**ICS26014 REPORT**

**CONTENT**

1. Services
   1. What are services?

* Services refer to programs that listen for and respond to network traffic. Other services allow direct access to your computer. These include:
  + Web servers, file servers, FTP servers, email and proxy server
  + Remote access programs such as Remote Desktop
  + Open ports
  + Allowing others open access to your computer and your files
  1. How to tell if services are necessary?
* In general, services are necessary if:
  + There's a clear University business or educational need for them
  + They are generally appropriate given a role at the University
  + They don't allow anonymous access or guest access to your computer or files unless there is a specific business need to do so (this is normally controlled with file sharing settings)
* Services also must NOT:
  + Introduce a security risk
  + Interfere with other University resources or the network
  + Create an excessive burden on campus infrastructure or resources
  + Services creating any of the harmful conditions above are subject to blocking or disconnection from the campus network per ITS' Procedures for Blocking Network Access.

1. Disabling unused services
   1. Why turn off unnecessary services?

* Eases the computing load.
* To reduce the resource footprint, such as memory usage, on the computer.
* To make a computer more secure. However, it is also possible to disable vital security services, so we must avoid accidentally exposing the system to outside threats.
  1. Status

Each service shows its Status indicating whether a service is running, stopped or not loaded/running (blank). Status is heavily influenced by the varied Startup Type options available:

* Automatic services load and start at boot time and are usually running. Disabling these unnecessary services will typically have the greatest effect on system performance.
* Automatic (Delayed Start) services will start just after the system boots.
* Automatic (Delayed Start, Trigger Start) services will start after the system boots, but only when the service is called. The service will not run if it is not called.
* Manual services allow Windows to start a service if it is needed. In many cases, Manual services are often unnecessary and are not currently running.
* Manual (Trigger Start) services allow Windows to start services when the service is specifically called. If the service is not called, the service will not start.
* Disabled services will not start even if the service is called, and this can sometimes cause unwanted or regularly occurring errors in Event Viewer.

1. Identify what could be unused services in an enterprise/network
   1. Services that are safe to disable

* Communication services
  + Bluetooth Support Service handles discovery and association of Bluetooth devices. Stopping or disabling this service will prevent installed Bluetooth devices from operating properly and prevent the computer from discovering or pairing new devices.
  + Infrared Monitor Service handles management and file transfers using infrared devices. Stopping or disabling this service will prevent infrared devices from operating.
  + Internet Connection Sharing is a legacy service that handles network translation, addressing, name resolution, DNS, and intrusion protection for home and small office networks.
  + Remote Registry service enables remote users to change registry settings on the PC. Disable this service to prevent remote changes to the registry.
  + TCP/IP NetBIOS Helper service supports NetBIOS over TCP/IP and NetBIOS name resolution. Disabling this service will prevent network printing.
  + Telephony service provides Telephony API support for applications that use telephony devices on the local computer. Disable this service if there are no telephony devices used on the PC.
* Media services
  + Audio Video Control Transport Protocol service handles some Bluetooth elements, and can be disabled if the PC does not use Bluetooth audio device or wireless headphones.
  + Fax service enables the PC to send and receive faxes. Disable this service if the PC is not intended to support fax operation, which is also dependent on other services such as print spooling and telephony.
  + Touch Keyboard and Handwriting Panel service handles touch keyboard and handwriting management for late model PCs such as Microsoft Surface Pro PCs. Disable this service to stop the touch keyboard from running.
  + Windows Camera Frame Server service allows multiple client devices to access video frames from cameras. Disable this service if the PC is not used for video or video editing tasks.
  + Windows Image Acquisition services support image handling from scanners and cameras. Disable this service if the PC is not receiving image data from scanners or cameras.
* Security services
  + BitLocker Drive Encryption service provides secure OS boot and full volume encryption for storage volumes.
  + Certificate Propagation service is typically related to smart card use, copying user and root certificates from smart cards into the user's certificate store.
  + Encrypting File System service supplies the principal mechanisms needed to store encrypted files on NTFS volumes.
  + Netlogon service handles the connection between the PC and the local domain controller that authenticates users and network services such as DNS.
  + Smart Card Services handle smart card operations by the PC. Smart cards are tamper-proof devices used to enhance authentication security for tasks such as system sign-on and securing email.
  + Windows Defender Antivirus Service is basically the default antimalware tool under Windows.
  + Windows Defender Antivirus Network Inspection Service is the default intrusion detection/prevention tool under Windows.
  + Windows Defender Firewall is the default network firewall under Windows that checks and controls network traffic access to communication ports, blocking unauthorized access to the computer across the internet or LAN.
* Windows services
  + File History service makes copies of files to a backup location, enabling users to recover files from accidental loss.
  + Parental Controls service enforces parental control choices for child accounts under Windows.
  + Print Spooler service organizes print jobs and printer management.
  + Sensor Service manages various sensors on mobile devices such as Microsoft Surface Pro for tasks such as device orientation sensors for display auto-rotation.
  + Windows Biometric Service enables applications to capture, compare, manipulate and store biometric data.
  + Windows Error Reporting Service can send error information to Microsoft when programs stop working, as well as produce logs for diagnostic and repair services.
  + Windows Insider Service must be enabled for the computer to use the Windows Insider Program.
  + Windows Mobile Hotspot Service allows a computer to share a cellular data connection with another device.
  + Windows Time Service handles date and time synchronization for all clients and servers in the network.

