Windows System Recovery and the NIST Cybersecurity Framework

Posted on September 21, 2018

Part 1

1. a) Create a system restore point for a Windows 10 system. To create a restore point in Windows, first launch Cortana and, say, open the control panel, after which the control panel opens and select Recovery. In the next screen, select Configure System Restore. Next, turn the system restore Utility on, and everything is set. Click OK, and the system restore will be created.

b) Use a specific system restore point to roll back changes made to a Windows 10 system. Open Cortana and search for Create a restore point on the next screen. Click on System Properties

Click on the Next button, then select the most recent known working restore point. This helps to fix the problem. Click on the Scan for affected programs button, click Close, and then click the Next and Finish buttons and the computer will be restored to its state before the event.

c) Delete system restore points from a Windows 10 system restore points are stored in protected hidden OS to delete restore points. Search for the control panel, open the control panel, click on the Recovery icon, and click on Configure System Restore. Then, on the next screen, click on System Protection from the protection setting, select a drive to delete all restore points, click on the configure button, and click on delete button and click on continue button to confirm, then close when finishing the restore points will be deleted from the computer.

2. a) incidence response. First, the resources needed are defined, and a plan for the response- before the occurrence highlights the framework to respond to the incidence. Stop anything from being further removed.in case of hacking of a website, it is to prevent further hacking by blocking communication channels like internet access to prevent further data access or data loss (NIST Cybersecurity Framework).

What happened after the hacking or the incident? Identify what has been done or changed or the data that has been stolen. Use system logs to identify what has happened. This can be achieved by running internet connectivity monitors. Then, the consequence of the data that has gone public, that is, data that has gone to the competitor domain in business, is identified. Rebuild, backup, and recovery- depending on what happened to the system or website. Get to know what was unauthorizedly accessed, fix the vulnerable points to prevent any occurrence from happening again, and reset system passwords. Using the backup and the rebuilt system, recovery tools are used to recover the system to normal. The Windows registry is a database where all settings and operating

systems are stored, and the OS's components are programmed to use it. In occurrence, in the window, a key is added to the Windows registry. To back up the Windows registry, go to the start, search for regedit.exe, click on the registry key to backup, select File, and then Export and save the backup (NIST Cybersecurity Framework).

b) Blocking network requests -minimizing administrator privileges limits the execution of content that requires registry modifications. This prevents system configuration change from unauthorized changes. Also, the use of monitor mode, which provides logs of changes executed (NIST Cybersecurity Framework)

Ensure the files that have been accessed are in good version, as well as the creation and modification date. Monitor the changes made by the unauthorized access and reconcile changes. Focuses on the priority and take alerts before more damages are done to the file (NIST Cybersecurity Framework).

c) In Windows 10, go to start> setting > update and Security >recovery, click Get started, and then click on Reset this PC. On the next screen, click on Keep My Files, choose the files to remove, and confirm your action.

d) Cleaning of the control panel using the Windows registry. You can remove the installed app and changes that are HKEY_LOCAL_MACHINE\SOFTWARE\windows\currentVersion\uninstall. Identify the applications to remove and delete by deleting its key.

Part 2

Use of local group policy in Windows 10 to prevent automatic update: use the Windows key +R and type gpedit.msc and browse to Windows update, right-click to configure automatic update, enable the policy and choose auto download and notify for install, click on apply and ok to complete. Planning of the incident where you assess threat detection and conduct cyber hunting practice. After preparation, monitor event occurrence to detect any and alert. After the event is analyzed, coordinate the shutdown of the device. Rebuild the OS and change the passwords for all accounts. After the rebuild, complete the documentation, update intelligence threats, and create preventive measures to prevent future incidents. The following are notes, warnings, and restrictions to put in place: turn off compatibility view, turn off the Windows Defender and other Microsoft networks, turn off automatic download and installation of applications, and do not allow automatic update location. Turn off all automatic updates of Microsoft features and specify the Microsoft intranet update service location. Turn off the download of the ActiveX version list automatically. For tailored experience, do not use diagnostic data and enable NTP client (NIST Cybersecurity Framework).

Also, protect the clipboard and what is copied in it, ensure browsing protection through input spoofing, and protect messages from queueing.

Reference

https://www.nist.gov/programs-projects/cybersecurity-framework

http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructurecybersecurity

https://www.federalregister.gov/articles/2013/02/26/2013-04413/developing-a-framework-to-improvecritical-infrastructure-cybersecurity

http://csrc.nist.gov/cyberframework/rfi_comments.html

http://csrc.nist.gov/cyberframework/nist-initial-analysis-of-rfi-responses.pdf
http://www.nist.gov/itl/csd/cybersecurity-framework-workshop.cfm
http://www.nist.gov/itl/csd/cybersecurity-framework-workshop-may-29-31-2013.cfm
http://www.nist.gov/itl/upload/draft_outline_preliminary_framework_standards.pdf
http://www.nist.gov/itl/csd/3rd-cybersecurity-framework-workshop-july-10-12-2013-san-diego-ca.cfm
http://www.nist.gov/itl/upload/draft_framework_core.pdf