presented, marks may be reduced for poor presentation.
* You MUST show all your work.
* Late submission will result in ZERO marks being awarded.
* The work should be your own, copying from students or other resources will result in ZERO marks.
* Use **Times New Roman** font for all your answers.

# Question One

***02 Marks***

1. A) What are the three categories of factors required in the process of authentication, give examples for each category?

B) In a Mandatory Access Controls environment, what type of clearance and tag is required to access a document classified as “Secret” and categorized as “Flight Plans”?

|  |  |  |
| --- | --- | --- |
| Factor | Brief | Example |
| **Knowledge** | Something you know  Most common factor to use and the easiest to beat. Considered single-factor authentication. | Password / PIN |
| **Possession** | Something you have  Prove your identity by something you own it and use it during authentication. Considered multi-factor authentication | Smart card / Token |
| **Inherence** | Something you are  Use Biometric methods, which you are the only person who has it. This factor offers strongest authentication but its susceptible to errors depend on its sensitivity. | Fingerprints / iris scans |

A)

B)

The person who would like to access the document classified as “Secret” and categorized as “Flight Plans

**MUST** have equal or higher clearness as well as being tagged to the same category.

User security clearance = {Secret or Top Secret} AND tagged to “Flight Plans” category.

# Question Two

***03 Marks***

1. A) What is remote access security? Write two policy statements supporting remote access security?

B) List the two most common remote access technologies. Define each one briefly.

C) Is monitoring legal in the USA’s Judiciary System? If not, why? And if so, for what reasons is it legal?

A) Remote access security mean how we can grant a secure access to the user to have him connected to our internal organization network from outside (external network).

We can control the remote access security through several things as below:

* Apply mutual Authentication
* Insure the security of remote access communication and user stored data can’t be compromised.
* Detect any data modification during transition to insure the integrity.
* Availability of the access whenever user need it.
* Apply physical security to user Clint devices.

Policy statements example:

1) Only company approved remote connections are allowed to provide remote connectivity to the corporate network.

2) Authentication for remote access must be strong and utilize two-factor authentication.

B)

|  |  |
| --- | --- |
| VPN | Is a virtual privet network that securely connects users and ensures that only authorized users can access the network and the data can’t be intercepted. |
| **Remote Access Portal** | A protected environment with the necessary security controls. Designed to give remote users limited access to specific applications or information. |

C) YES its allowed for reasons and purpose.

Reason for that vary:

1- The activity which you would like to monitor is within your property.

2- You should own the equipment

3- You have a reasonable purpose to monitor other activity, ex. ensures the quality of work, or place security

4- protect your property from robbery and fraud

# Question Three

1. A) Discuss about Commercially Available Software and Open Source Software with examples.

|  |  |
| --- | --- |
| Commercial Software | Open Source Software |
| 1- Created, developed and supported by profitable company, who sell license to use their software. Ex. Microsoft. | 1- Created , developed by group of developers who made the modification to improve the software so it is always used by users everywhere , and they update it based on the user needs. |
| 2- The source code is closed and only profitable company who can edit it | 2- The source code is open for everyone to modify and enhance. |
| 3- More secure, usual development and fix | 3- less secure, developer from around the world , really they gathered together, therefore less development and fix |
| 4- software cost is Expensive | 4- software cost is Free or small donation to support the developer community |
| 5- great service and support in case of any problem. | 5- week service and support and some delay. |

B) List and Explain different levels of software releases.

|  |  |
| --- | --- |
| Software Release | Open Source Software |
| **Alpha** | The first release of software which is used to test the software functionality. In commercial software, this version is available internally for the developer only. However, in open source software, it's being released for the external as well. |
| **Beta** | This version has passed the alpha testing, and it is released to the user for usability testing. So any reported error will be fixed by the developer. Beta software version can be unstable and might let to crashes or data loss. |
| **Release Candidate** | It is a software version with the potential to be the final software product to be released to the public unless fatal bugs have been found. |
| **Production Release**  **(**General availability/go live**)** | This version has passed all testing, and its already available commercially for all the user to get and use it. |

# Question Four

***03 Marks***

1. A) Define information security incident.

Its a series or single of unanticipated or unwanted information security events that have high probability of compromising business operation and threatening information security

B) Complete the following table:

|  |  |  |  |
| --- | --- | --- | --- |
| Incident | Required Internal Notification | Severity Level | Required Response time |
| User access to content or sites restricted by policy | Chief Information Security Officer. Designated incident handler. | **3** | 24 Hrs |
| Denial of service attack | Chief Executive Officer.  Chief Operating Officer.  Legal counsel.  Chief Information Security Officer. Designated incident handler. | **1** | Immediate |
| Malware detected on multiple systems | Chief Operating Officer.  Legal counsel.  Chief Information Security Officer. Designated incident handler. | **2** | 4 Hrs |

C) Describe the process for performing digital forensics with your own words.

The below reflect my personal experience from the 2012 cyber-attack.

Most of the people thought that when we discovered that our enterprise has been breached or became a victim of cybercrime, we solve the immediate problem. For cybercrime investigator, that is the tip of the iceberg.

We usually go through a process of identifying, preserving, analyzing and presenting digital evidence about the crime. To support our task, we use special tools to capture, analyze and keep the evidence during our investigation activity.

We make sure to analyze storage media, hardware and OS, networks, and application. Depend on the criticality of the infected application, system or network the level of the investigation will be determined.

**The investigation process usually divided into three phases :**

**Phase 1 - Data collection**

- we obtain search authority and involve Ministry of interior. (MOI)

- document the chain of custody

- hash and duplicate all evidence

**Phase 2- Examination and analysis**

- validate our tools.

- performed analysis on the gathered data

- reproduce the methods and outcomes for assurance

**Phase 3- Reporting**

- the conclusion is made

- expert testify is presented to MOI

Usually, in a significant investigation, teams from MOI, External forensic company, and Company team is performed to assist in such investigation. This will help in avoiding any mishandling or destroying to the preserved evidence by unskilled staff