Practical Steps to Take to Mitigate Computer and Network Risks

Eugene Infraguard Meeting
308 Forum Building, Lane CC
Friday, March 12th, 2004

Joe St Sauver, Ph.D.
joe@uoregon.edu
Computing Center
University of Oregon

The Level of Today's Talk

- Given that this is a mixed audience of computer/network folks and non-computer/ non-network folks, I'm going to try to deliver a talk geared for that audience with a "little something for everyone" – largely non-geeky, but with indulgences where necessary.
- This presentation's level of verbosity (which is relatively high) is designed to accommodate both folks who are here today, and folks who may look at this talk afterwards.

Technical (NOT Policy-Oriented) Focus

- While sound security policies can be as (or more) important than doing the right technical things, for today's talk we're going to largely focus on concrete technical issues rather than general policy issues.
- My goal is to give you specific tasks ("homework," if you will) that will lead to perceptible improvements in your company's computer and network security.

Obligatory Disclaimer

- While the suggestions in this presentation *may* improve your security, and reasonable care has been used in compiling this presentation, no brief presentation of this sort can substitute for an onsite, comprehensive and intensive security review done at your site by qualified professionals. We recommend you have one done.

- If you do elect to take any of the steps outlined in this document, you acknowledge that some of those steps may include inherent risks of their own, including but not limited to loss of data, or loss of functionality/usability.

- Make a complete backup of your system, including all personal files and your system's registry, before making ANY changes.

- You understand and acknowledge that even if you follow all the recommendations in this presentation, you and your network or system may still be vulnerable to known and/or as-yet-unknown security threats.

- Mention of a particular hardware or software product in this presentation should not be taken to be a recommendation excluding equally capable equivalent products. Products change over time, and needs can vary dramatically, so always do your own evaluation before purchasing any product.

The Security Problem in a Nutshell

‘I'm here to tell the security pros reading this that we are in deeeeeep trouble when it comes to securing the computers of [your typical American computer user].

‘Security is just not a concept that "normal" folks focus on. It's not even on the radar screen. It's just not thought about at all.’

“Joe Average User Is In Trouble”
By Scott Granneman Oct 22, 2003
http://www.securityfocus.com/columnists/193

The Sky Is Still Blue, The Grass Is Still Green, and The Sun Is Still Shining…

- Do we even really have a problem? Maybe we're all just being too shrill, or looking for boogey men where none really exist.
- Maybe we really don't have anything to worry about… maybe there's just a bunch of doom-saying (cyber-security-money-wanting!) apocalyptic ninnies running around talking about how the sky is falling, the sky is falling when every thing is really pretty much OK...

Problem/No Problem? You Decide

- One nice overview of daily IT security issues is Infocon from the IWar people; archives and mailing list subscription information available online at http://www.iwar.org.uk/pipermail/infocon/
- Or consider this note:

"Companies in manufacturing industries are putting more emphasis on security than any other information technology initiative, according to research from analysts at Gartner." http://zdnet.com.com/2100-1105-5169182.html (March 3, 2004))

Personally, I Believe Security Is The #1 Computing and Networking Issue Today

- Absolutely and without question, in my opinion, the number one computing- and networking-related challenge we all face today is computer and network security.
- Computer and network security problems affect corporations and small businesses, governments, higher education, grade schools and high schools, individuals and families alike – all of us are struggling.

Government and Critical Infrastructure Sites (G&CISs) Face Some Special Security Risks

- G&CISs face special risks:
  -- hacker/crackers (and terrorists) know that they're newsworthy "high value targets"
  -- some hacker/crackers may think G&CISs either aren't paying attention, or can't afford to harden their sites
  -- still others may think that G&CISs lack the political will to publicly prosecute attackers (perhaps due to the potential for negative publicity, or prosecutorial case overload).

Some Public War Stories

- 'GOP staff members of the Senate Judiciary Committee had free access to sensitive Democratic computer files because of what investigators termed a "significant lack of security" on the committee's network. A report by the Senate sergeant at arms has blamed the poor controls on the IT administrator's inexperience and lack of training.

  '"Forensic analysis indicated that a majority of the files and folders on the server were accessible to all users on the network," said the report, released yesterday. **"Any user on the network could read, create, modify or delete any of the files or folders."'** http://www.gcn.com/vol1_no1/daily-updates/25196-1.html (March 3, 2004)

- "FBI agents arrested a Louisiana man last week under the cyberterrorism provisions of the USA PATRIOT Act for allegedly tricking a handful of MSN TV users into running a malicious e-mail attachment that **reprogrammed their set-top boxes to dial 9-1-1 emergency response**." http://www.securityfocus.com/news/8136 [while this was obviously a trivially small attack, imagine the same attack delivered more broadly, to 100's of 1000's of hosts via a mass mailing worm] (February 26, 2004)

