CCS Technologies
616-997-TECH (8324) | support@ccstech.net | www.ccstech.net

Offices Located in Allendale and Grand Haven

6261 Lake Michigan Dr.
Suite B
Allendale, MI 49401

(616)997-8808

Hours: M-F 8-5

Contact Information

Ryan McMillen, President
rmcmillen@ccstech.net

Joe Halstead, Op. Mgr.
jhalstead@ccstech.net

Jorge Arias, Lead Tech.
jarias@ccstech.net

Drew Rowe
drowe@ccstech.net

Jeff Verry
jverry@ccstech.net

Karen Strickland
kstrickland@ccstech.net

Matt Doornbos
mdoornbos@ccstech.net

Rich Raab
rraab@ccstech.net

Ty Maxim
tmaxim@ccstech.net

The Time for Updating or Replacing That Windows 7 Computer Is...Passed

It is no longer a question of if, but a question of when. The vulnerabilities in Windows 7 are known and will continue to be unpatched for enough time that the chances of your Windows 7 (or Server 2008) machine being the target of a hacking attempt or other compromise at some point in the future is just about 100%.

Everyday since Windows 7 became unsupported (last year) more and more security holes remain unpatched and wide open for attack. Windows 7 is now in a state where no security software in the world could reasonably protect you or your network if someone were able to compromise a Windows 7 PC in your business. Think you are safe because you have very few Windows 7 PC's? It only takes one to open the door to your entire network!

Besides bypassing other security measures, one of the most important aspects of an operating system vulnerability is that once it is known, hackers will exploit millions of systems at the same time. The widely publicized Target and Home Depot data breaches from a few years ago are perfect examples of why this is so dangerous. Once a hacker knew they could get into one of the propane kiosks outside a Home Depot, they could get into all of them.

Recently, hackers found a way to attack a piece of software that has grown exponentially in its use – Zoom. How did they manage to break in and exploit the software? It was the combination of using a fully supported installation of Zoom but using it on Windows 7! Zoom ended up patching this on the following Friday, but there always comes a time when software manufacturers must give up and concentrate only on the current version of Windows, which is Windows 10. Big players such as Apple and Intuit have already weighed in, requiring Windows 8 or higher for their latest Windows based software to work. Zoom will undoubtedly follow suit at some point soon, so the writing is on the wall.

So, what is worse than the hassle of software not working? The prospect of the data on your computer or network being stolen, held ransom or your computer itself hijacked for other purposes. Picture someone stealing your car, then using it to rob a bank. This is exactly how a lot of the exploits on the Internet work.

Our hope is that news of vulnerabilities and exploits will act as a wake-up call. It will only be a matter of time before your luck runs out and one of your Windows 7 systems allows Ransomware to enter your network, steal your data and extort you.

If you have any questions of concerns on what to do next, please reach out to us and we can guide you through the options to keep you up to date. It's not that expensive and it's assuredly less expensive than an attack!

For further Reading:

https://www.forbes.com/sites/daveywinder/2020/07/10/zoom-confirms-zero-day-security-vulnerability-for-windows-7-users/#10ff8a06753d

https://quickbooks.intuit.com/learn-support/en-us/install-new-products/windows-7-support-is-ending/00/401264