A hard approach to system security

Is hardening your systems worth the time and trouble? Most say yes.

By John Edwards
September 22, 2010 06:00 AM ET

Computerworld - Glenn S. Phillips, president of Pelham, Ala.-based Forte Inc., says that the dedicated Windows workstations his company sells to hospital emergency room administrators must not only be secure, but also absolutely tamperproof. After all, lives depend on the machines' flawless operation.

Forte's applications show inbound EMTs the emergency room's current availability status, "so our software must be the program that is always running," Phillips says. "We cannot have anyone closing our program, adding games, changing Windows settings and so on."

Hardening basics

Chase Carpenter, a unit manager in Microsoft's Windows Server unit, says a hardening strategy should focus on the following tactics.

Reduce the attack surface by:

- Removing any nonessential tools and features.
- Disabling any unnecessary services and protocols.
- Removing or securing any file shares.

Restrict user access by:

- Limiting user accounts.
- Restricting access rights.

Protect against known and theoretical attacks by:

- Configuring common security settings.
- Applying necessary patches and updates.
- Using encryption where possible to protect critical data.

Configure the system to detect attacks by:

- Configuring the system to log appropriate and inappropriate user access.
- Configuring the system to make it difficult or impossible for attackers to cover their tracks.

Phillips and others who need to create highly secure workstations or servers are turning to hardening to create a virtual steel wall against intruders. The hardening process involves removing nonessential tools and utilities from an operating system or application, any of which could be used to help an attacker gain unauthorized access to system settings or data.

The approach can be used to substitute for or (more commonly) complement other security technologies and practices, such as network firewalls.

Going old-school

Hardening, a technique that's been around since the earliest days of networked computers, gradually fell into the shadows as software developers incrementally boosted their products' internal security, and as newer and more sophisticated security technologies and practices arrived

Top Stories
- Phishing scams likely, warns DHS
- Image gallery: Steve Jobs through the years
- Elgan: How Apple will kill cable TV
- Wireless carriers prep for Hurricane Irene

on the scene.

"Operating systems and applications are more secure than ever," observes Chris Rafter, vice president of consulting services at Logicalis, a systems integrator in Bloomfield Hills, Mich. Yet improved software security hasn't made hardening any less practical or useful. "It's still one of the least expensive and most effective ways of protecting yourself or preventing infections or outages -- just basically closing security holes that might affect your company adversely," Rafter says.

Peter Makohon, a senior security and privacy manager at the New York office of professional services firm Deloitte & Touche, says hardening is coming back into fashion as more enterprises face pressure to patch every possible security loophole that could conceivably be exploited as an entry pathway. He says that a growing push for stricter compliance measures from private and public regulators is inspiring many enterprises, particularly those involved in finance, health care and other highly regulated industries, to take another look at hardening. "They are now hardening, spending more time securing their more critical assets," Makohon says.

Just about any enterprise can benefit from hardening, Rafter says. "Operating systems and applications are definitely a lot more secure than they were a long time ago, but there's still logic to turning off unnecessary services and basically only activating and using what you really need," he contends. "Plus, it doesn't require a great deal of effort."

1 2 3 4 Next page

From CIO.com

- 21 Chrome Web Apps for Serious Work
- Why You Shouldn't Buy a Discounted TouchPad Tablet
- Workplace Conflict: How to Diffuse Battles with Co-Workers
- What CIOs Need to Know About HP's Acquisition of Autonomy

Questions From IT Pros

- How do I protect my privacy on Google+?
- What's the best way to restore a Mac OS X Lion drive?
- How do I determine the cost of running Hadoop?
- How do I prevent a SQL injection attack?

» Read more at ITworld Answers

Additional Resources

WHITE PAPER

Options for Protecting against Web Threats

This independent paper from senior analyst Jon Collins at FreeForm Dynamics considers how Web-based security threats are evolving, within the context of IT trends including mobile, home computing and other forms of remote access that could potentially increase the attack surface of the companies. It defines the scale and types of threat, what to look for in a corporate web security solution and compares the different types of technological approach available to companies and the processes that need to be considered for effective protection.

Read now.

WHITE PAPER

Enter the Security KnowledgeVault

Security is not an option. This KnowledgeVault Series offers professional advice how to be proactive in the fight against cybercrimes and multi-layered security threats; how to adopt a holistic approach to protecting and managing data; and

WikiLeaks: How am I Affected?

The latest WikiLeaks episode has raised questions about how organizations and governments protect their sensitive information. While this incident was isolated, it has...

