

Checklist of immediate changes:

1. Ensure Sophos End-point Protection Suite is installed on the computer used for payment processing (Virtual Terminal machine) and is pointing UBC IT's Sophos Enterprise Console.
 - a. RDP into Sophos Enterprise Console server (*sophosec1.it.ubc.ca*) to check that the computer has no outstanding alerts/errors and is placed in correct group
 - b. Check **Control Panel > Add/Remove Programs** on the local computer to make sure the full suite is installed (Sophos Anti Virus, AutoUpdate, Client Firewall, Diagnostic Utility, Network Access Control, Remote Management System)
 - c. If the Sophos suite is not installed then
 - i. Download the zip file: http://sophosec1.it.ubc.ca/VTInstaller_fwnc.zip
 - ii. Run the setup.bat and enter your assigned group name (eg "CBM\group")
 - iii. When Sophos is finished installation, reboot the computer.
 - iv. Log onto the Enterprise Console and check the computer is placed in the correct group. If not, it will be put into the "Unassigned" -- you can drag and drop it to the appropriate group.
 - v. open up any departmental firewalls for ports 8192-8194 TCP in and out and limited to sophosec1.it.ubc.ca (137.82.132.14) to help with communication between the Enterprise Console and the VLAN where the computers are.
2. Configure the Sophos firewall settings on the Enterprise Console to ensure that outbound traffic are restricted
 - a. If you are starting from the new default settings, or original default settings, follow the Firewall_Config_New.docx guide.
 - b. If you are starting from your existing custom firewall settings, follow the Firewall_Config_Existing.docx guide.
 - c. All changes MUST be documented and submitted back to UBC IT (sissupport@mail.ubc.ca). Please follow the documentation style at the end of the document.
3. Configure the Sophos Enterprise Console to automatically send email alerts to yourself/support team
 - a. On the Enterprise Console, go to **Tools > Configure Email Alerts**
 - b. Use *smtp.interchange.ubc.ca* for the SMTP server
 - c. Set anything for the sender; set yourself or your support team for the recipient.
 - d. Feel free to tweak the subscription options, but you should be signing up for **Alerts** and **Errors** under **Critical level exceeded**
4. Turn on Windows/Automatic update on the local computer:
 - a. Windows XP:
 - i. Click **Start**, click **Run**, type **sysdm.cpl**, and then press **ENTER**.
 - ii. Select **Automatic Updates** tab and the automatic installation option and click **OK**.
 - b. Windows Vista/7:
 - i. Click **Start**, type **Windows update** in the search box, and then click **Windows Update** in the **Programs** list.
 - ii. In the left pane, click **Change settings**.
 - iii. Select the automatic installation option and select **Give me recommended updates the same way I receive important** updates and click **OK**.
5. Make sure FTP, Telnet, TFTP, and IIS services are disabled or removed on the local computer.
 - a. Windows XP - Check the following:
 1. **Control Panel > Administrative Tools > Services**
 2. **Control Panel > Add/Remove Programs**

3. **Control Panel > Add/Remove Programs > Add/Remove Windows Components**
 - b. Windows Vista/7 - Check the following:
 1. **Control Panel > Administrative Tools > Services**
 2. **Control Panel > Programs >**
 3. **Control Panel > Programs > Turn Windows features on or off**
6. Ensure that the local computer has the latest security patches/upgrades installed.
 - a. Windows XP must have service pack 3 installed.
7. Restrict login onto the local computer to only authorized users as much as possible
 - a. Authorized users should not be using admin accounts
8. Open up departmental firewalls to allow NMC's internal vulnerability scanner
 - a. Nessus scanner-177.net.ubc.ca (142.103.198.177)
9. Disable or set RDP to use secure encryption
 - a. If you do NOT need RDP, then disable it via Control Panel > Systems > Remote tab.
 - b. If you do need it, please follow the instructions on RDP_setup.docx to ensure that the necessary controls are deployed.
10. Uninstall the Sophos suite on any computer that will no longer be used for payment processing
 - a. Disable the tamperproof protection on the local computer. Password is sophosec1
 - b. Uninstall the Sophos applications
 - c. Log onto the Enterprise Console and delete the computer from the group
11. Let UBC IT know when changes are completed
 - a. Send any relevant documentation and IP address of all Virtual Terminal machines to UBC IT (sissupport@mail.ubc.ca)

Required ongoing support for the Virtual Terminal machine

1. Physically inspect the computer and it's immediate environment on a quarterly basis for rogue access points
 - a. Look for suspicious things such as a USB key attached to a printer that is used by the Virtual Terminal machine.
 - b. Maintain a log of the check. Include details such as the person conducting the check, the inspection date, result of the inspection
 - c. You may choose to check for wireless rogue access points if you wish.
2. Security patches/updates must be installed within one month of release by vendor. This applies to all system components and applications
 - a. Automatic windows/Microsoft updates should take care of most things
 - b. Unless there is an automated solution in place for other applications such as Firefox, Adobe Reader, Java, etc., a monthly manual check will be required.
3. Ensure that Sophos email alerts are looked after
 - a. Any data security incident should follow UBC's Incident Response Plan
 - b. Ensure documentation of data security incidents
4. Remediation of issues detected from the internal and/or external vulnerability scans.