

Securing your Data

Some time ago computers were generally unprotected, attacks of any type were rare and the most likely compromise was from a boot sector virus on an infected floppy disk. By the late 90s there was a small chance of virus attack via email or Trojan programs in downloads and most people needed an antivirus program if they used the Internet for Email. Early 00s were the territory of the new mass mailing email borne viruses/worms and the start of the script kiddies and remote access Trojan explosion. Everyone needed Antivirus software and most people needed a firewall. Now it is the mid 00s and we are at the point of Spyware madness, everyone that uses Internet Explorer needs an anti-Spyware program or two, everyone needs a firewall, everyone needs anti-virus and anti-Trojan software and although they don't know it yet everyone needs an IDS of some sort.

Along with the Spyware come the diallers, some of which dial premium rate lines that can be any cost – the worst I have seen is a dialler which connects to a line in Germany with a **£99 per minute** rate, don't forget that a 1 second connection incurs the 1 minute charge so potentially your PC could spend £1000 in a minute for you without you even knowing. Ant-Spyware and Anti-Trojan software all of a sudden doesn't seem so expensive does it?

If you have all of that as well as a kernel level system guard you are state of the art and well protected. It won't stop you being attacked and it probably won't stop you getting compromised by a superior attack – but it's all you can do. I have lost count of the number of people that I have seen that **can't** have been infected/hacked/rooted (rooted – taken control of, derived from the Unix super user **root**) because of their protection but there it is in front of them. Most security tools rely on signatures to detect malware (hostile coding – a program that is written with bad intentions) which gives them one big, large, ultra-monstrous, mahooooosive flaw – it's so huge it should be funny – new code goes straight through *whoosh*, unhindered in any way and you are w00Ted. Hence the need for an IDS (Intrusion Detection System) – it won't necessarily stop it but it should let you know something has gone awry and give you a chance to respond before the battle is lost.

People seem to be unaware of root kits at the moment as well, never heard of them and can't comprehend what it means. A root kit is a system which hides itself when installed – it is low level and intercepts calls to the file system etc... so that AV scanners and the like cannot detect it. If you look for it from explorer you won't find it – it will intercept the access and return false information to the system, once it is there you cannot find it because it is in control of the things you will use to detect it – bummer! To detect a root kit you must boot from a different system and scan your disk with it, even then they can be hard to find if they use encryption, exe-packers or the like and don't use standard registry keys.

At this point I think it's a good time to tell everyone reading this about the only way they can really **protect** themselves – stressing that there is **only** one way. Everyone knows what it is but very few people actually do it, even large companies ignore it on occasion. One large computer security company were recently caught out without it much to their embarrassment and consequent loss of business. Backups. Consider the impact of losing all your data right now – incidentally this is

most likely to happen due to hard disk failure not hackers/viruses or whatever. If the thought of losing all your data has filled you with trepidation – that's good, feel the terror and don't just sit on your arse - do something about it. Don't put it off until tomorrow because tomorrow never comes.

Data security comes down to cost (doesn't everything). If your data is worth little then don't spend a fortune protecting it, take a realistic view of what it is worth. With large hard drives costing only £80 nearly everyone can afford to have a spare drive in a removable tray or external housing to accommodate their backups. For bigger budgets any or all of a dedicated backup system with special tape drives, offsite data storage people and RAID implementations should be considered. If the cost of losing your data would exceed the £40-80 for a second drive then get down the shop now and buy a drive – you will be soooo glad you did when the first drive eventually packs up - and they all do.

:Recommendations for home users:

1. Use a good antivirus and keep it up to date

Norton Antivirus, Panda Antivirus, Kaspersky, McAfee, Nod32, F-Prot, Avast!, E-trust Antivirus and many others are out there and are good tools just pick one that has a long standing reputation in the field and it will likely be good. Personally I use F-Prot, Norton, E-Trust, Panda, Antivir, Kaspersky, AVG and Avast! On various systems and would recommend them all.

2. Use Windows XP built in firewall

Firewalls require a certain amount of knowledge to use correctly or they become worse than useless. For those that don't have the knowledge alerts popping up all the time are just stupid and the Windows XP built-in firewall is the best, it is even better in SP-2. Non Windows XP users should check out Sygate Personal Firewall and if you are prepared to pay for your protection then get Black Ice PC Protection it is and always has been the best. Only GRC regulars could doubt this – what's that saying now something about the blind leading the blind. If you have a DSL/cable connection use a router instead of a modem because it will have a built in firewall that will protect your LAN side without the need for a software firewall on the PCs this is a much better arrangement and the cost difference is negligible.

3. Use an alternative browser for general web surfing

There is no getting around it Internet Explorer is as solid as Swiss cheese and the whole world knows it. It may be the best browser out there but it has more holes than a fishing net and even at the latest patch level I believe there are still more than 18 outstanding vulnerabilities that MS has yet to get around to looking at. Don't use something like Crazy Browser or MyIE2 as they are Internet Explorer add-ons and therefore contain the same vulnerabilities. Using Mozilla FireFox or Opera will save you from a lot of browser hijacking and drive-by downloads which in turn will protect your PC from Spyware at the commonest entry level. Both also include pop-up blocking capabilities – FireFox is even free. These alternatives are not perfect either so check for patches occasionally but they have a far lower risk profile. Some sites will need IE or they won't function, only use them if you know they are safe to use!