More Incidents… Some Amusing, Some Not

- ‘A Raleigh, North Carolina cable news channel shut down a Web application designed to allow local schools and businesses to report weather-related closings last week, after a handful of puckish university students discovered they could use it to add textual graffiti to the station's newscast. […] According to screen shots saved by observers, **other messages sprinkled among the genuine closings that rotated through the ticker included "1337 5p34k Linguistic Services," "All Your Base Are Belong To Us,"** and a note that "Tutone Inc." would be closed, and employees should call "Jenny at 867-5309" for more details.’ http://www.securityfocus.com/news/8191 (March 4, 2004)

- ‘In January 1982, President Ronald Reagan approved a CIA plan to sabotage the economy of the Soviet Union through covert transfers of technology that contained hidden malfunctions, including software that later triggered a huge explosion in a Siberian natural gas pipeline, according to a new memoir by a Reagan White House official. […] "In order to disrupt the Soviet gas supply, its hard currency earnings from the West, and the internal Russian economy, **the pipeline software that was to run the pumps, turbines, and valves was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds,**" Reed writes. "**The result was the most monumental non-nuclear explosion and fire ever seen from space,**" he recalls, adding that U.S. satellites picked up the explosion.’ http://msnbc.msn.com/id/4394002/ (Feb 27, 2004)

Privacy Compromises…

- 'Eureka [CA] police began investigating Wednesday how confidential e-mails related to a fraud lawsuit against Pacific Lumber may have been stolen and leaked to the media. District Attorney Paul Gallegos alleged that **about a dozen e-mails were stolen from the computer of Assistant District Attorney Tim Stoen**. The e-mails, dating from February 2003, describe advice given by a local environmentalist to Stoen on the Pacific Lumber lawsuit.' http://www.mercurynews.com/mld/mercurynews/7987056.htm (Feb 19, 2004)
- "A government contractor posted a $100,000 reward Tuesday in the **theft of Social Security numbers and other personal records of 500,000 military service members and their families** in 16 states." (January 2, 2003) http://www.wired.com/news/privacy/0,1848,57045,00.html
- "On January 16, 2003, it was discovered that a computer hard drive containing the personal records of more than one million Canadians was missing from ISM Canada." http://www.priva-c.com/privacyhorizon/lessonslearned_ism.asp

Denial of Service Attacks…

- 'With little notice by law enforcement or the outside world, online sports betting parlors, or sports books, have suffered a plague of sustained **distributed denial-of-service (DDoS) attacks in recent months that have knocked some Web sites offline for days or weeks.** Other sites have been forced to pay protection money to keep their gambling operations online * * * The trouble usually starts with an ominous e-mail and a sudden and unmanageable surge in Internet traffic * * * "Your site is under an attack and will be for this entire weekend. You have a flaw in your network that allows this to take place," according to a copy of such an e-mail provided to IDG News Service. * * * "You can ignore this email and try to keep your site up, which will cost you tens of thousands of dollars in lost wagers and customers, or you can send us $40k by Western Union to make sure that your site experiences no problems," the message continues.' http://www.infoworld.com/article/04/01/29/HNsuperbowl_1.html
- [discussing worms like Mydoom] "This is a much larger attack network than anything we have seen before. **With this kind of horsepower, you could take down not just one site, you could take down thousands of sites – big sites – at the same time and keep them down for quite a while.**" http://www.computerworld.com/securitytopics/security/virus/story/0,10801,89827,00.html

Mundane Issues, Many With Easy Solutions

- Fortunately, many security issues are mundane and tractable, and quite easy to deal with, IF people are paying attention.

  "Gartner reports that more than 90% of security exploits are carried out through vulnerabilities for which there is a known patch."

  http://www.nwfusion.com/news/2002/1111bigfix.html

Your PCs Running Windows

- In this section, you'll notice that we largely focus on PCs running Windows. That's for a couple of reasons:
  -- PCs running Windows represent ~94% of the desktop market as of late 2003 (see: http://content.techweb.com/wire/story/TWB20031008S0013)
  -- Windows operating systems also have roughly 50% of the server OS market
  -- Rebut able hypothesis: hackers crack Windows because that's what's "out there"

1. If You're Running An Old Version of Windows Your Must Upgrade (or Switch OS)

- Many companies and end users are still running older versions of Windows such as Windows 95, Windows 98, Windows 98 Second Edition, Windows ME, NT 4.0, Windows 3.11, etc.

  If you're among them, you must upgrade to a current version (or switch OS if you prefer :-)).

  You cannot safely stay on these earlier versions of Windows.

