REDMOND OBSERVER

By Andy Patrizio, ★ Advisor, Computerworld
FEB 25, 2017 9:18 PM PT

Opinions expressed by ICN authors are their own.

NEWS ANALYSIS

94% of Microsoft vulnerabilities can be easily mitigated

Just turn off Administrator's rights on the PC and you can lock it down.

If you want to shut out the overwhelming majority of vulnerabilities in Microsoft products, turn off admin rights on the PC.

That's the conclusion from global endpoint security firm Avecto, which has issued its annual Microsoft Vulnerabilities report. It found that there were 530 Microsoft vulnerabilities reported in 2016, and of these critical vulnerabilities, 94% were found to be mitigated by removing admin rights, up from 85% reported last year.

[Further reading: Fighting ransomware: A fresh look at Windows Server approaches]

This is especially true with the browser, for those who still use Microsoft's browsers. 100% of vulnerabilities impacting both Internet Explorer and Edge could be mitigated by removing admin rights, Avecto reported. One bit of progress is that 109 vulnerabilities impacting IE 6 through 11 were reported in 2016, way down from 238 in the previous year.

"Privilege management and application control should be the cornerstone of your endpoint security strategy, building up from there to create ever stronger, multiple layers of defense. These measures can have a dramatic impact on your ability to mitigate today's attacks. Times have changed; removing admin rights and controlling applications is no longer difficult to achieve," said Mark Austin, co-founder and CEO of Avecto, in a statement.

Windows 10 was found to have the highest proportion of vulnerabilities of any OS (395), 46% more than Windows 8 and Windows 8.1 (265 each). Avecto found that 93% of Windows 10 vulnerabilities could be mitigated by removing admin rights.

Microsoft Office was hit with 79 vulnerabilities in 2016, up from 62 in 2015 and just 20 in 2014. This data includes Office 2010, Office 2013, Office 2016 and the various applications. Removing admin rights would mitigate 99% of the vulnerabilities in older versions and 100% of those vulnerabilities would be mitigated in Office 2016, the latest version of Microsoft's software. Office 365 was not included in the results.

[To comment on this story, visit Computerworld's Facebook page.]

The admin rule also applies to Windows Server, where admin privileges would be more necessary and justifiable. Overall, 319 vulnerabilities were reported in Microsoft Security Bulletins affecting Server 2008, 2012 and 2016, and 90% could have been mitigated by the removal of admin rights.

[Prepare to become a Certified Information Security Systems Professional with this comprehensive online course from PluralSight. Now offering a 10-day free trial!]

Avecto said this method of turning off admin privileges works alongside tools such as antivirus to proactively prevent malware from executing in the first place, rather than relying on detection and response after the event.

It's a shame that this message is being missed. Avecto has been issuing this warning for years, and it doesn't seem like anyone is listening. The percentage of apps impacted seems to rise every year. Just three years ago the percentage of apps affected was 92%.

This should be a no-brainer for most firms. I can understand why they might not turn off admin for workers, because the limitations will undoubtedly lead to more screaming from workers who find themselves restricted for some functions, including installing software. No one wants to increase the calls to the help desk.

But Avecto has been issuing this guidance for years and it seems like no one is listening. The number of infections and breaches tells me that.

This article is published as part of the IDG Contributor Network. <u>Want to Join?</u>

Andy Patrizio is a freelance journalist based in southern California who has covered the computer industry for 20 years and has built every x86 PC he's ever owned, laptops not included.

Follow 👤 ✉ 🐦 in g+ 🔊

How to handle Windows 10 updates

YOU MIGHT LIKE

MD: Lasik is Obsolete. Do This Immediately to Restore Vision
Outback Vision

See How To Avoid Gutter Cleaning For Life
Leaf Filter

Want Better Appetite Control? Do This Once Daily (Easy but Very Effective)
Gundry MD

SHOP TECH PRODUCTS AT AMAZON

1. Oeveo Side Mount 142 - 10H x 4W x 12D | Computer Wall Mount for Lenovo ThinkCentre SFF, Dell OptiPlex SFF, and other Computers | SCM-142 $39.99
2. Artisan Power UniData ICW-1000G and WPU-7800 Phones Replacement Battery. 1200 mAh $32.00
3. Mount-It! MI-753 Triple Screen LCD Computer Monitor Desk Mount Stand Arm for 19, 20, 22, 23, 24 Inch Monitors VESA 75 and 100 Compatible Full Motion, Tilt, Swivel, Rotate, 66 lbs Capacity, Black $59.99

Ads by Amazon