Farouk Umar Farouk

15/ENG02/025

Assignment

XYZ Mobile Security Policy

The XYZ company allows the use of mobile devices such as smartphones and tablets as they important tools which can be used to achieve and aid the company's business goals.

Although the use of mobile phones is allowed if the appropriate measures are not taken these devices can be easily exploited by hackers which can raises a significant risk to the company's data security. If the necessary and appropriate security procedures and measures are not taken the company's infrastructure will be become compromised. This unauthorized access may lead to data loss, poor data integrity, system infection and array of threats that may arise from this access.

Hence, the company has to safeguard its assets; customers, intellectual property and reputation. This document will outline the practices all employees should abide by to ensure the safe use of mobile devices and their applications.

Scope

- All mobile devices; employee owned or company issued are governed by this security policy. This policy affects mobile devices alone and does not cover

company laptops; see XYZ laptop security policy.

- Applications on personal devices that have access to the company's data infrastructure, personal network, cloud services are also subject to this policy.
- Exemptions: Ordinarily no device or employee is exempted; for there to be an exemption to this policy the cost of implementation would be too high for the company and a risk analysis needs to be carried out by the company's security experts.

Policy

Technical Requirements

- Devices must store all user saved password in an encrypted password safe.
- Only devices managed by the IT department has access to internal network of the company.
- All user credentials and passwords must comply with the company XYZ password policy and must be different with other credentials used within the company.
- All mobile devices must use device encryption before accessing corporate emails.

User Requirements

- Users must immediately report all lost or stolen devices to the company's IT department.
- Users are allowed to only load corporate data to their mobile device(s) necessary to their roles.
- Devices must be kept up to date with manufacturer or network provided patches. As a minimum patch should be checked for weekly and applied at least once a month.
- Users must have separate emails for personal and work purposes and must be cautious of merging the two.
- The user is responsible for the backup of personal data and the company is not responsible for data loss to devices being wiped because of security reasons.
- Users must not use corporate workstations for backup or synchronization of personal data.
- The above requirements will be checked regularly and should a device be noncompliant that may result in the loss of access to email, a device lock, or in particularly severe cases, a device wipe.

Scenarios where IT department takes action; device wipe (full or partial) and other activity

- Loss or stolen device.
- A device is rooted or jailbroken.
- An application on the device may be a security risk or vulnerability.
- The user exceeds the maximum failed password attempts.

Industrial Espionage Scenario

Company XYZ is an electric automobile car company. As a security expert I was hired by their security department to gain unauthorized access into their systems which contains confidential information regarding their manufacturing specifications, designs, blueprints, procedures and testing documentation. The tasks given all fall under the data assets of the company.

The first step to be carried out is reconnaissance which involves data infrastructure analysis which involves the understanding of the company's network and systems architecture. The goal of reconnaissance is to identify the weak point of the target, any information gathered about the target may be the crucial piece needed to reveal the critical weakness in the defense of the target. This reconnaissance is similar to that of the military. In this phase of the attack, time will be spent observing and probing the target's computer systems and networks to find their weakness. Any weaknesses found may lead to the successful infiltration.

Somme of the critical information which must be obtained in this phase are listed below:

1. Network information:
    a. IP addresses
    b. Subnet masks
    c. Network Topology
    d. Domain names

2. Security Policies:
    a. Firewalls
    b. Password complexity requirements
    c. Expired/disable account retention
    d. Physical security
3. Human Information:
    a. Vulnerable individuals
    b. Frequent hangouts
    c. Computer knowledge.
4. Host Information:
    a. Hardware
    b. Architecture type
    c. Operating system family and version

Now I start this reconnaissance by foot printing, which is the act of minimally interacting with the targets network without raising flags in the logs. I would first start with the public site in such a way I can establish a TCP connection without alerting the admins of the intrusion. Social engineering can also be combined to gain information on the staff with social media stalking, actual stalking at hangouts, finding the right incentive for a potential inside man or other opportunistic staff. Network information can also be obtained freely via public records online. Every IP address and Domain

Name must be registered in a public database. As a result, a few queries to the right places will provide the target domain's IP address range, DNS servers.

