**15/ENG02/005**

**AKEGH PETER TERKUMA**

**COE510 (COMPUTER SECURITY TECHNIQUES) ASSIGNMENT**

**Question 1:** Develop a security policy for an XYZ company on the use of mobile devices in that company.

**Solution**

Smartphones, tablet computers, and other mobile devices are very important tools for the organization to achieve business goals. These mobile devices are also a significant risk to data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorized access to the organization’s data and IT infrastructure.

In order to safeguard its customers, intellectual property and reputation, company XYZ has needs to protect its information assets. In this document, a set of practices and requirements for the safe use of mobile devices and applications are outlined.

**Scope**

* All mobile devices (whether owned by the company or owned by employees), that have access to corporate networks, data and systems are governed by this mobile device security policy. The scope of this policy does not include corporate IT-managed laptops.
* Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk authorized by security management must be conducted.
* Applications used by employees on their own personal devices which store or access corporate data, such as cloud storage applications, are also subject to this policy.

**Policy**

**Technical Requirements**

* Devices must use the following Operating Systems: Android 2.2 or later, iOS 4.x or later.
* Devices must be configured with a secure password that complies with the company’s password policy. This password must not be the same as any other credentials used within the organization.
* Devices must store all user-saved passwords in an encrypted password store.
* Only devices managed by IT will be allowed to connect directly to the internal corporate network.
* These devices will be subject to the valid compliance rules on security features such as encryption, password, key lock, etc. These policies will be enforced by the IT department using Mobile Device Management software.

**User Requirements**

* Users may only load corporate data that is essential to their role onto their mobile device(s).
* Users must report all lost or stolen devices to the company’s IT immediately.
* If a user suspects that unauthorized access to company data has taken place via a mobile device, they must report the incident in alignment with the company’s incident handling process.
* Devices must not be “jailbroken” or “rooted” or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
* Users must not load pirated software or illegal content onto their devices.
* Applications must only be installed from official platform-owner approved sources. Installation of code from untrusted sources is forbidden. If you are unsure if an application is from an approved source, contact the company’s IT.
* Devices must not be connected to a PC which does not have up to date and enabled anti-malware protection and which does not comply with corporate policy.
* Devices must be encrypted in line with the company’s compliance standards.
* Users may must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system.
* The above requirements will be checked regularly and should a device be non-compliant that may result in the loss of access to email, a device lock, or in particularly severe cases, a device wipe.
* The user is responsible for the backup of their own personal data and the company will accept no responsibility for the loss of files due to a non-compliant device being wiped for security reasons.
* Users must not use corporate workstations to backup or synchronize device content such as media files, unless such content is required for legitimate business purposes.

**Question 2:** You have been hired by a security company as a security expert to perform the role of an industrial espionage on a XYZ company. Using all the available tools, discuss how to carry out this attack without been noticed.

**Solution**

**Industrial espionage** is the act of obtaining [secret](https://en.wikipedia.org/wiki/Secrecy) or [confidential information](https://en.wikipedia.org/wiki/Confidentiality) from companies or corporations or divulging of the same without the [permission](https://en.wikipedia.org/wiki/Consent) of the holder of the information.  Industrial espionage is conducted by companies for commercial purposes.

**How to Carry out an Industrial espionage on Company XYZ**

* **Using Personal Computers**

Computers are key in exercising industrial espionage due to the enormous amount of information they contain and the ease at which it can be copied and transmitted. I can be disguised as a subsidiary worker (maybe a cleaner or a repairman) to gain access to unattended computers and copy the needed information.

A known employee of Company XYZ may be out of the office with his laptop; I could find a way of conning him/her away from the laptop for some time. This leaves me with access to the laptop for that period of time to copy whatever needed information.

* **Using the Internet**

The rise of the internet and computer networks has expanded the range and detail of information available, and the ease of access. Before now, most companies had their networks isolated from other networks; however, over the years there has been need to connect to the internet, leaving these networks more vulnerable to attacks.

As a security expert, I can use the internet to hack into the network of Company XYZ to gain access to secrets on work computers and servers to steal the needed information. With this access, I can also plant malicious software on computers in the network rand activate it later when needed.

