OLADIMEJI OLUFUNKE MAYOWA

15/ENG02/042

COE510 (COMPUTER SECURITY TECHNIQUES) ASSIGNMENT

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

Answer

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.

Other:

- All mobile devices must be protected by a strong password and must not be disclosed to anyone.
- If you lose your mobile device or it is stolen, it should be reported immediately.
- Do not download applications from untrusted sources always verify first before making any download.
- Block potentially dangerous applications.
- Enable the Remote lock and data wipe option on the mobile device just in case the device gets lost.
- Encryption mechanisms must be verified before sending sensitive information over a wireless network.
- Follow up safe disposal practices when you dispose your mobile device and ensure all sensitive information are erased/removed completely.

- 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

How to Carry out an Industrial espionage on Company XYZ

- **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.

- **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.

- **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 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.

Question 3:

(a) 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

(b) 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:

(a) Caesar substitution cipher (key 5)

ABCDEFGHIJKLMNOPQRSTUVWXYZ

From the English alphabets above Caesar shift % gives:

VWXYZABCDEFGHIJKLMNOPQRSTU

Decrypted Caesar cipher: ONENAMCBOELOIUN

(b) 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**