All Security Webcasts

Featured Security Blog

INSIDER **Preventing security threats from cleaning staff**

By Richi Jennings

Do you know who's in your building at night? Can you positively vouch for all those here-today, gone-tomorrow contract staff who clean and maintain your offices? Physical access is a worryingly simple vector for data-stealing malware. INSIDER (free registration requested) *more*

Newsletter Sign-Up

Receive the latest news test, reviews and trends on your favorite technology topics

- [x] **Computerworld Daily News**
- [ ] **Security**
- [ ] **Virus and Vulnerability Roundup**
- [ ] **Security: Issues & Trends**

Your Email

Industry

Job Title

Company Size

Country

Subscribe View all newsletters | Privacy Policy

IT Jobs

Software Engineer, Computer Engineer,...
Fort George G Meade, MD - National Security Agency (NSA)

Chief Technology Officer
New York, NY - Purpose

Chief Technology Officer Job
Los Angeles, CA - Thomson Reuters-boston

Chief Technology Officer (CTO)
Boulder, CO - Motus IT

Senior Software Engineer, Office of the...
Sunnyvale, CA - Yahoo!

See All Jobs Post a job for $295

job title or company location Go

Jobs by SimplyHired

how to hire a qualified security assessor. Make security your Number 1 priority.

Read now.

WHITE PAPER

Guide to SMB Communications

To date, small businesses have been unable to cost justify an IP-based communications system. This paper provides organizations with fewer than 250 employees a way to meet unique voice and data communications needs even with a limited budget and small IT staff.

Read now.

Add New Comment

Login

Showing 6 comments

Sort by newest first

Anonymous

Center for Internet Security Standards
Can't believe that CIS (CISecurity.org) has not been mentioned as a template for creating hardened OSs (Windows, Linux, Solars, IOS, etc) and applications (SQL Server, Oracle, MySQL...)

Organizations like mine (financial) that have been implementing hardening across the board for the last few years will know that it is critical to maintain hardening settings the same way any other system configurations are. We deploy CIS Level 2 hardening settings via GPO to all workstations and servers.

The discipline of hardening an environment at a macro level really forces an IT organization to a level of maturity that necessarily improves process and security in other areas.

09/30/2010 07:41 AM Like Reply

Anonymous

Center for Internet Security Standards
Can't believe that CIS has not been mentioned as a template for creating hardened OSs (Windows, Linux, Solars, IOS, etc) and applications (SQL Server, Oracle, MySQL...)

Organizations like mine (financial) that have been implementing hardening across the board for the last few years will know that it is critical to maintain hardening settings the same way any other system configurations are. We deploy CIS Level 2 hardening settings via GPO to all workstations and servers.

The discipline of hardening an environment at a macro level really forces an IT organization to a level of maturity that necessarily improves process and security in other areas.

09/30/2010 07:41 AM Like Reply

Ron

Great, but ..

This advice is a starting point, but it is too high level. How about providing links to more detailed instructions?

At least in 'nix you can remove services and applications not explicitly needed. That is not as easy to do in Win. Try to figure out which windows services you can turn off. They have cryptic names and many don't have useful descriptions. Even going to hardening sites is marginally helpful.

Here are a few links to Win hardening tips I've collected. I found that advice often carries over to new versions, ie from XP to Vista to Win7 with only slight adjustments:
http://downloads.techrepublic.... (this is a good one)

http://downloads.techrepublic....

http://www.zdnet.co.uk/news/it...

http://windows.uwaterloo.ca/Ma...

http://www.pcworld.com/article...

http://blogs.techrepublic.com....

http://www.windowsecurity.com/...

http://www.worldstart.com/tips...

http://www.smartpcutilities.co... - a tool for Vista Services optimization. It's been a while since I tried it.

09/22/2010 05:38 PM Like Reply

hansel

Evenmmc.dll
We had a work computer hit by an unknown file called evenmmc.dll. The infected computer's CPU was tasked 100% making the use of the computer almost inpossible. I took the infected HD and put it in another computer as slave to remove that file and on restart the CPU is not tasked 100% and now the computer is useable. There is some unknown program running in the backround and I am not through repairing this workstation. That file was also in the registry under Control Session manager/appcertdlls and I also removed the file from there before restarting

09/22/2010 11:00 AM Like Reply

Anonymous

Seriously, how long does your app stay running?
and how long does your MS Windows OS stay running?

Lives are involved and you said you use MS Windows, so I can't seriously consider clicking to Page 2.

09/22/2010 08:05 AM Like Reply

Fatman

I guess someone failed to read the EULA
IIRC, Microsoft's EULA expressly disclaims the use of Windows in life safety situations.

(flame bait)
Secondly, why would anyone want their life dependent on the proper function of Windows???
(/flame bait)

09/22/2010 08:14 AM in reply to Anonymous Like Reply

Skip to top

About Us **Advertise** **Contacts** **Editorial Calendar** **Subscribe to Computerworld Magazine** **Help Desk**
Newsletters **Jobs at IDG** **Privacy Policy** **Reprints** **Site Map** **Ad Choices**

The IDG Network: CFOworld | CIO | Computerworld | CSO | DEMO | GamePro | Games.net | IDC | IDG | IDG Connect | IDG Knowledge Hub | IDG TechNetwork | IDG Ventures | InfoWorld | ITwhitepapers | ITworld | JavaWorld | LinuxWorld | Macworld | Network World | PC World