

Exam Report: 7.11.5 Practice Questions

Date: 1/23/2020 1:34:56 pm  
Time Spent: 11:38

Candidate: Garsteck, Matthew  
Login: mGarsteck

Overall Performance



View results by: ☐ Objective Analysis ☒ Individual Responses

Individual Responses

Question 1: Incorrect

Match each bring your own device (BYOD) security issue on the right with a possible remedy on the left. Each remedy may be used once, more than once, or not at all.

Preventing malware infections

Implement a network access control (NAC) solution.

Supporting mobile device users

~~Enroll devices in a mobile device management system.~~

Specify who users can call for help with mobile device apps in your acceptable use policy.

Preventing loss of control of sensitive data

~~Specify where and when mobile devices can be possessed in your acceptable use policy.~~

Enroll devices in a mobile device management system.

Preventing malicious insider attacks

~~Specify who users can call for help with mobile device apps in your acceptable use policy.~~

Specify where and when mobile devices can be possessed in your acceptable use policy.

Applying the latest anti-malware definitions

~~Enroll devices in a mobile device management system.~~

Implement a network access control (NAC) solution.

Explanation

Even though it entails a host of security risks, bring your own device (BYOD) is very common practice in the modern work environment. Security administrators need to keep the following BYOD security issues in mind:

- If a user's tablet or phone has been infected with malware, then the infection can be spread when she connects her device to your organization's network. Consider implementing a network access control (NAC) solution that remediates devices before allowing them to connect to your network.
- If a user copies sensitive data to their device, your organization could potentially lose control of that information. Consider requiring personal devices to be enrolled with a mobile device management infrastructure, such as Windows Intune, to enforce mobile device security policies.
- If a user is so inclined, she could use her mobile device to conduct a malicious insider attack. Implement an acceptable use policy that specifies where and when mobile devices can be possessed within the organization.
- Relying on the end user to implement operating system and anti-malware definition updates is unwise. Instead, consider implementing a network access control (NAC) solution that remediates devices before allowing them to connect to your network.
- If a user brings a personally-owned device on site, then the question of who will provide support for the device and the apps used on the device needs to be clearly identified. Implement an acceptable use policy that specifies where users can get support for personally-owned mobile devices, which apps are can be used with organizational data, and where users can get support for these apps.

References

LabSim for Security Pro, Section 7.11.  
[All Questions SecPro2017\_v6.exm BYOD\_SEC\_02]

Question 2: Incorrect

Match each bring your own device (BYOD) security concern on the right with a possible remedy on the left. Each remedy may be used once, more than once, or not at all.

Users take pictures of proprietary processes and procedures.

Specify where and when mobile devices can be possessed in your acceptable use policy.

Devices with a data plan can email stolen data.

~~Specify who users can call for help with mobile device apps in your acceptable use policy.~~

Specify where and when mobile devices can be possessed in your acceptable use policy.

Devices have no PIN or password configured.

Enroll devices in a mobile device management system.

Anti-malware software is not installed.

Implement a network access control (NAC) solution.

A device containing sensitive data may be lost.

Enroll devices in a mobile device management system.

Explanation

Even though it entails a host of security risks, bring your own device (BYOD) is very common practice in the modern work environment. Security administrators need to keep the following BYOD security issues in mind:

- If a user is so inclined, she could use her mobile device to conduct a malicious insider attack. For example, she could use the built-in camera, which nearly all modern mobile devices have, to take pictures of sensitive internal information. She could also use the device's mobile broadband connection to transfer stolen data to parties outside the organization, bypassing the organization's network security mechanisms. To defend against these activities, implement an acceptable use policy that specifies where and when mobile devices can be possessed within the organization. For example, the possession of mobile devices may be prohibited in high-security areas.
- If a user copies sensitive data to their device, your organization could potentially lose control of that information. For example, the user may not have implemented appropriate security settings on their device, allowing anyone who gains access to the device to view the sensitive data. In addition, the user may lose the device, allowing anyone who finds it to access the sensitive data. To address these issues, require personal devices to be enrolled with a mobile device management infrastructure, such as Windows Intune, to enforce mobile device security policies.
- To ensure anti-malware software is installed, consider implementing a network access control (NAC) solution that remediates devices before allowing them to connect to your network.