4. Remove the MS Java Virtual Machine

Microsoft's dodgy implementation of Java has been the route of entry for many a

piece of malware, be rid of it by downloading Microsoft's own JVM removal tool 'unmsjvm.exe' which is available from Microsoft.com and many other websites. If you really like all that java stuff or you need it (some OL Banking software and various proprietary tools require it) you can download and install the real java from Sun Microsystems (<http://java.com/en/download/manual.jsp>). Incidentally Flash animations also have a lot of scope to do damage due to various bits that can be embedded into Flash movies, some sites are starting to recommend disabling Flash already. Adobe PDF files are also incorporating features that can be misused now – the landscape is ever changing.

5. Keep to the latest patch level

Although keeping your OS updated to the latest patch level won't mean you are bullet-proof it will mean that you are harder to attack than you might be and thus limit your 'vulnerability profile' – for dial-up users this might mean a lot of time downloading. Most people should just turn on the auto-updates feature that is a part of the operating system (Windows XP,2000, SuSE Linux). It is also worth occasionally manually checking via the Windows Update portal (if you are a windows user) – you must use IE to do this – at <http://windowsupdate.Microsoft.com>.

6. Use Anti-Spyware

SpywareGuard, Spybot Search and Destroy, IESpyAd, SpywareBlaster and Ad-aware are all free to use in some way or other and will keep 99% of Spyware out of your PC. Spyware is a bit misleading, nowadays a lot of this stuff is no holds barred malware designed to exploit you or your system for direct profit or criminal gain. Later variants of some parasitic spywares actually install hacker tools like the rootkit 'Hacker Defender' to facilitate hiding themselves. If you get exploited by something like that you are in a whole heap of trouble – better to prevent it ever happening. IE-Spyad will add all the known dodgy download sites to your 'Restricted Sites' zone in Internet Explorer and on it's own stop 90% of infections. SpywareBlaster and SpywareGuard will prevent any others that get through from installing – or at least alert you that something is going on. Ad-aware and Spybot S&D can be used to periodically scan your system in case any nasties did get through. Incidentally if you want to fork out a few quid Webroot's 'Spy Sweeper' combined with IE-Spyad will keep you pretty safely locked down.

7. Back Up your stuff

Ideally you will be using something like Acronis TrueImage, Symantec V2i Protector or Norton Ghost to make images of your hard drives as well as making rolling backups of the system state data with NT Backup and storing it offsite but that is a cost decision.

8. Use Microsoft's Baseline Security Analyzer

Microsoft provide a tool called the Baseline Security Analyzer which you can run on your system (2000 or XP) and it will identify common security mis-configuration and check your patch levels. It also checks for IIS and SQL issues and gives you instructions on what to do – even for using things like the IISLockdown tool and URLScan. In advanced use you can use it to scan a network for vulnerable machines.

9. Banish the Preview Pane

Email clients Outlook and Outlook Express use the inbuilt Internet Explorer as part of their interface and so are vulnerable to many if not all of the same exploits that

have been discovered in IE. With the preview pane enabled in either of these clients (or any built on them) your system can be compromised without you even opening the email – turn off the preview pane so you have a chance of filtering your mail first. In fact lots of software uses IE – like Microsoft Works, Quickbooks, Microsoft Office – too many to mention. This in itself is another good reason to install IE-Spyad which will restrict the actions of any known offending sites that may spam you through any of those routes. For email you can go further by turning off HTML mail or changing to alternative email clients like Eudora, Thunderbird or Pegasus Mail but of course you will want to check that the feature sets meet your requirements first.

10. Disable unnecessary services

Every service that your system runs is a possible point of entry or compromise, you should only run the necessary services. Services like the Messenger and Alerter services, FTP server, IIS and many others must be carefully considered before you allow them to run on your system. A good guide to service configuration can be found at <http://www.blackviper.com/WinXP/servicecfg.htm> with some additional tools and references.

Consider this a starting point

Don't think you are done when you get to this point, the landscape changes every day in computing. You need to be alert to issues and try to understand them if you want to have any chance of avoiding disaster. This is just a set of instructions – a shopping list if you like – it only informs you of today's best practice, tomorrow is another day. Incidentally if you are a MAC user it's not because you are any safer that I haven't mentioned you (you aren't) it's because there are so few of you it's not worth the effort.

Your data is the most valuable thing in your PC, hardware is easy to replace, software can be re-installed but if you lose your finance data, your digital video, your digital images, logos, documents etc...etc.. you need more than a few quid to get it back – if you can at all. Backup your data – then backup your backups!

After all that time and effort you are now a lot harder to crack from an automated or novice standpoint, you are no longer 'low hanging fruit'. You can go further and implement an IDS, a proxy server, disable Active-X Java and scripting languages, use DNSKong, implement Local or Group Policies and use back to back firewalling. A bit like Shrek (and onions) security is made up of layers.

Steven Lea I.T.