

Re: New install of winxp home.....

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-11/0749.html>

From: Stefan Kanthak (*postmaster_at_[127.0.0.1]*)

Date: 11/26/05

Date: Sat, 26 Nov 2005 21:27:24 +0100

"TAJ Simmons" <awesomebackgrounds@NOMORESPAM.nothing> wrote:

Your from is invalid! Use an existing address!
And top posting is nasty.

> *get hold of a CD of SP2 (service pack 2)*

Nothing more?

> *install a firewall (like zone alarm)*

A truly BAD advice: Zone Alarm and other so called Personal or Desktop Firewalls make Windows vulnerable again and don't work as advertised: due to errors in the products themselves and their use within critical code paths the attack surface is increased, they don't block malware from opening outbound connections, ask questions regarding outbound connections which Joe Average is unable to comprehend and thus can't answer correct, they disturb the user with superfluous popups of blocked inbound "attacks", are susceptible to privilege elevation with shatter attacks and some of them even open ports on the external interface(s).

The "Windows Firewall" performs well, doesn't add code to critical paths, doesn't cry "wulf" at every blocked inbound packet, has none of the other flaws and is automatically activated after installation of SP2!

> *"jim2" <jim2@discussions.microsoft.com> wrote in message*
> *news:CFF48023-DDFD-4ECB-91F1-2CAE681D3524@microsoft.com...*
> *> what patches should i install before i connect to the internet, if any at*
> *> all.*
> *> i would like to get most the updates as iso, any links to some infor would*
> *> be great.*

Download the SP2 and all subsequent patches on another already secured PC or order the SP2 CD from Microsoft; the latter does NOT contain the subsequent patches. These are (ordered by MSKB article number):

KB873339 (MS04-043), KB885250 (MS05-011), KB885835 (MS04-044),
KB885836 (MS04-041), KB887472 (MS05-009), KB888113 (MS05-015),

microsoft.public.security: Re: New install of winxp home.....

KB888302 (MS05-007), KB890046 (MS05-032), KB890859 (MS05-018),
KB891781 (MS05-013), KB893066 (MS05-019), KB893756 (MS05-040),
KB896358 (MS05-026), KB896422 (MS05-027), KB896423 (MS05-043),
KB896424 (MS05-053), KB896428 (MS05-033), KB896688 (MS05-052),
KB899587 (MS05-042), KB899589 (MS05-046), KB899591 (MS05-041),
KB900725 (MS05-049), KB901017 (MS05-048), KB901214 (MS05-036),
KB902400 (MS05-051), KB904706 (MS05-050), KB905414 (MS05-045),
KB905749 (MS05-047)

You should get the following hotfixes too:

KB885884, KB885894, KB886610, KB887742, KB887797, KB889527, KB892313,
KB893357, KB897663, KB898461, KB900930, KB904412, KB906569, KB907865

Install SP2 and all the patches,

– OR –

build a so called slipstream installation CD with SP2 and the patches
integrated (see MSKB 828930, 814847 and 296723, but 249149):

- copy your XP CD into an empty folder of your hard disk;
- run WindowsXP-KB835935-SP2-ENU.EXE /integrate:<path_to_folder>;
- run each of the patches .EXE with parameter /integrate:<path_to_folder>;
- search Google for how to burn a slipstream CD with your CD burning tool;
- reinstall XP.

Setup a NON-privileged (normal) user account for ALL of your everyday work.
Use your administrator account only for administration (hence it's name).

Turn on "Software Restriction Policies", remove .LNK from the list of
executable extensions (else all the shortcuts from the start menu, "SendTo"
and other places won't work) and allow execution of files only from
%SystemRoot% and below and %ProgramFiles% and below.

You won't need anti-virus software then (which almost always ain't uptodate
on Joe Average's PC)!

Turn on "Automatic Updates" and create the following registry key to be
informed of new updates when working with your non-privileged account:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\WindowsUpdate]  
"ElevateNonAdmins"=dword:00000001
```

If you are going to use Internet Explorer and Outlook Express (or Outlook):
at least turn off "Active Scripting" in the "Internet Zone" (and define
*.microsoft.com as "Trusted Sites", else you wont be able to use "Windows
Update" in Internet Explorer); unfortunately there is no means to disable
ActiveX (the most prominent attack vector) alone.

Configure Outlook Express not to use IE's HTML rendering engine, but show
all messages in plain text. You can get a .REG which will preconfigure
OLEXP from <http://home.arcor.de/skanthak/presetoe.html>; import this .REG
(with administrative rights) before you start OLEXP the first time.

microsoft.public.security: Re: New install of winxp home.....

Additionally consider to configure the proxy 127.0.0.1:9 except for *.microsoft.com in the Internet Explorer settings (at least for the administrative accounts), which will block access to all sites but *.microsoft.com.

If you're going to use Mozilla, Firefox and Thunderbird or Opera: these too have security bugs, but no ActiveX, and you'll need to update them regularly.

Visit (and read) <http://www.ntsvcfg.de/> if you wan't to harden the system further; <http://home.arcor.de/skanthak/harden.html> was written for Windows 2000, but can be adapted for XP.

Stefan

[

--

Writing on top because that's where the cursor happens to be is like shitting in your pants because that's where your asshole happens to be.