## References

LabSim for Security Pro, Section 7.11.

[All Questions SecPro2017\_v6.exm BYOD\_SEC\_03]

### ▼ Question 3: Correct

If a user's BYOD device, such as a tablet or phone, is infected with malware, that malware can be spread if that user connects to your organization's network. One way to prevent this event is to use a network access control (NAC) system.

How does an NAC protect your network from being infected by a BYOD device?

- ☐ The NAC notifies users that personally-owned devices are subject to random searches if brought on site.
- ☐ The NAC forces BYOD devices to connect to a guest network that is isolated from your production network.
- ➡ ☒ The NAC remediates devices before allowing them to connect to your network.
- ☐ The NAC specifies which apps can be used while the BYOD device is connected to the organization's network.

## Explanation

The NAC remediates devices before allowing them to connect to your network. This means that the NAC performs the following types of device management tasks before allowing a device to connect to the network:

- Operating system updates
- App updates
- Anti-malware installation
- Anti-malware definition updates

An alternative to using an NAC solution is forcing BYOD devices to connect to a guest network that is isolated from your production network. An acceptable use policy specifies which apps can be used while the BYOD device is connected to the organization's network. An acceptable use policy also notifies users that personally-owned devices are subject to random searches if brought on site.

## References

LabSim for Security Pro, Section 7.11.

[All Questions SecPro2017\_v6.exm BYOD\_SEC\_04]

### ▼ Question 4: Incorrect

Users in the sales department perform many of their daily tasks, such as emailing and creating sales presentations, on company-owned tablets. These tablets contain sensitive information. If one of these tablets is lost or stolen, this information could end up in the wrong hands.

The chief information officer wants you to implement a solution that can be used to keep sensitive information from getting into the wrong hands if a device is lost or stolen.

Which of the following should you implement?

- ☒ ~~A network access control solution~~
- ☐ An acceptable use policy
- ☐ A guest wireless network that is isolated from your organization's production network
- ➡ ☐ A mobile device management infrastructure

## Explanation

A mobile device management infrastructure, such as Microsoft Intune, can be used to wipe data clean from a device that has been lost or stolen.

A network access control solution can remediate devices before allowing them to connect to your network. An acceptable use policy can be used to define what kind of data is allowed on personally-owned devices and what kind of data is prohibited. A guest wireless network that is isolated from your organization's production network allows user-owned devices to gain internet access, but quarantines them from the rest of your organization's production network.

## References

LabSim for Security Pro, Section 7.11.


[All Questions SecPro2017\_v6.exm BYOD\_SEC\_05]

### ▼ Question 5: Incorrect

Users in the Sales department perform many of their daily tasks, such as emailing and creating sales presentations, on their personal tablets.

The chief information officer worries that one of these users might also use their tablet to steal sensitive information on the organization's network. Your job is to implement a solution that can prevent insiders from accessing sensitive information stored on the organization's network from their personal devices while giving them access to the internet.

Which of the following should you implement?

-  ☐ A guest wireless network that is isolated from your organization's production network
- ☒ ~~A network access control solution~~
- ☐ A mobile device management infrastructure
- ☐ An acceptable use policy

### Explanation

A guest wireless network that is isolated from your organization's production network allows user-owned devices to gain internet access, but quarantines them from sensitive information on your organization's production network.

A mobile device management infrastructure, such as Microsoft Intune, can be used to wipe data from a device that has been lost or stolen. A network access control solution can remediate devices before allowing them to connect to your network. An acceptable use policy can be used to define what kind of data is allowed and prohibited on personally-owned devices.

### References

LabSim for Security Pro, Section 7.11.

[All Questions SecPro2017\_v6.exm BYOD\_SEC\_06/]