1. Demonstration
   1. IOS-XE

* For example, IOS-XE typically will have only HTTPS and DHCP ports open. You can verify this with the show ip ports all command, as shown in the example.
* IOS versions prior to IOS-XE use the show control-plane host open-ports command. We mention this command because you may see it on older devices. The output is similar. However, notice that this older router has an insecure HTTP server and Telnet running. Both of these services should be disabled. As shown in the example, disable HTTP with the no ip http server global configuration command. Disable Telnet by specifying only SSH in the line configuration command, transport input ssh.

1. Tips
   1. Scan and analyze your environment.
   2. Verify which services and protocols you need
   3. Disable services and protocols that are not needed
   4. Maintain the same security procedures on services which are planned to be decommissioned, as any other, live services, including penetration testing where appropriate.
   5. Restrict services that are still necessary for some purposes and ensure that those intended for local use only are not made publicly available.
   6. Make a record of any temporary services which you will eventually need to disable.
   7. Perform thoroughly post-decommissioning checks to ensure that the procedure has succeeded. Use systematic tools such as port scanners to do this where possible.
   8. Ensure that any decommissioned hardware is disposed of in a safe, appropriate and compliant manner.

**REFERENCES**

* <https://its.ucsc.edu/security/services.html>
* <https://contenthub.netacad.com/itn-dl/16.4.5>
* <https://www.cert.govt.nz/it-specialists/guides/unused-services-and-protocols/disabling-unnecessary-services-and-protocols/>
* <https://www.stigviewer.com/stig/windows_2008_member_server/2017-03-02/finding/V-3487>
* <https://www.techtarget.com/searchenterprisedesktop/tip/How-to-safely-stop-unnecessary-Windows-10-services>
* <https://docs.oracle.com/en/database/oracle/oracle-database/18/ntqrf/about-disabling-unnecessary-services.html#GUID-3212FA35-10D9-4C19-B002-6F91E75F8790>
* <https://www.getsafeonline.org/business/articles/unnecessary-services/>
* <https://www.giac.org/paper/gcwn/15/disable-nonessential-devices-services-reduce-exposure-dos-attacks/100301>

**CANVA**

<https://www.canva.com/design/DAFS00DsKOo/-ZEGhO8vIfIWWfmFRcjcQw/edit>

**VIDEO**

<https://drive.google.com/drive/folders/1hOSXMNlI5P81tHiumgv3IqgAkVnnlX6J?fbclid=IwAR2EnCbASQIJnj0ibATnPf4mPIwJUzE4K92qiEoLm1z6yXIDASNC2Z1uk0k>