NAME: KAREEM JADESOLA ‘TANWA

MATRICULATION NUMBER: 15/ENG02/033

COMPUTER SECURITY TACHNIQUES ASSIGNMENT 1.

3RD April, 2020.

1. Security Policies on Mobile Devices for company XYZ.

**Introduction**

Mobile devices, such as smartphones and tablet computers, are important tools for the organization and their use is supported to achieve business goals. However mobile devices also represent a significant risk to information security and 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. This can subsequently lead to data leakage and system infection.

**Security Policy**

* Any employee who has been granted permission to add data or information owned by the company on their phones should agree to the following:
* report any loss or theft of their mobile device(s) to management within 24 hours (including on weekends).
* They consent to having their phone’s or mobile device’s data wiped by our network support staff in the event of loss or theft to protect any data stored on the device.
* IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to District and District-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts the District’s systems, data, student, staff and faculty at risk.
* Devices must be kept up to date with manufacturer or network provided patches. As a minimum, patches should be checked for weekly and applied at least once a month.
* Users 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. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify <Company XYZ> IT immediately.
* Devices must store all user-saved passwords in an encrypted password store.
* Users must only load data essential to their role onto their mobile device(s).
* If a user suspects that unauthorized access to company data has taken place via a mobile device, they user must report the incident in alignment with <Company XYZ>’s incident handling process.
* Devices must not be connected to a PC which does not have up-to-date and enabled antimalware protection and which does not comply with corporate policy. Any phone or mobile device that stores any data owned by ORGANIZATION NAME, whether owned by ORGANIZATION NAME or an individual staff member, must have the following security measures put in place:
* A screen lock (may be known by other names on different devices) must be implemented to require a password or code to be entered after being idle for 2 minutes or more.
* Staff members must not use the default passwords provided by their phone, but must create a new one.

1. So, in order to perform an industrial espionage hypothetically we will need to build a scenario case and characters involved in how it will occur.

Name of company hiring for espionage: **stealth enterprise.**

Name of company to be attacked: **XYZ company,** which is a company that deals with communications and networking.

Name of person hired to carry out espionage: **Sheila.**

So, stealth enterprise decides to hire Sheila to carry out an attack on XYZ company. Sheila being a very pretty and rambunctious lady, essentially an attractive woman does as much extensive research as she can on the company and came to have the following findings:

The head of HR: **Stephen.**

The head of internal operations: **Marcus.**

She also finds that every employee of the company can only enter into the company with fingerprint and ID CARD badge. Also, that guests can only enter if they want to see the managing director and the guest must have a very plausible reason for even seeing the Managing director.

Sheila decides to use social engineering techniques to carry out the attack, by seducing the head of internal operations, Marcus, as well as the head of HR (human resources), Stephen. She plans to seduce both men just in case it doesn’t work out with the other. So, Sheila searches Instagram, Facebook and twitter for both Marcus and Stephen. She finds that Marcus is on facebook and Stephen is on Instagram. Sheila creates fake accounts using the names “Alice Adeola” for Instagram and “Aduke Jacobs” for facebook. Afterwards, she sends both men direct messages and in a couple of minutes they both reply to her (keep in mind that Sheila is a very attractive woman) and she has meaningful/flirty conversations with these men. After a week of flirting, Marcus (head of internal operations) decides to ask her out to dinner, to meet in person and she looks her absolute best wearing the most risqué outfit she could find. Dinner with Marcus goes well and Stephen (head of HR) eventually asks her out for drinks and she does the same thing as she did with Marcus.

So, both relationship with Marcus move really fast but her and Sheila starts to plan how she would carry out the attack on the company. So, she spends the night with Marcus and she plans that as they are watching a movie on his company laptop and he goes to use the toilet or as he falls asleep, she will insert a flash drive into his laptop and install a software(virus) that will steal and copy all the credentials of all the clients of the company.

