

INFORMATION SECURITY MATTERS

August 2004
Volume 1, Issue 1

Cedric Bennett & Associates ◦ ced@bennettsite.com ◦ 650 858-0883 ◦ <http://bennettsite.com/cba>



Time-To-Exploit Is Rapidly Approaching Zero

The “SQL Slammer” worm suddenly attacked computers running Microsoft SQL Server™ in January of 2003, six months after the specific vulnerability and patch had been announced and made available by Microsoft. Eight months later, “Blaster” and nearly a dozen similar exploits attacked Microsoft Windows™ systems, this time only two weeks after the announcement of the vulnerability and availability of a corrective patch.

This time interval, between the widespread announcement of a vulnerability along with the appropriate corrective action and the appearance of exploits that take advantage of that vulnerability, is called “time-to-exploit.” Experts and pundits debate the reasons why time-to-exploit is growing shorter, who might be to blame, and so on. The important point for information security professionals is simply the fact that it is true. And shorter time-to-exploit means that there is less time available to take effective corrective action.

Here are several defensive approaches available to information security officers — unfortunately, none

Improve Security with Windows XP™ SP2 — Carefully

The long anticipated release of Microsoft’s major update to Windows XP™ called Service Pack 2 (SP2) is becoming available in August, even through Microsoft’s Windows Update Service™ later in the month. Service packs are normally used as a way to both consolidate an array of previously released corrections into a single product upgrade as well as

Inside This Issue

Time-To-Exploit Is Rapidly Approaching Zero	1
Improve Security with Windows XP™ SP2 — Carefully	1
Why This Newsletter?	2

of them are 'slam-dunk' easy to implement. One is to apply policies, processes, and technology designed to prevent exploits from reaching targeted systems (e.g., firewalls, anti-virus software, and configuration management). Another is to implement automated processes that can support the very rapid deployment of corrective patches once they are made available (e.g., patch management software). Network access management can be used to validate the identity of those attempting to enter the network, ensure that the machine is ‘clean,’ and route them accordingly thus reducing the number of infection-carrying systems coming onto the local network.

Please see *Time-To-Exploit* on page 2

“When time-to-exploit was much longer... the cost of repair was... lower than the cost of prevention.”

provide additional updates. In some cases they are additionally used to deploy new features and functionality. Service Pack 2 departs from that approach; it is a major upgrade release of XP focused on improving Windows security.

Of course, this is a very good thing!

Please see *Service Pack 2* on page 2

Time-To-Exploit from page 1

Since some exploits are still likely to be successful at compromising some systems, the deployment of software that can detect and signal unauthorized changes as well as running regularly scheduled backups can greatly reduce the cost and time burden of repairing damaged systems.

When time-to-exploit was much longer than it is today (months instead of weeks, days, and hours), the cost of repair was generally lower than the cost of prevention. Today that balance has shifted dramatically — the cost of prevention is much lower than the cost of repair (primarily because the cost of repair is rising).

That old adage encouraging ‘an ounce of prevention’ definitely pays off in the practice of information security. ♥

Service Pack 2 from page 1

Although the original version of XP was a significant security improvement over previous versions of Windows, it became obvious that it still contained a significant number of weaknesses and vulnerabilities. SP2 not only addresses many of those issues but actually redesigns and re-architects major portions of Windows. This is being done in an effort to not only repair and prevent vulnerabilities but also to reduce the level and extent of damage that might occur when some new vulnerability is exploited in the future.

However, this improved capability hasn’t come without a caveat. SP2 is such a major upgrade to XP that it is likely to cause some problems initially. Microsoft and beta testers all over the world have tested SP2 against a wide variety of standard applications. Unhappily, there is no way all that testing was able to examine how SP2 might act on your campus with your locally written or enhanced applications and your locally deployed infrastructure. Even Microsoft has been quite open in recommending to customers that things which have

been running successfully may fail under this new, more secure upgrade to Windows XP.

If you’ve been getting ready for SP2’s arrival all along, that’s great. If you’ve been caught a bit unprepared by this early August announcement, you should recognize that security-conscious early adopters and others will be trying to use SP2 on your campus almost immediately. Two things that you might consider doing are: (1) make sure that your campus help desk functions are ready for the increased workload and (2) complete testing local applications against SP2 right away — and don’t forget about applications under development! ♥

Why This Newsletter?

Although I’m now Stanford’s **emeritus** director for information security, some friends and colleagues have asked if I would keep in touch, providing them with my ideas and perspectives for managing information security in higher education. This notion is directly in line with my own objective of providing consulting assistance to other institutions of higher education and the organizations supporting them.

I thought a useful approach would be to write a newsletter and send it out to colleagues, friends, clients, and any others who might be interested. My hope is that some who receive this newsletter will feel moved to write or call to discuss ideas or suggest topics. My intention is to target it toward a broad readership, to keep it to just a couple of pages per issue, to make it readable in printed form or directly on a screen, to publish it multiple times per year, and to stop sending it immediately to anyone who declares their lack of interest.

Please feel free to comment back to me on anything about the newsletter, to share this freely with others, and to suggest others who you believe would like to receive this newsletter directly from me. ♥