FDM4 ERP WMS E-COM CRM

NewsAlert!

www.fdm4.com

May, 2017

Protect Yourself from Recent

Wannacry/Wcrypt Ransomware Attack

How do you protect yourself against the Ransomware attack being dubbed the "worst digital disaster to strike the internet in years" by multiple media sources, including Wired, **https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/** CNBC, **http://www.cnbc.com/2017/05/15/ransomware-wanncry-virus-what-to-do-to-protect.html** and the Telegraph? **http://www.telegraph.co.uk/technology/0/ransomware-does-work/**

The attack demonstrated major shortcomings in businesses' cyber-security around the world. From not performing regular updates to systems and software, to not knowing the number to contact their IT department when they were hit – many companies and government agencies felt the attack.

It turns out that much of Wannacry's cyberattack targeted a Microsoft Windows Vulnerability – which should have been easily prevented.

How do I Protect Myself?

Simply by performing the suggested updates, whether that is just a software update or a whole OS update depends on what you are working with.

The security issue really came to light because many companies are still operating Windows XP. It is important to be aware that XP is no longer officially supported. We recommend updating your systems to a more recent version of Windows to avoid future risks.

Windows 7 & 10, on the other hand are only secure from ransomware replication if you perform regular updates, and if all current patches are applied. Updates may not occur automatically, so be sure to check in with your IT department, or ours to ensure you're protected. We can also, in most cases, set your system up with automatic updates.

As for Windows Servers? You should be operating at 2008 or higher – and of course perform path updates as soon as they become available. If you are utilizing Windows 2003 consider an upgrade as soon as possible to protect your servers.

What about my Software?

FDM4 is constantly updating and improving our software to ensure your security. Our V15 browser-based ERP software doesn't share code across the network and thus, will not have the same constraints. The code for our V15 or higher software is not pulled across the network to a PC to run (GUI/.NET).

What this means is your FDM4 software is protected, even if one of your system falls victim to the ransomware.

If you haven't yet, consider updating to FDM4's latest software solutions today – keep your data protected and your operations running.

Need more information or assistance ensuring you're up to date?

Contact your Support Team or Sales today at:
salesinfo@fdm4.com or **866-676-3364.**

FDM4 America Inc. 9205 West Russell Road, Suite 335, Las Vegas, NV 89148
FDM4 International Inc. 1297 Airport Road, North Bay, ON, P1B 8G2
866.676.3364 • **www.fdm4.com**