

Windows 2000 - Living in the new (Security) Millennium

Hal Flynn 2000-01-25

The end is drawing near for Windows NT. Microsoft is pushing to release Windows 2000 on February 17, 2000. As we get closer to this proposed shipping date, an increasing number of companies will find themselves facing the problems of fitting Windows 2000 into their environments. With the massive Year2000 initiatives out of the way, and the Euro behind us, this should be a snap. It's just another upgrade from Microsoft that needs to be installed. Or is it?

Don't let the name "Windows" fool you into thinking it's just another upgrade of NT. Microsoft is making many strides in the area of Information Security for Windows 2000. Single sign on, Active Directory, PKI, Secure IP, Smart Cards and the MMC Security "Snap-In", just to name a few. Windows 2000 may look the same on the outside, but it's a completely different animal on the inside. In fact, one might argue that in the area of security- the word Windows is the only thing that is the same about Windows NT and Windows 2000.

Most companies, under normal circumstances, would have had full Windows 2000 test labs set up months ago. Quality Assurance departments, user support, system administration, network engineers and of course- security staff all would have been assessing their portions of the new operating system to make sure it fits into the environment. Unfortunately, because of Y2K this has not happened. So much time and effort was put into making sure everything was Y2K ready, that there was no time left over to test Windows 2000.

Instead of a huge company-wide Windows 2000 initiative, it has been a few people that have installed Windows 2000 on their desktops and perhaps a laptop or home PC to fiddle around with it. There is no true standardized testing that has been done by IT staff. No documentation of features, no testing of applications and business processes.

Management is pushing for Windows 2000 because it will help increase the bottom line. New features, increased user productivity, extended software availability, and lower cost of ownership are just a few of the promises that Microsoft is pushing onto the desks of our executives. To complicate matters, business partners are already developing software solutions that will run on Windows 2000.

With most of the security problems that NT brought us fixed and out of the way with Windows

2000, management can see no other path for the organization than to upgrade from NT to 2000. With six service packs and countless hot-fixes since WindowsNT4 was released, management just wants to put the security holes and risks of NT behind them and move onto a clean new version where everything has been taken care of for them already.

It is easy for management to look at this scenario and decide that Windows NT must go, and Windows 2000 must be brought in. However, from a technical point of view; the perspective is quite different. What management may not see, is that Windows 2000 will bring it's own suite of security issues. For every 'hole' that Microsoft fixed in Windows NT, will there be another one to fix in Windows 2000?

Time and time again, the introduction of a new OS (or major version upgrade, such as Windows 2000) has burned security professionals. For one reason or another, management's time frame for roll out is always about 10% of the time actually needed to adequately test and secure the OS in the environment. Being creatures of coffee and little sleep, we always seem to succumb to the task at hand and make things happen in the time allotted. We take our knowledge of the product, and our knowledge of security, and build a solution.

With so much time and effort being spent in the past year on Year 2000 projects, there has been little or no time on the security professionals' calendar to test Windows 2000. Who is going to port the NT policies to Windows 2000? Will Windows 2000 be forced into production before the security engineers give it the thumbs up? Hopefully not.

At this point in the game, many of us have installed Intrusion Detection Systems (IDS), or vulnerability scanners for our systems and networks. Most of us have also installed custom security policies on our servers and workstations so that our written policies and procedures can be enforced automatically. Our log files and events are managed from a single location. Security anomalies are logged and pager and console messages alert your staff. For those of us who have not quite made it to these levels (and there are quite a few), there are "general practice" security procedures which you follow. Either manually or in a custom automated fashion, you check logs, permissions and settings to maintain the overall security health of your systems and network.

This all changes with Windows 2000.

Your current security software (IDS, vulnerability scanners, policies, log analyzers, etc..) 1)

have not been ported by the vendors to run on Windows 2000. 2) Do not recognize known vulnerabilities in Windows 2000 (due to the fact that there is not enough widespread use and testing to compile a vulnerability database).

IT security staff and IT administration staff has little or no knowledge of Windows 2000. The security policies that have been written for Windows NT 4.0 are not "portable" to Windows 2000. Too much has changed with regards to authentication, and file systems for NT security policies to work without modification in Windows 2000. Staff needs to be brought up to speed on the OS as a whole first, and then retrained on their individual specialties in order to maintain effective security.

Much of the 3rd party software that you are using to do everything from PKI to Smart Cards to VPN is already bundled with the operating system in Windows 2000. How will your current software fit on top of that? Will the built-in VPN disable the 3rd party solution that you have already purchased?