Microsoft on Upgrades

- See “Product Lifecycle Dates – Windows Product Family” http://support.microsoft.com/default.aspx?scid=fh;[ln];LifeWin
- See also “Microsoft Bows to Pressure, Extends Support for Older Windows Versions” [sorta, sorta not] at http://www.eweek.com/article2/0,4149,1434318,00.asp (Jan 12, 2004)
- “Security 'impossible' for Win9x, buy XP now, says MS exec,” http://www.theregister.co.uk/content/archive/28100.html (11/14/2002)

And No, I'm Not Kidding About Considering Alternative Operating Systems…

- A monocultural Microsoft-centeric desktop environment creates certain risks that an environment consisting of a mix of PCs running Windows, Macs and Linux boxes doesn't have.
- Others have already noticed this, and are taking steps to move their organizations away from 100% reliance on Microsoft Windows. For example…

The Non-Windows Desktop

- '"Our chairman has challenged the IT organization, and indeed all of IBM, to move to a Linux based desktop system before the end of 2005," states the memo from IBM CIO Bob Greenberg...' http://www.eweek.com/article2/0,4149,1494398,00.asp
- "Scientists: The Latest Mac Converts" http://www.ecommercetimes.com/perl/story/32837.html
- "Mac OS X Site License Available [at the University of Oregon]" http://cc.uoregon.edu/cnews/winter2004/osx.html
- "Two U.K. government agencies—with more than 1.2 million desktop computers combined—announced in recent months that they would use desktop Linux and other open source software." http://www.reed-electronics.com/eb-mag/index.asp?layout=article&articleid=CA376443&industryid=2117&rid=0&rme=0&cfd=1
- "[Dave Thomas, former chief of computer intrusion investigations at FBI headquarters] told us that many of the computer security folks back at FBI HQ use Macs running OS X, since those machines can do just about anything: run software for Mac, Unix, or Windows, using either a GUI or the command line. And they're secure out of the box. * * * Are you listening, Apple? The FBI wants to buy your stuff." http://securityfocus.com/columnists/215

Changing "Religions" Aside…

- Let's assume you're stuck running Windows, at least for now…. what should you do to be as secure as possible within that overall constraint?

2. Microsoft Critical Updates

- It is absolutely vital that everyone at your site patch their systems when Microsoft releases Critical Updates… and those updates are now a routine monthly occurrence.
- When Critical Updates don't get applied, viruses and other malware will infest your systems, compromising confidential data and potentially turning those systems into network sniffers, spam delivery systems, and denial of service attack vectors.

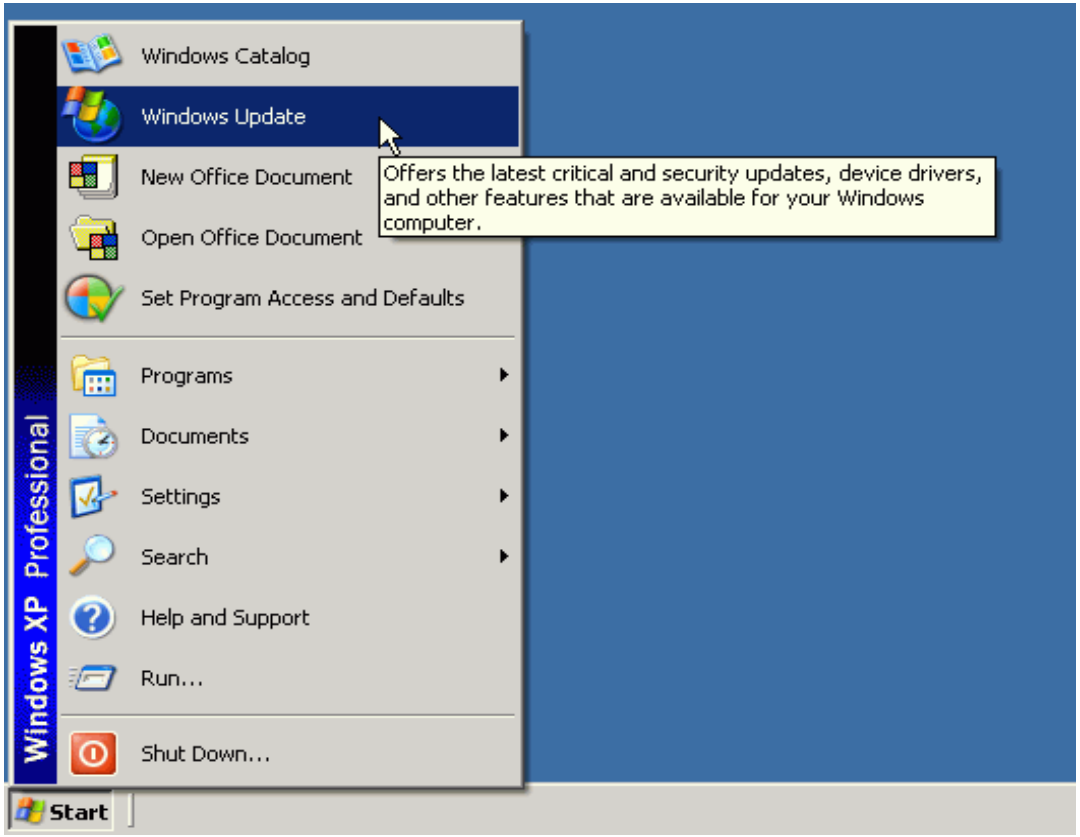
Getting Initially Up To Date

- If you're not currently fully patched up, you'll need to at least get all service packs and critical updates downloaded and installed. Doing so initially can be difficult for two reasons: (i) the sheer volume of updates can be onerous for dialup users, and (ii) unless you're behind a hardware (or software) firewall, you will commonly become infected before you can even finish downloading the required patches. (Yes, it has gotten that bad)