The next step will be the infiltration; where the goal is to gain remote control of the targets network. A computer program was developed to take advantage of target weakness and grant me remote access to as an administrator on a host system. Upon gaining remote access, copies of the required documents were downloaded over at a time so as not raise a flag.

Finally, to conclude the objective no trace must be left of the trespass. This is somewhat difficult because computers keep records of every logon, logoff, startup, shutdown, network connection, program execution, and error received. Erasing all trace of an intrusion is nearly impossible, which is why the masking the origin of the attack was done and diverting the attention of the intended target with a false one was done to delay the efforts that may be carried out in the investigation of the breach of security as well leaving a backdoor into the system for future attacks.

Now, after reporting back to my employers about how I penetrated their security and the pitfalls in their systems, I recommend some ways to detect and prevent similar attacks:

1. 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 the employees are aware of it, starting with upper management.
2. An efficient data access policy: The company should follow the principle of least privilege and prohibit access to all data unless necessary. This principle means that

access is granted to 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, it strongly limits the risks of competitors obtaining this data.

3. Education of employees: The best way to prevent employees from inadvertently helping the enemy is to educate them. Tell them about potential threats the company faces. Make employees aware of the role they play in the security of the organization. Teach them about simple security practices to use in their daily workflow. This helps protect the staff from social engineering and will prevent simple security mistakes.
4. Monitor Employee Activity: This makes all employees' actions fully visible and allows the company to detect data theft and take measures in a timely manner. In case an incident happens, the records will aid the investigation. Moreover, monitoring employees can deter opportunistic employees from stealing data, as they know their actions are recorded.
5. Response to threats in real time: A process should be created that uses analytics to detect any unusual behavior, this would prevent data breaches. Any alert system should also be in place to monitor and raise flags for the security team to take action, to compliment this an automated incident response system should be on ground to protect data in the event of an attack by tracing the origin, termination of an application process, blocking access or any other means of counter before the arrival of the security team.

3a)

3 HAMLETS = 3rd letter =M

1 ORACLE = 1st letter =O

9 MESSENGERS = 9th letter = R

1 SHELL = 1st letter = S

4 RODENTS = 4th letter = E

1 CALABASH = 1st letter = C

3 PROPHECIES = 3rd letter = O

1 DESTINY = 1st letter = D

6 COWRIES = 6th letter = E

Answer: MORSECODE

3b)

SING THAT RAP FALL = THINGS FALL APART

4) key = 5, TSJSFRHGTJQTNZS = 15 words

Column Transposition Cipher Therefore: 15/5 = 3 rows

Place along each column

A B C D E

t s h j n

s f g q z

j r t t s

After: tshjnsfgqzjrtts

Caesar substitution key = 5

t = 20^{th} – 5 =15^{th} letter = o

s = 19^{th} – 5 = 14^{th} letter = n

h = 8^{th} – 5 = 3^{rd} letter = c

j = 10^{th} – 5 = 5^{th} letter = e

n = 14^{th} – 5 = 9^{th} letter = i

s = 19^{th} – 5 = 14^{th} letter = n

f = 6^{th} – 5 = 1^{st} letter = a

g = 7^{th} – 5 = 2^{nd} letter = b

q = 17^{th} – 5 = 12^{th} letter = l

z = 26^{th} – 5 = 21^{st} letter = u

j = 10^{th} – 5 = 5^{th} letter = e

r = 18^{th} – 5 = 13^{th} letter = m

t = 20^{th} – 5 =15^{th} letter = o

t = 20^{th} – 5 =15^{th} letter = o

s = 19^{th} – 5 = 14^{th} letter = n

Answer: onceinabluemoon; once in a blue moon.