Remember when everyone ran Netscape until "Active Desktop" seemed to push Internet Explorer into our face every time we wanted to surf the web? Are your existing security software investments preserved moving into Windows 2000? For the most part, the answer seems to be no. With the majority of companies using 3rd party software to secure their networks, the fact that they now have to upgrade the security infrastructure can be a major issue. The benefits of things like single sign on, and native kerberos support far outweigh the perceived loss of time and investment in the move from NT to Windows 2000.

Somewhere along the lines, there seems to be a strong communications problem between Microsoft and 3rd party vendors. Everyone from Axent to Entrust to ISS is lagging behind when it comes to support for Windows 2000 in their security software. ISS product managers have stated that their products will both run on, and scan against Windows 2000 machines once Microsoft officially releases it. ISS customers will have to first test the new versions, then hope that there are no bugs and quickly slip it into production so that they are not exposed to potential Windows 2000 risks that may arise.

On the other hand, nearly all major (non-security) 3rd party software vendors are either currently or very near to shipping a Windows 2000 ready version of their software. Whatever the reason, it leaves security professionals with a serious dilemma. Do you push back the production rollout of Windows 2000 on your network until you are 100% prepared to make it,

and keep it secure? Or do you allow the system administrators to roll out Windows 2000 in order to keep management happy.

Without the proper tools to audit the operating system, check for vulnerabilities and enforce policies, the operating system is bound to raise havoc among many a network. What is the company's policy for authenticating older clients that do not support kerberos or encrypted transmission of passwords? Will the domain structure be revamped to integrate with Active Directory? How will this affect your security?

From a high level, your organization should have security policies that keep you prepared for whatever OS or application comes along. The truth of the matter is that many companies have security policies that are very specific to operating systems and applications, which makes it difficult to bring in something new. If we compare security policies to the Constitution, things can become much clearer. Instead of saying, "In Windows NT 4.0, file access auditing will be checked in the properties box of the logging dialog", you might say "File access logging will be enabled on the operating system level of all production systems". It's easy to see why the second example accomplishes the same thing in the end, but provides for much more portability of your policies as technology evolves.

This brings us to another point. Microsoft has come a long way with regards to user education in recent years. Full blown certification paths, online seminars, training partners and Microsoft Press books, just to name a few. While taking a look at their current Windows 2000 offerings (http://www.microsoft.com/train_cert/learncenter/win2000/default.asp), it was ironic to see that their only instructor led security course was "Securing Microsoft Windows NT Server". The course description did not even mention Windows 2000.

We were able to find an online course on Microsoft's web site (self-based training) that discussed smart cards, active directory and terminal server security in Windows 2000. In my opinion, it's more of a sales presentation with pretty slides and sounds than a security training course with good, technical information. A quick scan of Amazon (www.amazon.com) for Windows 2000 security books turned up one book by Syngress Media called "Configuring Windows 2000 Server Security". Although the notes for this book said it would be available in November 1999, our only option to purchase was pre-order which usually means it has not been published yet.

In our searches for Windows 2000 security information online, we turned up only a few results

of substance (they are included below for your reference). We even went as far as to check some of the Microsoft Training Partners, and none of them had Windows 2000 security courses yet.

Before Windows 2000 is put into our environments, the stated education for IT security staff needs to happen. In addition, the underlying security infrastructures need to be made increasingly more solid in order to preserve baseline security, regardless of which OS is installed on the network.

The following Windows 2000 security resources are currently available at the time of writing this article:

Microsoft has quite a few security-related presentations and white papers available on their web site:

<http://www.microsoft.com/windows2000/library/technologies/security/default.asp>

Microsoft also has several step-by-step guides on various security features of Windows 2000:

<http://www.microsoft.com/windows2000/library/planning/default.asp>

Aelita has a good presentation from Comdex about migrating from Windows NT to Windows 2000:

<http://www.aelita.net/Support/Library.htm>

This looks to be a good book about Windows 2000 Security:

<http://www.amazon.com/exec/obidos/ASIN/0789719991/securityfocus>

A TechNet article that discusses secure networking using Windows 2000 Distributed Security Services:

<http://www.microsoft.com/technet/win2000/win2ksrv/technote/disesewp.asp>

Another TechNet article that talks about the default ACL settings in Windows 2000:

<http://www.microsoft.com/technet/win2000/win2ksrv/technote/secdefs.asp>

Here is Tucows' listing of Windows 2000 Security Shareware:

<http://tucows.mirror.ac.uk/win2k/security2k.html>

Relevant Links

[Microsoft Windows 2000 Security Page](#)

by Microsoft [Subscribe to the Microsoft Security Notification Service](#) *by Microsoft* [Microsoft Security Advisories](#)

by Microsoft [Windows 2000 Security Handbook](#)

by Jeff Schmidt

[Privacy Statement](#)

Copyright 2006, SecurityFocus