Dealing With the "Chicken and Egg Problem"

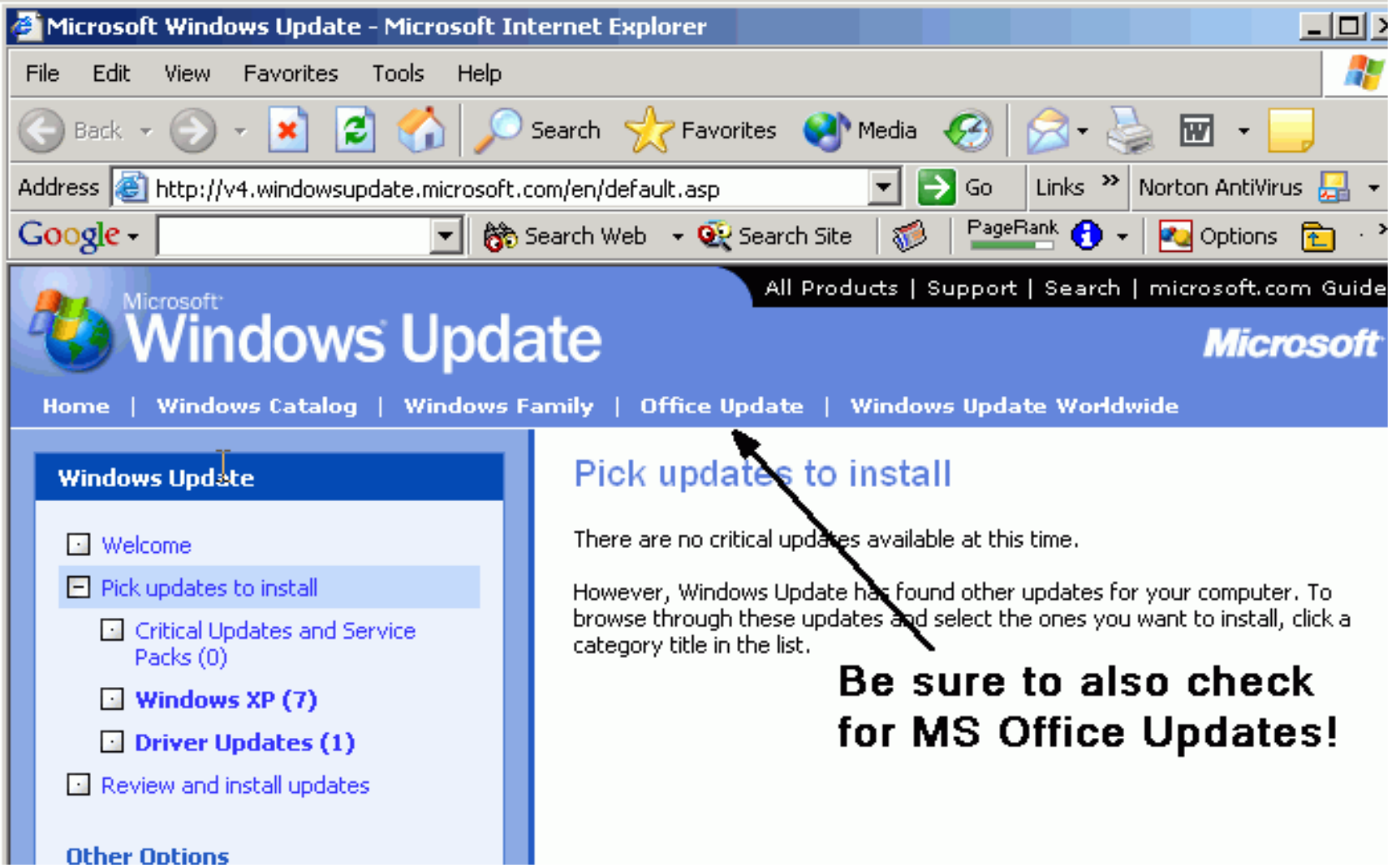
- One option is to request a copy of the free MS Security Update CD by mail (allow two to four weeks for delivery; you *may* have enough time to download the patches during that time :-)); see: http://www.microsoft.com/security/protect/cd/order.asp
- Alternatively, install a personal hardware firewall or a personal software firewall (such as ZoneAlarm), and ONLY THEN connect the host to the network to get critical updates. (No firewall? You will be infected in just seconds!)

