**COURSE CODE: COE 510**

**COURSE TITLE: COMPUTER SECURITY TECHNIQUES**

**NAME: IBINAIYE OLUWASEUN JOHN**

**DEPARTMENT: COMPUTER ENGINEERING**

**MATRIC NUMBER: 15/ENG02/028**

**NUMBER ONE:**

**Security policy on the use of mobile devices**

1. Always ensure the operating system is up to date.
2. Do not use mobile devices to record confidential information.
3. Avoid the use of personal phones for work tasks.
4. Do not connect to public Wi-Fi networks.
5. Ensure to use VPN for secure end to end connection.
6. Encrypt your mobile device.
7. Regularly backup your mobile device.
8. All mobile devices must be protected by a strong password and must not be disclosed to anyone.
9. If you lose your mobile device or it is stolen, it should be reported immediately.
10. Do not download applications from untrusted sources always verify first before making any download.
11. Block potentially dangerous applications.
12. Enable the Remote lock and data wipe option on the mobile device just in case the device gets lost.
13. Encryption mechanisms must be verified before sending sensitive information over a wireless network.
14. Follow up safe disposal practices when you dispose your mobile device and ensure all sensitive information are erased/removed completely.

**NUMBER TWO:**

**INTRODUCTION**

Espionage is the act of obtaining secret or confidential information without the permission of the holder of the information. This practice is clandestine and it involves stealing of sensitive information, espionage attacks on corporation is known as industrial espionage and one of the most effective ways to gather data information about a targeted organization is by infiltrating its ranks. This is carried out by an espionage agent.

**METHODS ON HOW TO CARRY OUT INDUSTRIAL ESPIONAGE (ESPIONAGE ATTACK ON CORPORATIONS)**

As discussed earlier, the most effective method of carrying espionage attack is by infiltrating the ranks of the corporation, one of so many methods to carry out this attack on the corporation/company is the use the social engineering.

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It is the use of psychological manipulation to trick people into making security mistakes or giving out sensitive information. The first step taken is to investigate the intended target and gather every necessary background information, such as position in the company, hobbies, passions amongst others needed to proceed with the attack. The target would be someone with a high level clearance in the company (someone who has access to confidential information about the company), after using social skills to gain the targets trust and the target and espionage agent are now friends. After, let’s say weeks of familiarization, the target gets comfortable with the agent and even begins to invite the agent to his/her house, now the agent has the advantage because most people do carry their work laptops/computers to their homes to get work done, the agent then uses his or her skills to gain access to that computer secretly and plant a malware on that computer system, the malware can be undetectable. Now the agent has achieved part of his and can now access highly sensitive information remotely (indirectly), can even direct data traffic to another workstation, monitor the activities of the target when he/she uses the computer system, etc. the agent will also ensure to install a backdoor via the company’s security system, so that incase the company upgrades their security system, the agent still has a way to get in and steal more information and give to who employs him/her.

Another method to carry out espionage attacks is the use of rootkits; rootkits are malware that infect computer systems on a deeper level so they can be undetectable. Computers are structured in layers. A program can only modify other software from the same layer or above but not from a deeper one since it does not have access. The deepest layer is the BIOS, which controls the computer system boot-up procedure and other software aspects. Rootkits are used by agents to target this access layer since antivirus programs find it difficult finding and removing the rootkit. In fact, the time taking by the antivirus to find and remove the rootkit is enough time for the agent to gather all the necessary information he/she needs. The agent uses the rootkit to enslave computers into botnets to listen to user’s internet traffic.

Another method used by attackers to carry out industrial espionage and gain access to information is the remote access Trojan (R.A.T). this is a Trojan malware that gives an attacker administrative control over the infected computer, once the RAT has been successfully installed, the agent can control the computer remotely, allowing him/her to install key loggers, form grabbing malware, activate the webcam, format drives, create a botnet and steal sensitive company data, business formulas and so on.

Another method is the use of spyware; spyware is a type of malware used by attackers to quietly collect valuable information about his/her target in the background. Online attackers use spyware to find out deeply personal information such as passwords, credit card data, personal photos. Key loggers and so on. Advertisers on the other hand, look for information related to your internet usage habits, such as location and search history, hobbies, interests in order to better target you with ads. Spyware from advertisers usually comes in free software such as browser toolbars, music programs, that come either stand-alone or bundled with another program.

Another method is the use of DOS/DDOS (denial of service/distributed dos) attacks, these sort of cyber-attacks seek to disrupt the Internet use of a user or service, by flooding its connection with useless information such as enormous amount of login attempts or excessive amount of traffic. Unlike a DoS attack, a DDoS relies on a large number of devices that can simultaneously assault the target, hence the name “Distributed” since the attacker’s resources are spread across many computers or other devices. Most cases involving DDoS attacks involve a botnet that has a sufficient amount of enslaved devices capable of launching a concerted attack.

