

Time For Action: When Windows Can't Protect You

Torsten Roessel



All things come to an end. And so it is with Microsoft Extended Support and Security Updates for Windows 2000, which will cease in July of this year. Any manufacturer with industrial applications based on Windows 2000 may wisely be considering a newer operating system right now, in order to remain in production with the needed security support. But migrating to a new operating system can be time-consuming, disruptive, and expensive.

Are there any better alternatives? This article presents one proven solution.

Microsoft Windows operating systems are widely used for networked industrial automation equipment. Unfortunately, these industrial Windows applications, like their counterparts in office networks, are also vulnerable to known and new Windows security loopholes that can be exploited.

What Should be Done?

Proceeding with “business as usual” while keeping both eyes firmly shut is not a recommended course of action. Worms, viruses, Trojans, and hacker exploits are problems not to be ignored. The widespread popularity of Microsoft operating systems has made them an all too appealing target for malware creators. In 2009, Microsoft issued forty-eight Security Updates relevant for Windows 2000, including thirty-one classified as “Critical,” the highest classification.

Time For Action: When Windows Can't Protect You

Published on Industrial Maintenance & Plant Operation (<http://www.impomag.com>)



In every month of 2009, at least one new breed of malware had to be dealt with. The notorious Conficker worm proved to be a particularly troublesome issue, as well as the dangerous and versatile Trojans Waledac and the Bredolab downloader, ushering in a plethora of evil malware and spyware from servers hosted mostly in Russia and China. The expiration of support for Windows 2000 means the end of available and automated security updates against these kinds of threats.

Expensive Upgrades

An obvious solution, of course, is the upgrade to a newer operating system with current support, now and for the near future. But upgrades are costly. New licenses need to be purchased and new software installed. And as new versions of Windows tend to be ever more hungry for resources, they often require the acquisition of new hardware and infrastructure as well. That is when the dreaded “unanticipated consequences” begin to occur, involving considerable extra work and expense. Certified systems and automated manufacturing processes typically require reiteration of an expensive approval process when altering any of their components. As a result of production complications greater than those in the office environment, significant upgrade expenses can quickly accumulate. And who wants the responsibility of triggering that cost avalanche when it is very difficult to calculate the potential security risks and the risks of unforeseen glitches that can affect production? Common sense and demonstrated logic often dictate “if it’s not broke, let’s not ‘fix’ it.”

Protection by Retrofitting Distributed Security Appliances

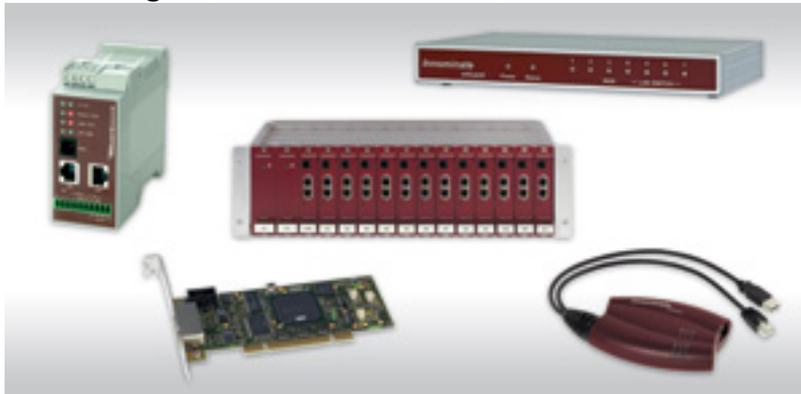
What virtually all software security risks share in common is that they are based on the weaknesses and vulnerabilities of network protocols and services. Hacker

Time For Action: When Windows Can't Protect You

Published on Industrial Maintenance & Plant Operation (<http://www.impomag.com>)

exploits and malware use these weaknesses over an IP-based network to gain access, control, and opportunities for damage and proliferation. If security updates against newly discovered vulnerabilities are no longer available, there is an increased risk to the unsupported system, which must continue to communicate with other network nodes, and often with portions of the outside world (engineering and programming consultants, remote maintenance services, etc.).

It is the purpose of firewalls to control and selectively filter unrestricted Ethernet and IP-based communications on the network. In addition to front office firewalls, there are industrial network security appliances that are needed to provide "defense-in depth" on the factory floor. This method of protection is better, faster, cost-effective and easily installed by technicians rather than network administrators. Availability is in various industrial-rated designs; for DIN-rail mounting, for 19" rack mounting in cabinets, as PCI cards or as dongle-style patch cords. An example is the family mGuard products from Innominate Security Technologies, Phoenix Contact, and select others.



No changes need to be made to the network configuration of the existing systems involved. Yet the devices operate invisibly and transparently, monitoring and filtering traffic to the protected systems by providing a Stateful Packet Firewall according to rules configured via templates from a centrally located server.

If required, the security of networked equipment may be further enhanced by additional mGuard features. Configuration of specific user firewall rules can restrict the type and duration of access for authorized individuals, who may login and authenticate themselves from varying locations, PCs, and IP addresses. Virtual Private Network (VPN) functions provide for secure authentication of remote stations, and the encryption of data traffic.

Conclusion

The clock is ticking. In a few months, untold numbers of Windows 2000 systems will no longer have access to Extended Support and Security Updates, when these end in July 2010. Nor may there be adequate time for analysis and evaluation of alternatives, decision making, planning, preparation and implementation of a new operating system. The right time to act is now. There are proven "defense-in-depth" security products available to provide protection for industrial networks.

For more information about current threats to networked industrial equipment, a

Time For Action: When Windows Can't Protect You

Published on Industrial Maintenance & Plant Operation (<http://www.impomag.com>)

*comprehensive 18-page White Paper “**Hacking the Industrial Network,**” including footnotes, clickable Internet research links and detailed references is available for download at www.innominate.com [1].*

Sources:

[Microsoft Support Lifecycle](#) [2]

[Microsoft Security Bulletin Search](#) [3]

[The Microsoft Windows Malicious Software Removal Tool](#) [4]

Microsoft® and Windows 2000® are registered trademarks of Microsoft.

mGuard® is a registered trademark of Innominate Security Technologies AG

About the Author:

Torsten Rössel is the Director of Business Development for Innominate Security Technologies AG in Berlin. He is a frequent speaker at industry conferences, and author of numerous articles on the protection of networked industrial systems and secured remote services for machinery over the Internet. He is available at: troessel@innominate.com [5].

Source URL (retrieved on 04/27/2015 - 9:14am):

<http://www.impomag.com/articles/2010/04/time-action-when-windows-cant-protect-you>

Links:

[1] <http://www.innominate.com/>

[2] <http://support.microsoft.com/lifecycle/>

[3] <http://www.microsoft.com/technet/security/current.aspx>

[4] <http://support.microsoft.com/kb/890830/en-us>

[5] <mailto:troessel@innominate.com>