When dealing with a Windows 7 computer infected with the WannaCry malware, immediate and effective action is crucial to secure the system and prevent further damage. Here’s a step-by-step plan to handle the situation, including an evaluation of various possibilities for securing the system:

Immediate Intervention

1. **Isolate the Infected System**

Disconnect the infected computer from the network (both wired and wireless).

- Pros: Prevents the spread of the malware to other systems.
- Cons: May interrupt critical operations if the infected machine is essential for ongoing tasks.

2. **Power Off the System**

Turn off the infected machine to halt any ongoing encryption processes.

-Pros: Stops the malware from encrypting more files.

-Cons: Any unsaved data will be lost, and some data might already be encrypted beyond recovery.

Securing the System: Possibilities and Evaluation

1. **Restore from Backup**

Restore the system from a clean backup taken before the infection.

- Pros: Ensures the system is free from malware, and data integrity is maintained if backups are recent.
- Cons: Data created after the last backup will be lost. Requires regular and reliable backup practices.

2. **Reinstall the Operating System**

Perform a clean installation of the operating system.

- Pros: Completely removes the malware, ensuring a clean start.
- Cons: Time-consuming, and all data and applications must be reinstalled and reconfigured. Essential to ensure data backup before reinstallation.

3. **Apply Security Patches**

Ensure all systems are patched with the latest security updates, specifically MS17-010 for WannaCry.

- Pros: Fixes the vulnerability exploited by WannaCry and protects against future attacks.
- Cons: Only effective after malware removal and might not be sufficient alone if the system is already compromised.

4. **Run Anti-Malware Tools**
   Use trusted anti-malware tools to scan and remove the infection.
   - Pros: Can potentially remove the malware without data loss.
   - Cons: Might not detect or completely remove all malware components. Risk of reinfection if root cause is not addressed.

5. **Network Segmentation and Monitoring**
   Implement network segmentation to limit the spread of malware and monitor for unusual activity.
   - Pros: Enhances overall network security and limits potential damage from infections.
   - Cons: Requires significant planning and resources to implement effectively.

6. **Update to a Supported Operating System**
   Upgrade from Windows 7 to a supported version like Windows 10.
   - Pros: Supported OS versions receive regular security updates, reducing vulnerability exposure.
   - Cons: May require hardware upgrades and involves a transition period with potential compatibility issues.

Detailed Steps for Each Possibility

Restore from Backup

1. Ensure backups are intact and malware-free.
2. Disconnect the infected machine from the network.
3. Restore the system from the backup.
4. Apply all necessary security patches after restoration.
5. Reconnect to the network once the system is secured.

Reinstall the Operating System

1. Backup essential data, if possible.
2. Disconnect the machine from the network.
3. Perform a clean installation of Windows 7 or upgrade to Windows 10.
4. Install all security updates and patches.
5. Reinstall necessary applications and restore data from verified clean backups.

Apply Security Patches

1. Download the MS17-010 patch from a secure, isolated system.
2. Disconnect the infected machine from the network.
3. Apply the patch offline.
4. Run a thorough scan with updated anti-malware tools.
5. Reconnect and monitor the system.

Run Anti-Malware Tools

1. Download updated anti-malware tools on a separate, clean system.
2. Transfer the tools to the infected machine using a secure method.
3. Disconnect the infected machine from the network.
4. Run the anti-malware tools in safe mode.
5. Apply all security patches post-cleanup.

Network Segmentation and Monitoring

1. Isolate critical systems from general network segments.
2. Implement strict access controls and regular monitoring.
3. Conduct a comprehensive network security audit.
4. Use intrusion detection and prevention systems (IDS/IPS).

Update to a Supported Operating System

1. Plan and schedule the upgrade to minimize disruption.
2. Ensure compatibility of applications with the new OS.
3. Backup all critical data.
4. Upgrade or clean install Windows 10.
5. Apply all security updates and patches.
6. Restore data and reinstall applications.

Conclusion

Each approach has its own advantages and disadvantages. A combination of these strategies, tailored to the specific environment and requirements of the organization, will provide the most effective defense against WannaCry and similar threats.