Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 3/26/2022 9:28:47 am • Time spent: 02:25

Score: 70%

Passing Score: 80%

Question 1: ✕ Incorrect

Your organization recently purchased 18 iPad tablets for use by the organization's management team. These devices have iOS pre-installed on them.

To increase the security of these devices, you want to apply a default set of security-related configuration settings.

What is the BEST approach to take to accomplish this? (Select two. Each option is part of a complete solution.)

- [ ] Require users to install the configuration profile.
- [ ] Configure and apply security policy settings in a mobile device management (MDM) system.
- [x] Enroll the devices in a mobile device management (MDM) system.
- [x] ~~Configure and distribute security settings in a configuration profile.~~
- [ ] Configure security settings in a Group Policy Object.
- [ ] Join the tablets to a Windows domain.

EXPLANATION

A mobile device management (MDM) solution can push policies directly to each tablet device over a network connection. This option enables policies to be remotely enforced and updated without any action by the end user. The tablet devices must be enrolled in the MDM system before the policy settings can be applied.

One of the key problems associated with managing mobile devices is the fact that they can't be joined to a Windows domain. This means Group Policy can't be used to automatically push security settings to mobile devices. For devices running Apple's iOS operating system, security settings can be distributed in a configuration profile. The profile can be defined so that only an administrator can delete the profile, or you can lock the profile to the device so that it cannot be removed without completely erasing the device. However, this option relies on the end user to install the profile, which can be problematic. It's also not a dynamic strategy. Making even the smallest change to your mobile device security policies requires a great deal of effort.

REFERENCES

9.6.2 Mobile Device Connection Facts

q_mbl_dev_conn_cell_secp7.question.fex

Question 2: ✔ Correct

Recently, a serious security breach occurred in your organization. An attacker was able to log in to the internal network and steal data through a VPN connection using the credentials assigned to a vice president in your organization.

For security reasons, all individuals in upper management in your organization have unlisted home phone numbers and addresses. However, security camera footage from the vice president's home recorded someone rummaging through her garbage cans prior to the attack. The vice president admitted to writing her VPN login credentials on a sticky note that she subsequently threw away in her household trash. You suspect the attacker found the sticky note in the trash and used the credentials to log in to the network.

You've reviewed the vice president's social media pages. You found pictures of her home posted, but you didn't notice anything in the photos that would give away her home address. She assured you that her smartphone was never misplaced prior to the attack.

Which security weakness is the MOST likely cause of the security breach?

- Sideloaded apps were installed on her smartphone.
- ➡ Geotagging was enabled on her smartphone.
- A Christmas tree attack was executed on her smartphone.
- Weak passwords were used on her smartphone.

EXPLANATION

Geotagging embeds GPS coordinates within mobile device files (such as image or video files) created with the device's camera. While this feature can be useful in some circumstances, it can also create security concerns. In this scenario, the vice president probably posted geotagged images to her social media accounts. The attacker likely analyzed the images to discover where she lived and then conducted a dumpster dive attack that yielded the sticky note with the vice president's VPN credentials. The best way to remedy this weakness is to simply disable this functionality in the mobile devices you manage.

Sideloaded apps can only be installed if the device administrator has specifically configured the device to allow them, so this is an unlikely cause. A weak smartphone password is a concern, but this would not be the cause of the exploit if the device were always in the vice president's possession. A Christmas tree attack is used to fingerprint network devices, not to gather personally identifiable information.

REFERENCES

9.6.2 Mobile Device Connection Facts

q_mbl_dev_conn_geo_tag_secp7.question.fex

Question 3: ✔ Correct

Which of the following mobile device security considerations disables the ability to use the device after a short period of inactivity?

- Remote wipe
- TPM
- GPS
- Screen lock

EXPLANATION

A lockout (or screen lock) disables the ability to use the device after a short period of inactivity. The correct password or personal identification number (PIN) unlocks the device.

Remote wipe, also known as sanitization, remotely clears specific, sensitive data on a mobile device. This task is also useful if you are assigning the device to another user or after multiple incorrect password or PIN entries. Data encryption also ensures data confidentiality on the device. Voice encryption (on mobile phones) ensures data confidentiality during transit. Global Positioning System (GPS) tracking can assist in a device's recovery by displaying its current location. Trusted Platform Module (TPM) is a hardware chip on the motherboard that can generate and store cryptographic keys to check the integrity of startup files and components.

REFERENCES

9.6.2 Mobile Device Connection Facts

q_mbl_dev_conn_lock_secp7.question.fex

Question 4: ✔ Correct

Your organization recently purchased 20 Android tablets for use by the organization's management team.

To increase the security of these devices, you want to ensure that only specific apps can be installed. Which of the following would you implement?

- Application Control
- App blacklisting
- App whitelisting
- Credential Manager

EXPLANATION

App whitelisting is the process of defining specific apps that users can have on their mobile devices. Apps not on the whitelist are not allowed to be installed.

Blacklisting apps is the process of defining specific apps that users cannot have on their mobile devices.