Windows Update



If you <u>don't</u> see this menu item, just use Internet Explorer to go directly to http://windowsupdate.microsoft.com/

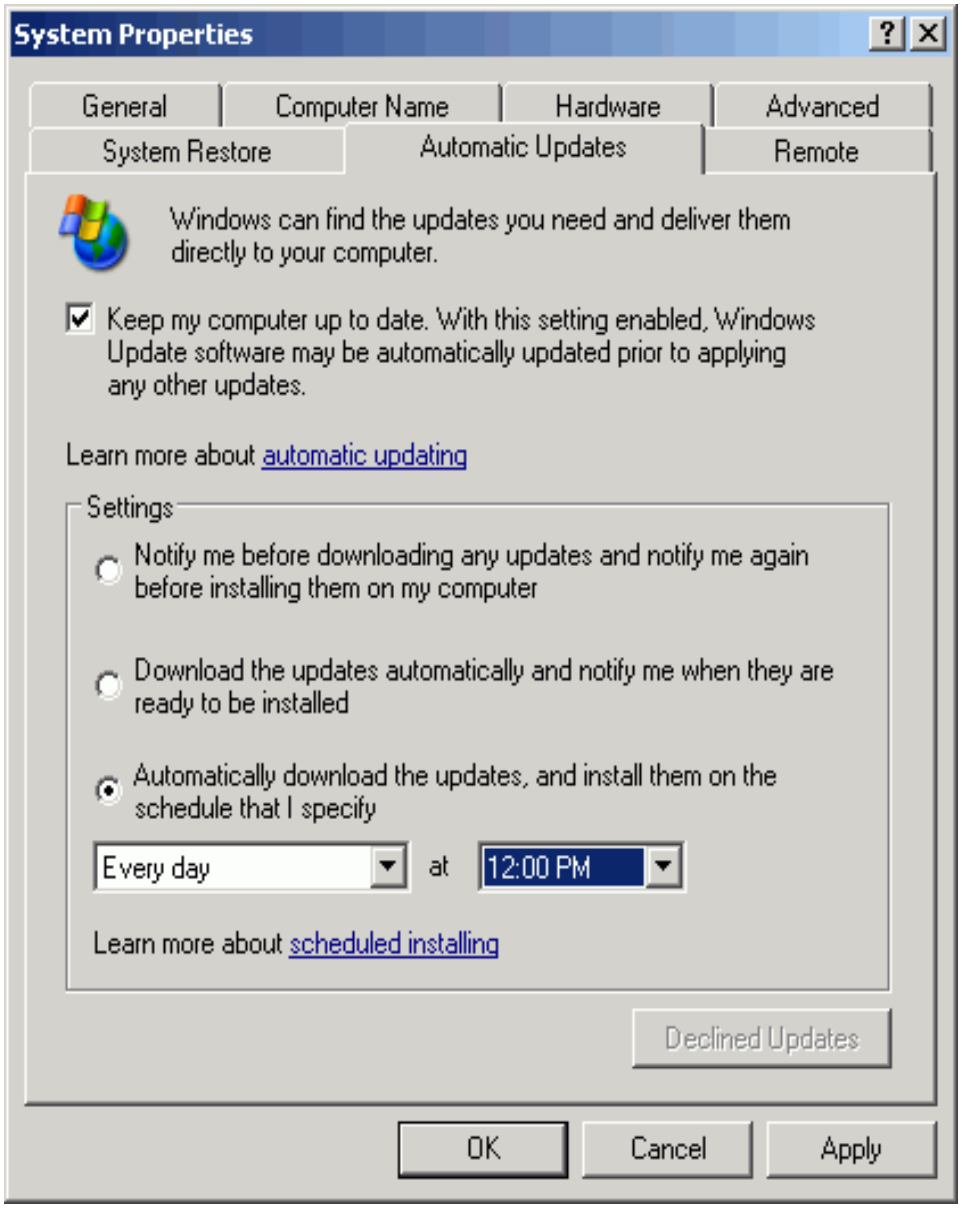
After Updating Windows Itself, Be Sure to <u>Also</u> Check for MS Office Updates



Enabling Automatic Windows Updates For Future Critical Updates

- Start → Settings → Control Panel → System → Automatic Updates Tab → Click on "Keep my computer up to date." Select "Automatically download the updates, and install them on the schedule that I specify." Choose "Every day" and pick a convenient time when your computer will be powered up and on the network. (multiple machines? Stagger the times) Periodically run Windows Update manually just to make sure nothing's "broken."

That Magic Automatic Windows Update Screen



Note Well: Automatically Applying Patches Is Not Without Its Own Risks

- I've personally had three production W2K servers get blown off the air by a single automatically-applied updates (thankfully all three were subsequently recoverable via SFC /SCANNOW). Trust me when I tell you that automatically patching can be risky.
- I highly recommend you read "Patch and Pray" http://www.csoonline.com/read/080103/patch.html ["It's the dirtiest little secret in the software industry: Patching no longer works. And there's nothing you can do about it. Except maybe patch less. Or possibly patch more."]

Trust, But Verify

- Scan your own networks to make sure users are patched up to date… Microsoft has tools at http://www.microsoft.com/technet/security/tools/default.mspx
- Commercial scanning products are also available, and may probe more for additional vulnerabilities/issues; nice review of some options at http://www.pcmag.com/article2/0,4149,1400225,00.asp (Dec 30, 2003)

There's More to Basic Windows Security Than Just Getting Critical Updates Done!

