How to build and maintain a safe computer for adolescents.

Christmas time was approaching last year and I was thinking of what I could get for my oldest daughter that would be useful. She had asked for a laptop and I was hesitant because at the time she was eight years old. My wife had just upgraded to a new system and I had an extra laptop that could be used. My first thought was to load this up with Linux and lock the system down. But this was not to be as I couldn't get the wireless driver to work (and in hindsight I'm happy about this). I did some research and decided to try a web proxy product coupled with another that would prevent changes to the operating system (OS). The following is the layout and approach I used to secure this laptop.

Target Platform:	Dell Latitude with built-in wireless.	
Software used:		
OS:	Windows XP Professional SP3	http://www.microsoft.com
Applications:	DeepFreeze version 6.41.020.1973	http://www.faronics.com
	Safe Eyes version 6.0.238	http://www.internetsafety.com
	Firefox 3	http://www.mozilla.com/firefox
	Avast AntiVirus (optional)	http://www.avast.com/

DeepFreeze locks the OS down so that any changes made while the system is running is erased every time the system reboots.

Safe Eyes is a proxy service that validates all network connections against a whitelist and blacklist that is maintained online.

Avast AV can be a free antivirus product.

OS Install

If needed reformat the hard drive. The end goal is to split the hard drive into two partitions. One partition for the OS and one for data. I had a 60 GB hard drive, so I opted to split it evenly. For those with really big hard drives, I would say anything over 120 GB, I would allocate 60 GB for the OS and put the rest to use as the data drive. Once that is done, install the OS. I used C: for my OS and D: for my data drive. Connect to the vendor's site and install all of their latest patches. If you require any drivers, e.g. video card, network, now is the time to make sure they are the latest revisions. It's also a good time to verify they work in the expected configuration.

The choice of OS. Safe Eyes works on Macintosh and Windows. I stated earlier that I was happy I ended with Windows. My reasoning for this is that I trust the Safe Eyes product. If I had ended with a Linux based system, I believe it would have been much harder to get the system to the same state that I have it now. I'm sure I could have put Dan's Guardian and squid on the local system and proxied all traffic through this software. However, even though this is free software, the amount of time to configure and test this approach would have rolled me into probably 20-30 hours. As it stands, I spent a little over 10 hours building and testing this system.

AntiVirus

Because I'm using DeepFreeze to lock down the OS, I have been having a debate for over two years with a few colleagues whether or not it is necessary to use an antivirus (AV) product. On one hand, the AV should update once a day with the latest signatures, hopefully preventing new viruses from exploiting vulnerabilities on the system. Now from the devil's advocate in me. If the system is patched regularly, there should be less risk to exploits (except for zero day exploits). On top of that, the system is an ideal candidate to be shutdown daily and only brought online when needed to play a quick game or do research for a project/paper. I'll let the reader decide if he/she needs to have AV on the system. I originally configured the system with Avast Free Antivirus. After several months, I decided to take it off and haven't had a problem with the system up to the point of writing this article. If you have a fast enough system, it certainly won't hurt anything to have AV on the system. Make sure you configure the product to retrieve updates either hourly or at regular intervals. When the system reboots it will always go back to the baseline image locked down by DeepFreeze. This means that when you reboot, the AV product will have to download the latest AV signatures again. A colleague read this and reminded me that teens are probably going to be going to Facebook, Twitter and MySpace and that the system would be safer with a good AV product. If your users are teens, then yes, I would want to have a good AV.

Web Browser

You can use any web browser you choose. I'm a proponent for Firefox, appreciating the speed and flexibility of the product. Once installed, perform a Google search for "optimizing firefox" and perform the configuration changes to about:config to each account that will be using the system (http://hubpages.com/hub/Optimizing-Firefox-3-Hacks-And-Tweaks).

DeepFreeze

I'm not putting screen shots into this article at this time because the products explain what they are doing. Go ahead and install DeepFreeze. At one point in the install, the installer will ask you what you want to protect. I chose to protect the C: drive and leave the D: drive alone. I did this because I want documents, pictures, and music stored on the D: drive, while the C: drive is reset to the baseline image after every reboot. After installing the product and rebooting, you will need to Thaw the OS. Hold the shift key and double click on the DeepFreeze icon in the lower right tool bar. This will bring up a password prompt, enter your password and choose to Thaw the OS and reboot the system.

Safe Eyes

Safe Eyes has a very good installer. Follow the prompts and setup with the defaults. I would recommend going to their site afterwards, logging in and setting the levels you feel comfortable with for your children to access the internet. I chose to block everything and only allow my daughter to go to predefined sites that I have checked and am comfortable with her viewing if I'm not around. On the website, setup the child's account. I set my children's accounts to block all websites and then added sites I trust to the Allowed Sites. I blocked all YouTube videos. Music is restricted at this point. Instant Messages are a no go. Games I allowed so that they can get on sites like clubpenguin.com and webkinz.com. Social Networking is setup to block information about where we live, phone number, and her school name. Email is blocked at this point because I don't want her emailing. The Internet Access Schedule is set from 4-8 PM weekdays and then 7AM-8PM weekends. You can also send alerts via email or text messaging to yourself.

Final Lockdown

Before locking the system down with DeepFreeze, it is highly recommended to test each child's user account and their web access limits. I performed both positive and negative test cases to make sure that the controls worked the way I defined them. The cool thing about Safe Eyes is that it checks each network session with the controls on their web site. So future modifications to rules will be stored on their site and download each time the system tries to communicate out. You will not have to Thaw and Freeze the OS over and over again when adding new sites for your child/children. Once you have tested and feel comfortable with the OS and the configuration, it is time to lock it down. Hold the shift key and double click on the DeepFreeze icon in the lower right tool bar. This will bring up a password prompt, enter your password and choose to Freeze the OS and reboot the system.

Maintenance

It is recommended that you update the OS and application patches at least once a month. To do this, you will need to Thaw the OS, install all patches and reboot as many times as necessary to insure that those patches are fully loaded. Update all applications as needed. When finished, Freeze the OS and reboot the system.

Conclusion

If you have followed the steps in this paper, you should have successfully deployed a secure environment for adolescents to utilize (trusted) online sites and prevent them from viewing questionable material. The OS will be reset back to the baseline every reboot; you won't have to worry about little Johnny or Susie deleting or modifying a critical file on the system. I stated that AV is a personal choice; you will have to make the decision if you wish to install this software. Safe Eyes is a solid product that does what it says. I've found that maintenance of the entire platform takes about 15-20 minutes a month. Cost – DeepFreeze was $45 and Safe Eyes was $50 (annual fee). I already owned the license for Windows XP, so no additional cost there. For $95 I am extremely happy with this setup and the minimal amount of time and effort I have to put into it for maintenance. My daughter is happy with the system and her friends are jealous that she has a laptop and internet access.

Contact and disclaimer information

Securityhardening.com provides ideas, concepts and patterns regarding computer security. This site and its content are intended as a way to share these thoughts with the security community. Any questions, comments, or complaints can be directed to the contact address on the support page. Anyone considering implementing any recommendation published on Securityhardening.com (in any form) should read the Disclaimer page.

-- Secure the system ... live life!

Copyright © 2010 securityhardening.com. All rights reserved.