Then as for Stephen, she plans on using phishing mails to steal sensitive credentials and banking information of the company. She sends him a text that she has mailed him a google doc for him to go through for her as a friendly gesture, when in actuality the link is a malicious HTML attachment masked using the website **bit.ly** to steal information. Malicious .HTML attachments aren't seen as often as .JS or .DOC file attachments, but they are desirable for a couple of reasons. First, there is a low chance of antivirus detection since .HTML files are not commonly associated with email-borne attacks. Second, .HTML attachments are commonly used by banks and other financial institutions so people are used to seeing them in their inboxes.

Ways of preventing such attacks from happening.

* **Monitor employee activity.**

You’ll never know whether your employees are acting maliciously, intentionally, or inadvertently unless you monitor their online presence. It’s especially important to keep an eye on privileged users, such as system administrators and upper management. They can easily gather intelligence while performing their normal tasks and explain any abnormal behaviour as a mistake.

* Conducting a security audit of the company premises. Identify and test the rights of data access and rights of physical access to sensitive spaces for all employees as well as service providers.
* Create a policy to protect sensitive data that covers how it is shared (or not) in conversations, meetings, telephone calls and paper documents.
* **Educate employees**

A key way to thwart a spy is to continuously educate employees. Educate them about potential threats your company faces and the role they play in the security of the organization. Teach them about simple security practices like changing passwords, and give them examples of social engineering attempts that they may encounter. Your employees are your first line of defence in corporate espionage. Make employees aware of the role they play in the security of your organization. Teach them about simple security practices to use in their daily workflow.

* **Secure your infrastructure**

Establish a secure perimeter around your company network. Conventional corporate cybersecurity software, such as firewalls and antivirus software, is your first line of defence. Make sure to separate valuable data from corporate network and limit access to it. Protect your border routers and establish screen subnets. A secure perimeter with a layered approach is the best way to protect yourself from industrial and economic espionage through hacking and malware.

* **Conducting a risk assessment.**

Find potential targets. You need to know what trade secrets and other valuable data your company possesses and how much they’re worth. You can evaluate your trade secrets by comparing them with products already available on the market or with known assets of your competitors. Once you identify your most valuable data, you can guess who may want it. Once you know possible threats and potential attack vectors, you can detect vulnerabilities in your own defences. Risk assessment is key to a risk-based approach to security, which should be part of the security strategy of every organization.

* **Maintain an efficient data access policy**

Many companies provide access to critical data and infrastructure by default. While it may be more convenient, this policy is not secure. Your company should follow the [principle of least privilege](https://en.wikipedia.org/wiki/Principle_of_least_privilege) and prohibit access to all data unless necessary.  Applying the so-called “need to know” principle means that you provide access only to employees who really need information. If unauthorized employees occasionally need to work with confidential information, they can do it under the supervision of authorized staff. By limiting the number of people with access to critical data, you strongly limit the risks of your competitors obtaining this data.

* **Establish an effective security policy**

All security rules should be formalized in a clearly written security policy. This policy should include rules prohibiting password sharing and employees bringing their own devices to work, among other things. Make sure all your employees are aware of it, starting with upper management.

3a. 3 hamlets = ha**M**lets

1 oracle = **O**racle

9 messengers= messenge**R**s

1 shell= **S**hell

4 rodents = rod**E**nts

1 calabash= **C**alabash

3 prophecies=pr**O**phecies

1 destiny= **D**estiny

6 cowries= cowri**E**s

The final message is read as MORSE CODE.

What was done here was, that according to the numbers in front of the text, the letters were counted.

3b. answer = THINGS FALL APART.

4. encrypted text is TSJSFRHGTJQTNZS

First, we decrypt the text using Caesar substitution decryption

Letters of the alphabet = ABCDEFGHIJKLMNOPQRSTUVWXYZ.

Using key 5, we shift to the left by five alphabet letters

Decrypted text now becomes ONENAMCBOELOIUN.

Next, we decrypt the message using columnar decryption

The text is 15 letters long and using key 5(5 columns), it gives us 3 rows i.e. 15/5=3

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| O | N | C | E | I |
| N | A | B | L | U |
| E | M | O | O | N |

The final message reads ONCE IN A BLUE MOON.