



Tech Insider Threat

E-mail this page | Print this page | BOOKMARK

Windows 7 Less Vulnerable Without Admin Rights

Most Windows 7 vulnerabilities can be mitigated by administrative rights limitations, report from BeyondTrust finds

Mar 29, 2010 | 10:44 AM

By Thomas Claburn, InformationWeek
Special to Dark Reading
DarkReading

Taking away the administrative rights from Microsoft Windows 7 users will lessen the risk posed by 90 percent of the critical Windows 7 vulnerabilities reported to date and 100 percent of the Microsoft Office vulnerabilities reported last year.

It will also mitigate the risk of 94 percent of vulnerabilities reported in all versions of Internet Explorer in 2009 and 100 percent of the vulnerabilities reported in Internet Explorer 8 during the same time period.

Finally, it will reduce the danger posed by 64 percent of all Microsoft vulnerabilities reported last year.

These findings come from a study conducted by BeyondTrust, which perhaps unsurprisingly sells software that restricts administrative privileges. The company argues that companies need its software to protect themselves, particularly during the time between Microsoft's publication of vulnerability information and the application of Microsoft's fixes.

"Enterprises continue to face imminent danger from zero-day attacks as new vulnerabilities are exploited before patches can ever be developed and deployed," said BeyondTrust EVP of corporate development Steve Kelley in a statement. "Our findings reflect the critical role that restricting administrator rights plays in protecting against these types of threats."

The risks poses by unchecked administrative rights aren't exactly new.

Here's what Microsoft had to say about such privileges in 1999: "Unauthorized or unknowledgeable people who have administrator privileges can maliciously or accidentally damage your organization if they copy or delete confidential data, spread viruses, or disable your network. It is vitally important to properly manage the users and groups that have administrative control over the servers and domain controllers in your network."

Insider Threat Reports



Inside Out: Protecting Your Partnerships -- and Your Data
Today's businesses depend on e-commerce among partners, but allowing third parties to access internal networks may endanger your data. How can IT security pros ensure that contractors, supplies and others get the access they need -- without becoming threats? This report offers some answers.



Rotten Apples: How To Detect And Stop Malicious Insiders In Your Organization
Most data leaks are unintentional - but in every enterprise, there are a few hard cases that defy this truism and threaten the very heart of your data. What can you do to stop these rotten apples from using their intimate knowledge of your organization - and its data access methods - to wreak havoc? This report offers a detailed look at how malicious insiders might attack your data, how they're motivated, and what you can do to stop them.



Understanding The Insider Threat
Think you know your trusted users? Think again. The availability of new Internet technologies and the pressures of a spiraling economy are changing the nature of the data breach, and your employees may have their fingers on the trigger. This report offers a look at the full spectrum of insider threats, and the risks associated with each.



Well-Meaning Employees -- And How To Stop Them
The most dangerous threat to your data isn't hackers or criminal insiders: it's the well-meaning employee, whose missteps may lead to the unintentional leak of your most sensitive corporate data. Learn how employees accidentally expose sensitive information, and how you can keep those good intentions from paving the road to your company's ruin.

Dr.Dobb's presents...
Server+client Fusion: An Architectural Proposal
Web applications have evolved from static HTML pages, to Dynamic HTML pages, to applets and Flash, and, finally, to Ajax technologies. In general, there are two significant driving forces behind the evolution of web application technologies...
Read more now...