- Once you've gotten your system up-to-date in terms of critical updates, you are not done; there are many additional important things you should do to harden your Windows system.
- A brief list of the top vulnerabilities to check and correct is at http://www.sans.org/top20/
- For a detailed study, see: *Microsoft Windows Security Inside Out for Windows XP and Windows 2000*, Microsoft Press (800 pages).
- **http://www.columbia.edu/kermit/safe.html**

3. Worms and Viruses

- You can't open the paper without seeing reports of a new virus – Blaster, Welchia, Nachi, SoBig, MyDoom, Beagle, Sober, Netsky – the impact of these viruses on the Internet at large has been devastating…

"Computer experts called 2003 ''the Year of the Worm.'' For 12 months, digital infections swarmed across the Internet with the intensity of a biblical plague. It began in January, when the Slammer worm infected nearly 75,000 servers in 10 minutes * * * The computer-security firm mi2g estimated that the worldwide cost of these attacks in 2003, including clean-up and lost productivity, was at least $82 billion (though such estimates have been criticized for being inflated)."
"The Virus Underground," The NY Times, Feb 8, 2004
http://www.nytimes.com/2004/02/08/magazine/08WORMS.html

Site License An Antivirus Product

- Do you have a site license for an antivirus program covering all of your users? You MUST do so. This is another absolutely non-optional security measure.
- Be sure your people keep their antivirus definitions up to date! Be sure they use their AV software both at work AND at home! Antivirus software with stale definitions, or antivirus software that's used only at some locations, is a recipe for disaster.

Some Antivirus Vendors

- UO currently site licenses Norton Antivirus from Symantec, however, there are also other commercial antivirus programs you should evaluate, including…
  http://www.grisoft.com/
  http://www.kaspersky.com/
  http://us.mcafee.com/ (caution: pop up ads!)
  http://www.sophos.com/
  http://www.symantec.com/
  http://www.trendmicro.com/

Some Free Antivirus Products for Home Use

- Avast! 4 Home Edition
  http://www.avast.com/i_kat_76.html
  (free for home use)
- AVG Free Edition
  http://www.grisoft.com/us/us_dwnl_free.php
  (for single home users, cannot be installed on servers, cannot be installed in a networked environment; the do also offer a 30 day free trial download of AVG 7.0)

Viruses Delivered By Email

- Does your company use a program on your email servers to strip executable attachments and zip files from incoming email? If not, you should.
  One popular tool used for stripping dangerous executable attachments running Sendmail is the Procmail E-mail Sanitizer. See: http://public.planetmirror.com/pub/impsec/email-tools/procmail-security.html
- Commercial A/V gateway software products are also available from the usual suspects. :-)

Handling The Viruses That Get Detected

- If you do have a program that strips viruses from incoming email, is it smart enough to NOT send misdirected "you've got a virus!!!" warnings to thousands of forged From: addresses every day?
- Bogus virus warnings can be a bigger problem for your users and neighbors than the actual viruses themselves…

Risks of Sending Bogus AV Notifications

- In fact, the problems associated with bogus antivirus notifications have become so severe that some sites have begun to automatically block all email coming from sites that have broken antivirus gateways.
- See, for example the 127.0.0.9 code at http://www.five-ten-sg.com/blackhole.php and http://www.attrition.org/security/rant/av-spammers.html
- Educate your antivirus software vendors!

4. Antispyware

- In addition to viruses, another category of malware that you should know about is "spyware."
- Spyware, also called "adware," can hijack your web browser, violate your privacy, and inundate your computer with advertising. Recent estimates are that ~5% of hosts may be infested. (http://www.newscientist.com/news/news.jsp?id=ns99994745)

Coping With Spyware

- Make sure your staff and users have and use anti-spyware software – it is fully as important as antivirus software these days. A variety of anti-spyware packages were recently reviewed by PC Magazine; see: http://www.pcmag.com/article2/0,1759,1523357,00.asp (2 Mar 2004)
- One particularly popular anti-spyware program at UO is Spybot Search & Destroy from http://security.kolla.de

Some Anti-Spyware Tips

- Coverage across products won't be perfect; use multiple products to cover the "corner cases" any single anti-spyware product may miss.
- To help avoid getting spyware, avoid P2P applications, instant messaging applications and the files shared via those channels.
- If all you're seeing are ads popping up on your display, be sure Messenger is disabled; see: http://www.stopmessengerspam.com/

5. Spam and Security

- Yet another security risk your company faces is spam, or unsolicited commercial email. (Yes, spam *is* a security issue, not just a huge irritation.)
- To understand the relationship between viruses, hackers and spam, see the excellent discussion at "Spammers, Hackers Increasingly Feed Off Each Other," http://www.techweb.com/wire/story/TWB20040212S0009

What About Legislative Efforts?

