MANAGE

A Windows security checklist for IT managers

Do the Windows security products you're considering address every security issue? Use this high-level checklist as a quick reference to make sure all your bases are covered.

By Rebecca Herold, Contributor

Rebecca Herold

At a large IT conference recently, I had the chance to speak with some IT managers about the resources they use to help them secure their systems, networks and applications. I asked specifically about any checklists or quick reference sheets they use to help them to choose the best security products for their Windows systems. Most shook their heads and shrugged their shoulders, and one summed it up nicely by saying, "When you find one, send it my way."

IT managers already have plenty of things that keep them up at night. Add to that concerns about the effectiveness of their Windows security products. Not only do they worry about how to prevent security incidents and privacy breaches in vulnerable systems, but they must also comply with a growing number of legal, regulatory and contractual security requirements. Regulatory requirements touch virtually every part of the business, including the following activities:

- Providing guest and anonymous access
- Limiting vendor access for maintenance purposes
- Controlling what users can do in the Windows environment
- Segmenting the Windows system to better protect sensitive information
- Documenting and auditing user activities and capabilities

More Windows security checklists

For more detailed documents covering the security requirements for all kinds of systems and applications, visit look at the

What IT managers need is a high-level checklist they can use as a quick reference to help ensure that the Windows security products they're considering address the full scope of security issues. The following is one version of that kind of checklist with all areas listed – in no particular order -- that need to be evaluated:

NIST Security Configuration Checklists Repository

✓ **Account management --** Can the security software be centrally managed using unique, nonshared IDs with administrative capabilities that can be logged? Can user accounts have security restrictions established, such as automatically disabling accounts after a specified period of non-use? Does it enforce strong passwords?

✓ **Backup and archives --** Can the software be configured to have the program code and related data backed up automatically according to a schedule you can establish and change as necessary?

✓ **Certifications --** Has the security software been certified by an objective and independent party to work as advertised? For example, has the software been certified to meet applicable FIPS standards? Or CIS certification?

✓ **Configuration settings --** Can you configure settings, such as the logon display, concurrent users, time limitations and so on, to be most appropriate for your organization? You should be able to establish configuration settings that are in compliance with your organization's security policies and standards.

✓ **Data protection --** Does the security software have protections built in to protect the data it generates, such as access controls and options to strongly encrypt the data?

✓ **Documentation --** Does the software have thorough, comprehensive and easy-to-understand documentation detailing how to use it along with descriptions of the possible side effects of using the software?

✓ **Identification and authentication --** Do end user identification and authentication capabilities exist so that you can control the people using the software and track when each individual uses the software?

✓ **Integration and compatibility --** Can you implement the security software into your existing Windows environment without needing to make a lot of changes to other existing applications, network settings, network interfaces and so on? The most secure Windows security products typically require the least changes within the existing Windows environment.

✓ **Known issues --** Does the security software come with a list of summarized issues about what may happen after you implement the software into your network? This will help you pinpoint any functional or operational problems caused by the software.

✔ **Licensing --** Does the software license agreement allow you to use the security software in all locations you need to, not only on network endpoints but also on mobile computers, employee-owned computers that are used for business and more?

✔ **Logging and audit trails --** Does the security software give you the ability to log a very wide variety of actions and events related to the security product, such as when it was used, who used it, the security problems that were discovered and so on?

✔ **Point of contact --** Does the security software vendor provide you with a specific person or department with whom you can communicate via email, postal letters and phones when you need questions, comments and suggestions addressed? Are problem reports associated with the security software available?

✔ **Product role --** Does the security software specify the primary purpose, function or use for the software? Be sure that the software you are purchasing to address a specific issue actually *does* cover that issue and not other issues that you're not really interested in.

✔ **Regulatory compliance --** Does the security software provide clearly written and succinct documentation stating the regulations it supports for compliance along with a description of specifically how the software supports compliance? Common security software compliance claims include those for HIPAA, GLBA, FISMA and Sarbanes-Oxley, but many don't explain the ways they support compliance.

✔ **Rollback capability --** Can any changes in the security software configuration be rolled back? And, if so, does documentation exist that explains how to rollback the changes?

✔ **Software integrity --** Does the security software have controls to protect the integrity of the software, as well as privacy protections for associated data? Without integrity controls, the software could be altered in a way that would make it less, or even not at all, effective in safeguarding your Windows environment.

✔ **Testing information --** Does the security software list the platforms upon which the security software was tested? Tests should have occurred on all platforms that exist in your network environment. Did the tests include security and privacy tests?

✔ **Troubleshooting --** Can you turn off the security software for troubleshooting or to perform specific types of audit activities without affecting network operation?

✓ **Upgrade issues --** What are the requirements for upgrading the software? Are upgrades to the software, including security patches, included in your purchase agreement and/or licensing agreement?

And just because you are buying security software, don't assume that the software itself is secure. You need to ask the questions from the checklist to help validate that it actually is secure.

Even if you already know the answers for all of the issues on this checklist, chances are all the people working with and supporting the IT Windows environment do not have the same knowledge. Give your IT staff a checklist to raise their awareness. Making documentation available makes them accountable for performing activities to ensure security exists within your Windows environment.

Rebecca Herold, CISSP, CISA, CISM, CIPP, FLMI, has more than 17 years of experience in IT, information security, privacy and compliance and is the owner and principal of Rebecca Herold LLC. She is an adjunct professor for the Norwich University Master of Science in Information Assurance program and is writing her 11th book. Her articles can be found at www.privacyguidance.com and www.realtime-itcompliance.com.

This was last published in November 2008

New edition of Windows 10 to take on big data

Windows OS updates get simpler -- but there's a trade-off

What causes desktop login and boot times to spiral out of control?

Load More

Start the conversation

Share your comment

Send me notifications when other members comment.

Add My Comment

VIRTUAL DESKTOP WINDOWS SERVER

SearchVirtualDesktop

How to plan a VDI test before a full deployment

Whether IT is running VDI for the first time or simply tweaking the back-end hardware, testing VDI is a complex but necessary ...

How Linux thin clients have improved

VDI shops should consider Linux-based thin clients as endpoints for their users for several reasons, including the fact that they...