First Network Group Inc

4-6 Perry Street
PO Box 1662
Wapakoneta, OH 45895

Located in historic downtown Wapakoneta, Ohio, FNGi has been instrumental in developing and supporting Internet Networks across the U.S. since 1993. The FNGi team can assist you with all phases of your Internet Network from initial planning through long-term support.

www.network1.net
800.578.6381

Windows 8.1 Update Rolling Out

Microsoft's latest operating system Windows 8 is receiving an update known simply as Windows 8.1. The update will be available for MSDN, TechNet customers and the general public on October 18th. OEM partners of Microsoft have received the final release already and will start shipping products with Windows 8.1 installed by the end of September.

Windows 8.1 is not a "Service Pack" update that we have become accustomed to with earlier versions of Windows. Previous "Service Packs" were a compilation of fixes and patches available for the OS and rarely included major operating system changes. Windows 8.1 will forego this concept and actually add substantial updates to the operating system itself. The new rapid release cycle that Microsoft is working with will trade the old release model for whole operating system updates similar to how Apple currently handles their updates to OSX.

Windows 8.1 will be provided free from Microsoft and the official release will come via the Windows Store App within Windows 8.

Some of the changes to expect with Windows 8.1:

- The Start Button is BACK! Clicking it will bring up the Start Screen however, not the Start Menu from previous versions of Windows.
- The Start Screen and Modern apps will work better on smaller displays (think 8 inch tablets) and more pixel dense large monitors.
- The Start Screen can be more heavily modified with background images and different tile sizes.
- Snap Views will support more than two apps and feature variable re-sizing.
- Searching across local and network storage has been greatly improved. Searches will also include online results from Bing.
- The Windows Store has been redone to make it easier to find useful apps and manage them more easily.
- Internet Explorer 11 will ship with the final release and see many improvements over the current IE10.
- Several updates to the Bring Your Own Device (BYOD) feature. Including NFC pairing and native Miracast support.
- More VPN client support and new auto-triggered VPN
- Improved security measures including Remote Business Data Removal, improvements to Windows Defender and Device Lockdown.

First Network Group, Inc has been hard at work preparing for this update. Our technicians are ready on Day 1 for the first customer who needs help. If you aren't already taking advantage of our 24x7 end-user Technical Support department or Customer Care center contact **Cory Lykins, VP** of **Tech Services** at **coryl@network1.net**. or **1-800-578-6381**, option 6.

FNGi FOCUS

YOUR CONNECTION TO THE LATEST NETWORK NEWS. OCTOBER-DECEMBER 2013

In This Issue

FNGi
First Network Group Inc

Instrumental in developing and supporting Internet networks across the U.S. since 1993.

The End of Windows XP

Twelve years ago, Microsoft released Windows XP. After 3 Service Packs and well over 300 updates, Microsoft ended their official "Mainstream Support" for Windows XP on April 14, 2009 and it entered the "Extended Support" cycle for Windows XP. On April 8, 2014, Microsoft will end their "Extended Support" cycle for Windows XP closing the final chapter on one of the most successful operating systems in the history of computing.

Windows XP was so successful that it took nearly 30 months for their Windows 7 operating system to overtake the global Windows XP install base. Today Windows XP still enjoys an install base of ~35% or roughly 800 million of the world's computers.

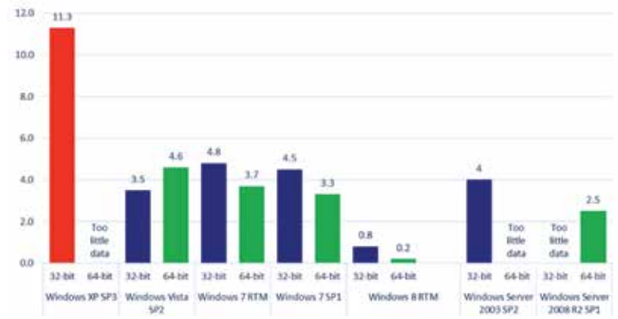
What does the end of the "Extended Support" cycle for Windows XP mean moving forward? The Mainstream Support life cycle allowed Microsoft to release "hotfixes", security updates and provide direct commercial and end-user support. The "Extended Support" cycle moved the product into only receiving security updates to the product and ended all other support. While Microsoft has made some allowances in the past for profound security-related issues for products outside of their Support Lifecycle system, on April 8, 2014, Microsoft will no longer be providing any new updates to Windows XP, including "hotfixes", service packs or security updates.

This will expose Windows XP users to a myriad of new and evolving security, malware and virus threats. Microsoft Security Intelligence Report volume 14 reports the following infection rates by operating system and service pack for the fourth quarter of 2012.

While Windows XP Service Pack 3 has made a significant reduction in the amount of security vulnerabilities and infections on the XP platform, XP still leads the pack in infection rates across all Windows operating systems. The combination of large user base with lack of security patches leaves a large target on the venerable operating system.

Continued on page 2

Infection Attack Vectors Q4 2012



THE END OF WINDOWS XP...Continued from page 1

To mitigate the risk moving forward, users must begin the transition from Windows XP when and where possible. The best option would be moving towards the latest operating system, Windows 8, as it is the most secure and reliable system Microsoft has yet to produce. That might not be an option for many people, so the next best option would be Windows 7. Between Windows XP and Windows 7 was Windows Vista, however, Vista is not an option as it is also nearing the end of its support lifecycle.