* **Using Malware**

I can use a malware or spyware to exploit vulnerabilities in the software used by Company XYZ. This malware will secretly switch on the computers recording devices to get digital copies of trade secrets, plans, and contacts.

How malware works: Malware infects a device through physical or virtual means; malicious programs can be delivered to a system with a USB drive or can spread over the internet through drive-by downloads, which automatically download malicious programs to systems without the user's approval or knowledge. Sophisticated malware attacks often feature the use of a command-and-control server that allows threat actors to communicate with the infected systems, exfiltration sensitive data and even remotely control the compromised device or server. Spyware   is made to collect information and data on the device user and observe their activity without their knowledge.

Spyware would be installed on the victims’ devices without his knowledge so has to steal his data and record his keystrokes which would give us his login details to the company’s network and free access to get anything we need as we can now pose as him on the network

* **Using Distributed Denial of Service attack**

This approach will involve using compromised computer systems to orchestrate a flood of requests to a target computer in Company XYZ; this would cause it to shut down and deny service to other users.

* **Using Social Engineering**

Social engineering is the psychological manipulation of people into performing actions disclosing confidential information. Using social engineering involves exploring the Relationship between Organizational Culture and Information Security Culture (ISC); ISC is the totality of patterns of behavior in an organization that contribute to the protection of information of all kinds. Research shows that employees often do not see themselves as part of the organization Information Security "effort" and often take actions that ignore organizational information security best interests. As a security expert, I can use the following social engineering approaches to carry out industrial espionage on Company XYZ:

* **Human based Social Engineering**: This involves person to person interaction. I may approach a target staff of Company XYZ claiming to be a new employee, repair person, or researcher (and even offer credentials to support that identity), with that I get to interact with the target having the opportunity to obtain/compromise the needed information about the company. By asking questions, I may be able to piece together enough information to infiltrate an organization’s network. If I am not able to gather enough information from one source, I may contact another source within the same organization and rely on the information from the first source to add to my credibility.
* **Phishing:** Using this process, I can a mail to a staff of the company; this mail will request the recipient to confirm a transaction or change login details. The victim will open the link thinking it is genuine and then get re-directed to a malicious website which captures information.

I can decide to target a single user within Company XYZ seeking unauthorized access to confidential data by using email. This process is referred to as **spear phishing**. Spear Phished emails can be sent in numerous forms. Some of them inform the recipient that the previous email has failed and a link is also provided, which would make the recipient feel that the email is genuine.  The link opened by the victim will be re-directed to website which would request the victim to enter their email address and password or click on the link will download a Trojan.

From the phishing process, personal information such as name, mobile number, email id etc. are gathered and can be used to access certain information that may have been restricted to only privileged staff of Company XYZ.

* **Using Malicious Mobile Applications**: Using this approach, I can trick targets in Company XYZ to download malicious app which pretend to be a genuine one. Through this app, the victims may get to disclose useful information such as email addresses and passwords that may help in gaining access to certain privileged information or services.

**Question 3:**

1. 3 HAMLETS: The 3rd letter is M

1 ORACLE: The 1st letter is O

9 MESSANGERS: The 9th letter is R

1 SHELL: The 1st letter is S

4 RODENTS: The 4th letter is E

1 CALABASH: The 1st letter is C

3 PROPHECIES: The 3rd letter is O

1 DESTINY: The 1st letter is D

6 COWRIES: The 6th letter is E

The plain text message is: MORSECODE

1. SING THAT RAP FALL

The plain text is: THINGS FALL APART

**Question 4:** Moriarty Smith works for XYZ Bank and you suspect him of sending customer details to credit card fraudster by email. You confront him but he sneers at you and says “You have no proof because you will never break my cipher. In fact, in my next email I will tell you when I think you will catch me”. From observation of his encrypted emails you suspect that he is encrypting his text using a Caesar substitution cipher (key 5) and a columnar transposition cipher (key 5). You intercept his very last email containing the short message TSJSFRHGTJQTNZS. What does it say?

**Solution:**

1. Caesar substitution cipher (key 5)

**ABCDEFGHIJKLMNOPQRSTUVWXYZ**

From the English alphabets above Caesar shift % 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**