- The Federal governments here in the US has made dealing with spam a priority, and has passed "The CAN-SPAM Act;" see http://www.spamlaws.com/federal/108s877.pdf
- Oregon, like 35 other states, also passed its own state anti-spam bill, SB910 http://pub.das.state.or.us/LEG_BILLS/PDFs/ESB910.pdf
- So far, despite all those new laws, the spam problem shows no sign of abating.

So Just How Bad Is It?

- If you're like many sites, 70 to 80% of all the emails sent to your users are spam. (see, for example: http://www.postini.com/stats/)
- You can block the vast majority of that spam by using suitable "DNS black lists" (here at Oregon we use and recommend the MAPS RBL+ from www.mail-abuse.org, along with the SBL+XBL from spamhaus.org, plus the NJABL open proxy DNSBL – that combination works very well for us.

Some Costs of NOT Blocking Spam…

- "Spam costs $20 Billion Each Year in Lost Productivity," http://www.technewsworld.com/perl/story/32478.html (12/29/2003)
- [If you think about all the prescription medication spam you and your employees receive, the following sort of reports should be particularly disturbing...]
  "FDA and Johnson & Johnson Warn Public About Counterfeit Contraceptive Patches Sold Through Foreign Internet Site"
  http://www.fda.gov/bbs/topics/NEWS/2004/NEW01017.html
- "The e-mail, which asks people to "update" their personal information - Social Security numbers, dates of birth, passwords and the like - or tells a well-concocted tale meant to trick people into divulging their credit card and bank account numbers, comprises more than half of the 15,000 monthly citizen complaints filed to the FBI's Internet crime center. The fraud schemes have become the single most prevalent crime on the Internet, experts say, and they have become markedly more sophisticated over the past few months."
  http://www.baltimoresun.com/news/nationworld/bal-te.journal13feb13,0,4731528.column
- See also: "National and State Trends in Identity Theft, January-December 2003", http://www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf

What About Content-based Spam Filtering…

- The main alternative to using DNSBLs is content-based spam filtering. One such popular application is SpamAssassin (see: http://www.spamassassin.org/index.html)
- While it is certainly tempting to take technical steps to insure that you never get porn spam or another email offering to enlarge particular body parts, we believe content based spam filtering scales poorly and can cause unpredictable delivery issues.

Handling False-Positive Filtering Issues

- Spam filtering, while now essential, will occaisionally block messages that are genuinely wanted ("false positives").
- When your company does spam filtering, be sure to allow users to opt out of default filtering if they want to do so. (While users can opt out of the default filtering on UO's large shared systems, so far only about 50 users out of ~42,000 have done so). Few may opt out, but having the option available is as an important "safety valve."

The Mail You (Try) to Send

- One last spam/email-related issue that should be "on your radar:" mail YOU send may not be getting through, and you may not even know it.
- For example, if you have your own network address block, you should ask to be sent AOL SCOMP spam reports for your network. See: http://www.nanog.org/mtg-0310/spam.html]
- Are your mail servers listed on the OpenRBL? http://www.openrbl.org/

Sustaining Your Email Deliverability

- Be sure your IT staff gets and acts on complaints sent to abuse@<yourdomain> [See http://www.rfc-ignorant.org/]
- Be sure the network provider you use isn't infested with spammers. See the ISP listings at http://www.spamhaus.org/sbl
- Investigate use of Sender Policy Framework (see: http://spf.pobox.com/)
- Send plain text, not html or attachments.

And If Your Company Does Routinely Do Large Mailings…

- Be sure your mailings comply with emerging industry practices (see, e.g., http://www.isipp.org/standards.php)
- Consider trying BondedSender (https://www.bondedsender.com/)
- "Test send" your draft messages to a user who is running SpamAssassin (see http://www.spamassassin.org/)
- BE SURE your mailings comply with the letter and the spirit of all antispam laws.

6. Software and Hardware Firewalls

- Some of you may have a hardware firewall installed at the border of your network. That firewall's fine, but no longer where it needs to be – the way some recent worms have ripped through large networks have made that clear. See, for example, "Picking At a Virus-Ridden Corpse: Lessons from a Post-Blaster, Post-Welchia, Post-Nachi, Post Mortem," http://www.syllabus.com/news_issue.asp?id=153&IssueDate=9/18/2003

Desktop Firewalls Are Needed

- You should be looking at per-workstation software firewall products (or inexpensive personal hardware firewalls, such as those from Linksys), instead of (or in addition to) your border firewall, much as you currently deploy anti-virus software on each desktop. This is routine practice on residential broadband networks; the rest of us need to catch up.

One Bit of Good News…

- The next major update for Microsoft Windows XP will have Microsoft's integrated Windows Internet Connection Firewall (ICF) "on" by default. This will make a huge difference for your Windows XP users (assuming they install that update!), however don't lose sight of the fact that most sites typically have systems running many earlier versions of Microsoft Windows (which lack the ICF).