If Windows XP must be used, for whatever reason, then a hardened security presence on the system must be maintained and updated regularly. There are many anti-virus, anti-malware and firewall software options available from Microsoft and third party vendors - both free and paid. The number of unprotected or under-protected Windows XP systems moving forward could create a ticking time bomb if left unchecked and unprotected.

http://www.microsoft.com/security/

NETWORK SECURITY: THE HUMAN FACTOR

In the last issue, I discussed the fundamentals of Network Security. As promised, this article focuses on Personnel and Policy as applied to the security of your network. Long ago, hackers and crackers realized that cracking a password, for example, was much more difficult than getting the access from someone who already had it. Tricking people out of information or into access – is commonly referred to as "social engineering" in Networking circles. This kind of social engineering comes in many forms, but you can mitigate it by supporting your security fundamentals with sound policy, reinforced by training and improved by review.

SOUND INFORMATION POLICY

The protocols protecting your Network from social engineering should start with sound policy about protecting sensitive information – including usernames and passwords. These should be limited to the employees who actually need them. Moreover, they should only be communicated in a secure way among authorized people with verified I.D. The easiest way for a hacker to get a password is to ask for it! Multiple studies have shown that up to 90% of people asked for a password will provide it if there is some kind of incentive (a cheap gift, contest finalist entry and chocolate have worked in the tests.) Often, these people do not even realize that they are providing sensitive information, the transaction just seems routine to them. Confidence schemes to extort passwords range from such simple forms to elaborate schemes. Sending a username and password in unencrypted e-mail is always a bad idea – even if one assumes the e-mail will never leave the local network. Protocols should specify that the recipient of such an e-mail (or text message) should immediately notify the administration for the password to be changed. Any request for username/password information that is not made in person by a qualified employee should be suspect. There are many books and articles that cover social engineering from phishing to tailgating and other hoaxes used to extort information, gain access or introduce foreign software into a system. These books are a good source of information while writing your protocols.

Having a protocol in place is a good start, but it is meaningless without training. Your training plan should also include a calendar for cyclical retraining. 1) Retraining reinforces the policies you have developed (2) A retraining cycle will make sure you train everyone necessary by covering personnel changes caused by turnover and promotion (3) The training cycle should be used to review and update your protocols at least annually. This will allow you to incorporate defenses against any novel threats that have been recognized since your policy was established. Combining the review with training should ensure your policies are up to date and effective. Today, hacking threats range from the inquisitive teenager in his mother's basement to state-actors hacking on behalf of foreign governments and at every imaginable level in between. There may be nothing that you can do to make your network 100% secure, but you will be much closer to "five nines" security if your network and policies are built around sound fundamentals and you minimize the opportunity for social engineering to exploit your personnel.

Steve Walter, President/CEO of **First Network Group, Inc.**
swalter@network1.net 1-800-578-6381 option 1
Visit our website for more info at www.network1.net

Find us on Facebook WWW.FACEBOOK.COM/FIRSTNETWORKGROUP

If you think someone else in your organization should be receiving this newsletter, visit our website at **www.network1.net** and view our newsletter page. Select the "Sign-up to receive our quarterly newsletter" link and add them to our list. **Thank you!**

*"Our technical support team at **First Network Group** has been thoroughly trained and has the resources available to them to help guide your users through this process."*

WINDOWS 8 E-MAIL ACCESS

Microsoft is continuing the process they started with Windows 7 by not including a default email client with their latest operating system Windows 8 – well, sort of.

Microsoft has optimized the Windows 8 operating system for touch input and a variety of devices from the typical desktop PC to tablets. To accomplish this they have created the Modern operating environment that is distinct from the classic "desktop" mode.

Microsoft has included a Modern mail app with Windows 8. While this app supports IMAP and can link to various web-based email clients, it really does not have the full depth and breadth of a traditional e-mail client.

Typically, we recommend bypassing the use of the Windows Mail App and instead relying on your own web-mail offering or downloading a more traditional e-mail client. The Windows 8 classic desktop mode allows you to run any of these programs: Microsoft Windows Live Mail (part of the Live Essentials Pack), Mozilla Thunderbird and of course any version of Microsoft Outlook from Microsoft's Office suite of programs.

Our technical support team at First Network Group has been thoroughly trained and has the resources available to them to help guide your users through this process.

If you are not currently taking advantage of our 18 years of experience providing outstanding end-user technical support, please contact **Cory Lykins**, **V.P.** of **Tech Services** at **coryl@network1.net** or **1-800-578-6381**, option 6 and we will get you started!

THE LATEST ON DHCPATRIOT

DHCPatriot version 5.3.0 should be in general release by the time you read this article.

Arguably, the most important new feature in this build is the "floating IP support" implemented with Virtual Router Redundancy Protocol (VRRP). This is a key feature to make the access to the DHCPatriot login page completely seamless. Previously, router configuration would need to be changed to force authentication traffic to a specific DHCPatriot in the case of an outage. Using VRRP allows a third IP address to "float" between the two devices. This allows the router to force authentication traffic to this third IP address. Other enhancements in this version include:

- "Searchable Option 82" information that is stored with the sessions;
- Template-based configuration of static address definitions in standard DHCP for quick configuration of ONT networks, for example;
- Optional protection of the authentication page against automated clients via a simple math problem;
- Checking stored credentials against the RADIUS server during an un-suspend operation;
- Optionally send RADIUS ALIVE (interim-update) packets upon DHCP client lease renewal;
- Optional RADIUS forwarding to external devices that need a RADIUS accounting stream.

Darren Ankney, V.P. of **Product Development**
dankney@network1.net 1-800-578-6381 option 3
Visit our website for more info at www.network1.net

DHCPatriot™