

Re: Is complete home security possible?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2005-02/0319.html>

From: Charles Newman (*charlesnewman1_at_comcast.net.spammers.will.be.shot.on.sight*)

Date: 02/08/05

Date: Mon, 7 Feb 2005 15:06:17 -0800

X-No-Archive: Yes

"Leythos" <void@nowhere.lan> wrote in message
news:pan.2005.02.06.13.33.27.389552@nowhere.lan...

> On Sat, 05 Feb 2005 23:17:26 -0800, Charles Newman wrote:

>> *If you are a gamer, some computer games will only run in
>> administrator
>> mode. Flight Simulator does this I know. If I log in under anything other
>> than an administrator level account, I will an error message on FS98,
>> FS2002, and FS2004, saying that I need to be an administrator to
>> use the program, and I have heard of a lot of other games having this
>> problem.*

>
> *Then you still need to ONLY run as administrator to do the tasks that
> require administrator access – if playing your game, don't browse the web,
> don't get email, don't do anything buy play the game, then switch back to
> a User account when done. Trust me, even if you don't like it, this one
> thing will prevent a LOT of issues.*

Just one problem, FS2002 and 2004 have to go to the Web to
download the latest worldwide weather (FS2004 does this
every 15 minutes). There are a couple of other weather programs
for FS98, and later, which update every 30 minutes. So, playing
with Flight Simulator, if I want the latest real world weather, it
has to go to the Web. At least FSMetar does not require
Internet Explorer to work.

>
>>> *10) Monitor the in/outbound logs from your NAT router – this will tell
>>> you
>>> what's going on with the public network connection. If you get a linksys
>>> router you can download WallWatcher for free and it's very clear as to
>>> what's happening with your Internet connection.*
>>>
>>> *11) If you're machine is compromised, get a router with NAT, get behind
>>> it, and then wipe/reinstall your system – while you're get people
>>> telling*

comp.security.firewalls: Re: Is complete home security possible?

>>> *you that you don't have to go to that extreme, do you know of any way*
>>> *YOU*
>>> *can be sure that you have a clean machine? I've never signed a document*
>>> *saying a compromised system was clean unless I wipe/reinstall it, and I*
>>> *won't either.*
>>
>> *No argument there. I have a clean disk image made from Norton Ghost,*
>> *and I regularly ghost my machines once a month. You should regularly ghost*
>> *your machines once a month.*
>
> *I've used Ghost since it was owned by BinaryResearch (5.0) and I would*
> *never ghost once a month – there are too many updates and patches and*
> *security issues to deal with to do it monthly, and on a properly*
> *configured system once a year is too much (unless it's a heavy development*
> *system).*
>
>> *In another newsgroup, one guy called my crazy for regularly ghosting*
>> *my machines to get rid of any malware, but it is the only way to be sure*
>> *nothing bad is lurking inside your machine. Where I went to college, they*
>
> *If you don't do any serious work with your computer then re-imaging it*
> *would not really be an issue, but you're failing to address the real issue*
> *– security. Re-Imaging is not addressing the issue of security. If you*
> *were to take the amount of time you invest into imaging, updates, patches,*
> *reinstalling apps, you could easily protect the machine from malware and*
> *not have to waste so much time.*

Well, I keep important files on a second hard disk in the NAT Box, so losing files when ghosting the machine is not much of an issue. I have two very high capacity hard disks (over 100GB), and I use one to periodically back up files on the second hard disk. If you use Ghost, you also need a >100MB hard disk to store the Ghost images.

>
>> *had a program they ran daily before closing the labs for the night*
>> *which restored the machines to a specific configuration and got rid of*
>> *any software that any students may have installed during the day, as*
>> *well as any viruses and the like that may have come in.*
>
> *Completely different scenario – we always reimage training center machines*
> *before each class – it only takes about 15 minutes and ensures that the*
> *student has a clean and working machine. This is not the same as you,*
> *being the only user, re-imaging your machine because you've not taken the*
> *time to learn about securing it.*

Where I went to college used a program similar to the much-touted Evidence Eliminator, only much more sophisticated. This program did two things. It zeroed the disk and restored the desired configuration. People like ejfudd820 may tout Evidence Eliminator, and you have to admit that it is good at

Re: Is complete home security possible?

comp.security.firewalls: Re: Is complete home security possible?

what it does, but the program they used in the labs would blow EE away. They used this to keep the University, and any of its administration out

of trouble, if any student/staff/faculty ever did something illegal. The primary worry was software piracy. The program would first erase any file not in the list of files to keep and then it would zero the disk space as it went. Web cache, internet history, unauthorized software installations, etc, etc, we would be erased and zeroed, and then files they wanted on there restored. The software they used did keep the university out of hot water a few times. I did hear of investigators investigating for software piracy, but they were unable to recover anything from the hard disks. It also kept the university out of hot water once when one of the counselors was arrested for downloading child porn. Because this program wiped and restored the hard disk on his office computer regularly, the authorities were unable to recover any evidence against the university, so the university avoided any criminal or civil liability, though the last I heard the counselor was doing hard time for downloading child porn. The counselor got into trouble, but the university was kept out of hot water because of the program they used to regularly wipe and restore disks on their network. The only evidence was from the person's home computer, so he was the only one that got into trouble, and the university got off scott free. .