Some Notes About Software Firewalls

- Note that many "free" software firewalls aren't actually licensed for free use by businesses!
- If using a software firewall, beware of ongoing maintenance costs.
- Novice users can also easily be confused when it comes to making decisions for software firewalls about what applications to accept or block.
- One review of personal software firewalls: http://grc.com/lt/scoreboard.htm

Notes About Hardware Firewalls

- Hardware firewalls can be installed "backwards," in which case they can act as a rogue DHCP server, handing out RFC1918 addresses to everyone on their subnet.
- Some hardware firewalls may use uPnP if not carefully configured: http://cc.uoregon.edu/cnews/spring2003/upnp.html
- Some hardware firewalls may come bundled with wireless access points (which have their own security issues)
- Reviews? See: http://grc.com/lt/hardware.htm

One Unexpected Consequence of Deploying Desktop Firewalls

- There is one unexpected consequence of deploying desktop firewalls that you should be aware of: once you deploy a desktop firewall, particularly if you deploy a software firewall product, you and your staff will be amazed by just how often your systems are getting probed. The level of ongoing "background radiation" associated with hacker/crackers activity can be fairly shocking.

7. Passwords

- Once you know how often hacker/crackers are "poking" at your systems, the importance of strong system access controls becomes much more understandable, although most companies, like most universities, still rely on usernames and passwords (rather than hardware crypto tokens or other advanced authentication solutions), largely because of the cost of those alternatives ($60 to $70 per token or more).

Regular Passwords Aren't Really "Free"

- Gartner estimates that up to 30% of calls to a typical helpdesk are password related. (http://www.nwc.com/1317/1317f13.html)
- Estimates for the cost/call vary widely, but let's hypotheticall assume you use comparatively inexpensive interns, and peg that cost at $5/call (it is probably far higher when you think about the lost productivity of the employee with the password problem). How often do YOUR users forget/need to have their passwords reset?

It might make sense to look at more secure alternatives…

- When you factor in the actual costs of using "free" passwords, and the improved security that hardware tokens or other advanced methods can offer, it might make sense to begin moving away from plain passwords. A nice discussion of some of the issues is available at http://www.giac.org/practical/GSEC/Lawrence_Thompson_GSEC.pdf

If You're Stuck With Passwords

- Do you insist that your users choose a strong password? (If at least some users aren't complaining, those passwords probably aren't as crack resistant as they should be)
- Do they require users to periodically change their password? How often?
- How do passwords get assigned and distributed? How do they get reset if forgotten?

Protection of Passwords with Encryption

- One direct theat to password based authentication is “sniffing” (evesdropping on passwords while they’re transmitted over your local network or the Internet).
- Has you taken steps to replace plain text services with their encrypted analogs? UO now has, both for interactive logins (“telnet”) and for POP/IMAP. After we changed, the services worked the same from the user’s perspective, but now they’re resistant to evesdropping…

8. Wireless Security

- Speaking of encryption and avoiding sniffing, this is a particularly important concern if you have wireless networks.

  If you don't believe this is an issue, review some of the wireless sniffing tools mentioned at http://infosecuritymag.techtarget.com/2003/apr/sniffingair.shtml

Wireless Can Be Used in Some Critical Spots

- ‘Paul Blomgren […] measures control system vulnerabilities. Last year, his company assessed a large southwestern utility that serves about four million customers.“ Our people drove to a remote substation," he recalled. "Without leaving their vehicle, they noticed a wireless network antenna. They plugged in their wireless LAN cards, fired up their notebook computers, and connected to the system within five minutes because it wasn't using passwords. […] Within 15 minutes, they mapped every piece of equipment in the operational control network. Within 20 minutes, they were talking to the business network and had pulled off several business reports.’ http://www.memagazine.org/backissues/dec02/features/scadavs/scadavs.html

Wireless Security Is Very "Hot" Right Now…

- "Evolution of Wi-Fi in Academia" http://www.ncne.org/training/techs/2004/0125/presentations/0104radulovic2_files/v3_document.htm
- "Wireless Security" http://www.ncne.org/training/techs/2003/0803/presentations/pptfiles/0803-elliott1.pdf
- … there was even a March 1, 2004 NWACC Wireless Security Workshop in PDX: http://www.nwacc.org/conferences/wirelesswkshp.html

One Solution for Wireless Access Control

- UO is currently deploying ReefEdge (see http://www.reefedge.com/) to handle authentication and access control for its wireless network (see http://micro.uoregon.edu/wireless/)

Some Pages With Suggestions For Configuring Your Wireless Access Point

- "Four Steps You Need To Take," http://www.linksys.com/edu/page10.asp
- "Exploiting and Protecting 802.11b Wireless Networks," http://www.extremetech.com/article2/0,1558,1152933,00.asp

9. System Integrity

- One often overlooked area is verification of system integrity/detection of unauthorized changes to key system files.
- A nice discussion of some “tripwire” type products is available at: http://cc.uoregon.edu/cnews/fall2003/sysintegrity.html
- If you find files have been changed w/o authorization, I suspect you will suddenly be interested in…

10. