AGOYI ISAAC OTUOZE

15/ENG02/002

COE 510 ASSIGNMENT 2

**QUESTION ONE**

Develop a security policy for an XYZ company on the use of mobile devices in that company

1. Mobile devices must have strong authentication, use password controls: every mobile device in the xyz company should have built in biometrics such as fingerprint scanners, facial recognition, voiceprint recognition etc. This is to make the authentication of the company’s staff more secured
2. The use of third party software or applications on mobile devices should be limited or blocked: the XYZ company should establish policies to limit or block the use of third-party software. This is the best way to prevent possible compromise and security breaches resulting from spyware applications. By your own device management (BYOD) should also be encouraged.
3. Regular mobile security audits and penetration testing should be performed on mobile devices: the mobile devices in the XYZ company should be tested regularly for loopholes whereby if any is found, and upgrade should be made. This is to make the software more secured.
4. Special firewalls and separate gateways should be created when directing mobile traffic: the traffic that passes through the mobile devices should be monitored closely, whereby firewalls and access points measures are applied to make it more secured
5. Mobile devices must have antimalware software installed on them: Software updates to mobile devices often include patches for various security holes that can be an open door for mobile malware and other security threats. Therefore, it is a security best practice to install the updates as soon as they become available.
6. The company’s mobile devices should be securely kept to avoid being misplaced: the mobile device should be kept out of the reach of those who aren’t staff in other to prevent damage and misplace of the devices.
7. Backup Device Content on a Regular Basis: Just as you backup your computer data regularly, so should you backup data on your company’s mobile devices. If a device is lost or stolen, you’ll have peace of mind knowing your valuable data is safe and that it can be restored
8. Mobile communications should be secured: in other to ensure that the communication from one mobile phone to the other is secured and safe, we ensure that the wireless communication means are encrypted, in other to prevent them from being easily intercepted. We also ensure that mobile communication is being configured with VPN services to allow for logging and management.
9. Unsecured wireless network and Bluetooth should be avoided from discovery: this should be done in other to avoid any form of snooping from unauthorized network into company XYZ mobile phone network

**QUESTION TWO**

To carry out this attack on the XYZ company, we use a malicious software which can involve virus, worms, trojan horse, etc.

**How to carry out the attack without being noticed**

I first introduce a trojan horse program. A Trojan Horse neither replicates nor copies itself but causes damage or compromises the security of the computer.

The aim of the program is to compromise the security of the company and thereby also capture the logins and password to make spying of the company’s online resources easier. Another major reason why I start with this particular malware is because it uses social engineering so it comes in the form of a useful document.

A Trojan horse software would also be beneficial because it can pop up as a window that is unharmful thereby making it unsuspicious.

Then I also introduce a spyware since the aim is to spy on the XYZ company because it collects information from every user without their consent and it is very difficult to detect the presence of the spyware.

The above malicious software’s (Trojan horse and spyware) which I would like to us to spy on the XYZ company can be spread in different ways, but the method I would consider is the use of spam message. A spam message is usually sent in the form of an email which wasn’t requested.

I would also consider another method know as zombie programs, whereby a corrupted computer in the XYZ company is taken control of and thereby attacks other computers connected to it over the network. This method is commonly used for large scale organizations.

Another method I will consider in spying on the XYZ company is phishing, this is done by tricking the company to provide personal details such as social security number, bank account number etc.

**THE SECURITY MEASURES TO BE TAKEN.**

In other to prevent hackers from carrying out the following harmful activities mentioned above, the following should be done

1. Install quality antivirus: all windows users in the company should install professional, business-grade antivirus software on their PCs. This is needed to protect against a wider range of threats (such as worms) and enable additional protective features (such as custom scans).
2. Perform daily scans: regardless of the infection source, enabling complete, daily scans of a system's entire hard drive adds another layer of protection. These daily scans can be invaluable in detecting, isolating, and removing infections that initially escape security software's attention.
3. Don't click on email links or attachments: users should never click on email attachments without at least first scanning them for viruses using a business-class anti-malware application. As for clicking on links, users should access Web sites by opening a browser and manually navigating to the sites in question.
4. Deploy DNS protection: users can protect themselves from all these threats by changing the way their computers process DNS services. While a computer professional may be required to implement the switch, OpenDNS offers free DNS services to protect users against common phishing, spyware, and other Web-based hazards.
5. Do not reply to spam messages: almost all spam messages are malicious emails sent by unknown sources. These sources could be hackers who aim to hack into the computers of their victims. Never respond to spam messages because through this, the spammer will know that the email address is active and thus, it increases the chance of your email to be constantly targeted by the spammer.
6. Never give out the company’s e-mail address publicly**:** you should remember that everyone can easily access the Internet. That means, spammers are also lurking on the Internet and are constantly seeking available email addresses which they will send spam emails to. Posting the company’s email address publicly allows others to send spam emails, or worse, hack the account if you are using a weak password.
7. Enter Your Sensitive Data in Secure Websites Only: In order for a site to be ‘safe’, it must begin with ‘https://’ and your browser should show an icon of a closed lock.
8. Avoid Third-Party Downloads  
   Any download is a potential threat. Websites, ads, and messages that contain automatic downloads often hide malware. Avoid clicking through to any banners and suspicious links, don’t use shortened URLs and think carefully before allowing any download.
9. Use a Firewall  
   Firewalls screen data that enters your device from the internet. While most operating systems come with a built-in firewall, it’s also a good idea to use a hardware firewall for full protection. Trojan horses are a complex form of malware, so you need more than two eye to spot them. Using security software like antivirus, anti-malware and firewalls will give you an extra layer of protection.
10. Regular Backup Your Data:

In case, if your computer is infected with a virus or malware, regular data backup helps to restore your data. It is sensible to encrypt all your data so in case if the data is stolen or lost, there are strong chances of being secured.

1. Do not open attachments in spam:

You could get infected with Trojans that will send your email contacts to a spammer as well as entrap you in a spammer distribution chain i.e. your computer might be the one that the spammer uses to send spam emails.

1. Keep your browser updated:   
   Make sure that you use the latest version of your web browser and that all of the latest Internet security patches have been applied.
2. Keep Your Operating System Current:

Whether you are running Windows, Mac OS X, Linux, or any other OS, keep it up to date. OS developers are always issuing security patches that fix and plug security leaks. These patches will help to keep your system secure. Similarly, keep your anti-virus software up to date. Viruses and malware are created all the time. Your scanning software is only as good as its database. It too must be as up to date as possible.

\

**QUESTION THREE**

1. 3 HAMLETS – M
2. 1 ORACLE – O
3. 9 MESSENGERS – R
4. 1 SHELL – S
5. 4 RODENTS – E
6. 1 CALABASH – C
7. 3 PROPHECIES – O
8. 1 DESTINY – D
9. 6 COWRIES – E

Result is MORSE CODE

**3B.** THINGS FALL APART

**QUESTION FOUR:**

Encrypted message TSJSFRHGTJQTNZS

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

ABCDEFGHIJKLMNOPQRSTUVWXYZ

From the English alphabets above Caesar shift of 5 gives:

**VWXYZABCDEFGHIJKLMNOPQRSTU**

Decrypted Caesar 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