In conclusion one of the most important precaution taken by the espionage agent is to erase his/her footprints or tracks which can lead the investigators tracing back to him. Erasing footprints can be done by the use of Virtual Private Networks (VPN), clearing logs, modifying logs and registry files, removing all files and folders created, destroying the Network Interface Card (NIC) of the computer system used and this makes it impossible to track the MAC address (media access control). With all these precautions taken the industrial espionage has been carried out successfully and making it almost impossible for security agents/investigators to track the attacker(s).

**SECURITY MEASURES TAKEN TO PREVENT SUCH ATTACKS**

The security measures to be taken by the xyz company are listed below;

1. **Do not expose your internal network**

**The process of transferring files in and out of the enterprise must be carried out without exposing and risking the internal network. No type of direct or indirect communication should be allowed between the partner and the enterprise**

1. **Make sure that intermediate storage is secure**

**While information is waiting to be retrieved by the enterprise or sent to the business partner, it must reside in a secure location. This is especially critical when the intermediary storage is located on an insecure network, such as the enterprise’s DMZ, outsourced site, or even the internet.**

1. **Ensure that Data at Rest is protected**

**The cornerstone of protecting storage while at rest is encryption. Encryption ensures that the data is not readable and thus maintains its confidentiality. But encryption that places high demands on managing is ineffective. By using transparent key management there is absolutely no need for user level or administrator level encryption key management or awareness, and the use of advanced cryptographic protocols, such as AES 256bit for both storage and session encryption and signing, guarantees the protection of the data**

1. **Protection from data deletion, data loss**

**The protection of data by encryption is simply one part of the problem. Files may be accidentally or intentionally deleted or changed. Always keep older versions, ensuring an easy way to revert to the correct file content or recover from data deletion.**

1. **Protection from data tampering**

**Data inside protected storage must be tamper proof by integrating authentication and access control that ensures that only authorized users can change the data. In addition, to ensure that data manipulation that somehow bypasses the access control doesn’t go unnoticed, digital signatures must be employed to detect unauthorized changes in the files.**

1. **Auditing and monitoring**

**Comprehensive auditing and monitoring capabilities are essential for security for several reasons. First, it allows the enterprise to ensure that its policy is being carried out. Secondly, it provides the owner of the information with the ability to track the usage of its data. Thirdly, it is a major deterrent for potential abusers, knowing that tamper-proof auditing and monitoring can help in identification. Finally, it provides the security administrator with tools to examine the security infrastructure, verify its correct implementation and expose inadequate or unauthorized usage.**

1. **End-to-End network protection**

**Security must also be maintained while the data is being transported over the network. The process of transferring data must be in itself secure. Users that store or retrieve data must be authenticated, sometimes using strong authentication mechanisms. In addition Access control must ensure that users only take appropriate action, and that only authorized actions are carried out.**

1. **Process Integrity**

As data transfer is an essential part of a larger business process, it is critical to be able to validate that this step in the process was executed correctly. This requires the solution to provide auditing features, data integrity verification and guaranteed delivery options.

1. **Carry Out Risk Assessments**

Conduct cybersecurity risk assessments on a regular basis in order to mitigate the risks. There should be a separate department in your company that is dedicated to minimizing the risk of data loss. Risk Management is one of the key factors that contribute towards the growth of your company as it keeps the business safe from getting exposed to competitors who are always looking for insights. You can also hire a professional like a Cybercrime Consultant or Risk Mitigation Specialist, these are experts at protecting your company against threats and are known for producing positive results for your business.

1. **Keep an Eye on Employees**

Employees are one of the key elements of the company because they have insights of the business and are privy to the operations. Keep employees motivated and discourage them from leaking out crucial information, try to make them more loyal to the company. In addition to this, keep a backup of all the messages that are exchanged between employees. Check on how they use passwords and keep these passwords safe from unauthorized personnel. You can use a Password Manager for generating and managing the passwords of your company.

**NUMBER THREE:**

1. 3 HAMLETS ---------------- third letter is M

1 ORACLE------------------- first letter is O

9 MESSENGERS-------------- ninth letter is R

1 SHELL---------------------- first letter is S

4 RODENTS---------------------- fourth letter is E

1 CALABASH--------------------- first letter is C

3 PROPHECIES---------------------------- third letter is O

1 DESTINY--------------------------------- first letter is D

6 COWRIES---------------------------------- sixth letter is E

The result of this decryption is **MORSE CODE**

1. **SING THAT RAP FALL**

**NUMBER FOUR:**

Encrypted message TSJSFRHGTJQTNZS

1. **Ceasar substitution cipher (key 5)**

ABCDEFGHIJKLMNOPQRSTUVWXYZ

VWXYZABCDEFGHIJKLMNOPQRSTU

Decrypted ceasar cipher- ONENAMCBOELOIUN

1. **Columnar transposition cipher (key 5)**

**Using Key = abcde**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **a** | **b** | **c** | **d** | **e** |
| **1** | **2** | **3** | **4** | **5** |
| **o** | **n** | **c** | **e** | **i** |
| **n** | **a** | **b** | **l** | **u** |
| **e** | **m** | **o** | **o** | **n** |

Plain text = ONCE IN A BLUE MOON