The Credential Manager function that is implemented in most mobile operating systems can store usernames and passwords for the end user.

Application Control is implemented by each mobile operating system. It determines how apps are installed and where they come from.

REFERENCES

9.6.2 Mobile Device Connection Facts

q_mbl_dev_conn_white_secp7.question.fex

Question 5: ✔ Correct

A smartphone was lost at the airport. There is no way to recover the device. Which of the following ensures data confidentiality on the device?

- GPS
- Remote wipe
- Screen lock
- TPM

EXPLANATION

Remote wipe, also known as sanitization, remotely clears specific, sensitive data on a mobile device. This ensures that whoever has the device cannot see the sensitive data. This task is also useful if you are assigning the device to another user or after multiple incorrect entries of the password or PIN. Data encryption also ensures data confidentiality on the device. Voice encryption (on mobile phones) ensures data confidentiality during transit.

Global Positioning System (GPS) tracking can assist in the recovery of the device by displaying its current location. A lockout (or screen lock) disables the device's interface after a short period of inactivity. The correct password or personal identification number (PIN) unlocks the device. Trusted Platform Module (TPM) is a hardware chip on the motherboard that can generate and store cryptographic keys to check the integrity of startup files and components.

REFERENCES

9.6.2 Mobile Device Connection Facts

q_mbl_dev_conn_wipe_secp7.question.fex

Question 6: ✕ Incorrect

Which of the following is the recommend Intune configuration?

- Account portal
- Intune Standalone
- ~~Hybrid MDM~~
- Company portal

EXPLANATION

Intune Standalone is the recommended deployment method. Intune Standalone is a cloud-only solution that is managed using a web console that can be accessed from anywhere with internet access.

Hybrid MDM with Configuration Manager is a solution that combines Intune's mobile device management capabilities into Configuration Manager.

The Account portal is used to manage subscriptions, users, groups, and domains.

The Company portal is used by end users to manage their own account and enroll devices.

REFERENCES

9.6.4 Enforcing Mobile Device Security Facts

q_mbl_dec_sec_config_secp7.question.fex

Question 7: ✔ Correct

Which of the following is a solution that pushes security policies directly to mobile devices over a network connection?

- ➡ Mobile device management (MDM)
- Group Policy
- Application Control
- Credential Manager

EXPLANATION

Mobile device management (MDM) is a solution that pushes security policies directly to each device over a network connection. MDM solutions enable policies to be remotely enforced and updated without any action by the end user. Many companies have MDM products, including Apple, Cisco, and Microsoft.

The Credential Manager function that is implemented in most mobile operating systems can store usernames and passwords for the end user.

Group Policy cannot be used to automatically push security settings to mobile devices. This is because the devices cannot be joined to a Windows domain.

Application Control is implemented by each mobile operating system. It determines how apps are installed and where they come from (App Store, etc.).

REFERENCES

9.6.4 Enforcing Mobile Device Security Facts

q_mbl_dec_sec_mdm_secp7.question.fex

Question 8: ✕ Incorrect

The IT manager has tasked you with configuring Intune. You have enrolled the devices and now need to set up the Intune policies.

Where would you go to set up the Intune policies?

- In the Company portal, select **Management > Policy > Add Policy**.
- ➡ In the Admin portal, select **Policy > Add Policy**.
- In the Company portal, select **Policy > Add Policy**.
- ~~In the Admin portal, select **Management > Policy > Add Policy**.~~

EXPLANATION

To set up Intune policies, access the Admin portal and then select **Policy > Add Policy**.

REFERENCES

9.6.4 Enforcing Mobile Device Security Facts

q_mbl_dec_sec_policies_secp7.question.fex

Question 9: ✔ Correct

Which of the following Intune portals is used by end users to manage their own account and enroll devices?

- Account portal
- Add Intune Users
- Company portal
- Admin portal

EXPLANATION

The Company portal is used by end users to manage their own account and enroll devices.

The Admin portal is used to manage enrolled devices and policies.

Add Intune Users is a configuration task that is completed in the Account portal.

The Account portal is used to manage subscriptions, users, groups, and domains.

REFERENCES

9.6.4 Enforcing Mobile Device Security Facts

q_mbl_dec_sec_portal_secp7.question.fex

Question 10: ✔ Correct

Your organization recently purchased 20 Android tablets for use by the organization's management team.

You are using a Windows domain. Which of the following should you use to push security settings to the devices?

- Application Control
- Credential Manager
- Intune
- Group Policy

EXPLANATION

Intune is Microsoft's cloud-based mobile device management (MDM) platform that allows a network administrator to remotely manage and secure mobile devices.

The Credential Manager function that is implemented in most mobile operating systems can store usernames and passwords for the end user.

Group Policy cannot be used to automatically push security settings to mobile devices. This is because the devices cannot be joined to a Windows domain.

Application Control is implemented by each mobile operating system. This determines how apps are installed and where they come from.

REFERENCES

9.6.4 Enforcing Mobile Device Security Facts

q_mbl_dec_sec_settings_secp7.question.fex