

Lotus knows how mashups can help your business.
Smarter software for a Smarter Planet.

TRY LOTUS NOW



Magazine
Subscribe & Get a Bonus CD
Customer Service

PCWorld
Business Center

Discover [news](#), [guides](#), and [products](#) for your business

- Software & Services
- Office Hardware
- Security
- Servers & Storage
- Cell Phones & Mobile
- Operating Systems
- Networking & VOIP
- Virtualization



Tech Audit

Real tech solutions for real small businesses. [» More Tech Audit](#)
[» RSS](#) [» All Blogs](#)

Lotus knows.

SECURITY

March 30, 2010 11:06 AM

Configure Admin Rights for More Secure Windows 7

By Tony Bradley

- Print
- Digg
- Twitter
- Facebook
- More...

A new study from [BeyondTrust](#), a software developer focused on solutions for managing privileges in Windows, has some interesting results for organizations that have made the switch to Windows 7. The key finding shows that 90 percent of critical Windows 7 vulnerabilities could be mitigated simply by not allowing standard users to run with administrator privileges.

PEOPLE WHO READ THIS ALSO READ:

- [» What You Need to Know about Microsoft's Emergency IE Patch](#)
- [» US Court Orders Ukrainian to Pay for Insider Trading Hack](#)
- [» Adobe Could Be Your Security Weakest Link](#)
- [» Is the FCC Crafting Policy Based on Lousy Data?](#)
- [» E-mail Accounts of Foreign Journalists in China Hacked](#)
- [» Protect Your Data from the Next 'Card Hacker'](#)

Recommendations by [loomia](#)

Windows 7, like its predecessor Windows Vista, has a variety of security features and controls that do not exist in Windows XP. Features like tighter control of access to the system kernel, DEP (data execution prevention), ASLR (address space layout randomization), and MIL (mandatory integrity levels)



None of these security controls is a "silver bullet" defense by itself. However, ASLR combined with other security functions such as DEP, and the security aspects of UAC (User Account Control) help Windows 7 (and Windows Vista) to defend itself against many threats that would work on Windows XP and other prior operating systems.

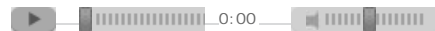
Don't confuse "more secure" with "impervious", though. At the recent CanSecWest Pwn2Own competition, a security researcher was able to [circumvent the ASLR and DEP security measures](#) and exploit a flaw in Internet Explorer 8 to take control of the target Windows 7 machine.

However, as the BeyondTrust study indicates, even if an attacker can get past the Windows 7 defenses, most malicious code can be stopped in its tracks just by ensuring that the user is not running as an administrator. The reason is that malicious code generally runs with the rights and privileges of the logged in user, so running as a standard user will restrict the malicious code to running under the standard user context--rendering it unable

Is Your Data at Risk?



Downtime can be disastrous for a business. Learn to mitigate business risks and costs. [Read this Strategy Guide.](#)



Business News Daily

Get the latest technology news that's important to you and your business, fresh seven days a week.

to attack critical system functions.

A [press release from BeyondTrust](#) quotes Steve Kelley, EVP of corporate development, "Enterprises continue to face imminent danger from zero-day attacks as new vulnerabilities are exploited before patches can ever be developed and deployed. Our findings reflect the critical role that restricting administrator rights, plays in protecting against these types of threats. As companies migrate to Windows 7 they need to be aware that despite enhanced security features on the new operating systems, better controls for administrative rights are still needed to provide adequate protection."

The BeyondTrust study also found that removing administrator privileges can mitigate 94 percent of all Internet Explorer vulnerabilities (100 percent on Internet Explorer 8), 100 percent of all Microsoft Office vulnerabilities, and 64 percent of all Microsoft vulnerabilities reported in 2009.

This shouldn't come as any real surprise to most IT administrators. Security experts have repeated the mantra of not letting standard users run with administrator privileges since malware has existed. What has changed, though, is that Microsoft has listened to feedback from the field regarding the issues encountered by customers when configuring workers as standard users, and has implemented changes to address those concerns.

You can expect user backlash--especially from executive level management who prefer to have god-like powers to install and remove whatever software they choose on the system. However, setting aside the broader legal and security issues--as well as the complexity of user support--introduced by letting users have administrator privileges, the bottom line is that simply changing Windows 7 systems to run as standard users can prevent nearly two-thirds of the potential attacks.

Wouldn't you have much more time for more proactive and important tasks--and wouldn't you sleep better at night--by implementing this one simple change?

Tony Bradley is co-author of [Unified Communications for Dummies](#) . He tweets as [@Tony_BradleyPCW](#) . You can follow him on his [Facebook page](#) , or contact him by email at tony_bradley@pcworld.com .

Best Prices on Windows OS

MOST POPULAR

ALL CATEGORIES

PCWorld



Windows 7 Home Premium

\$79.98 and up

[See All Prices](#)

PCWorld



Windows 7 Professional

\$114.99 and up

[See All Prices](#)

PCWorld



Windows 7 Ultimate

\$134.49 and up

[See All Prices](#)

PCWorld



Windows 7 Professional

\$104.98 and up

[See All Prices](#)

[See all Best Prices on Windows OS](#)

See also:

Latest in Business Center Blogs



TECH AUDIT - MARCH 31, 2010 2:34 PM

Take Advantage of New Simplified Cisco Wireless Routers

Small and medium businesses can simplify wireless networking with new Cisco Linksys E-series routers.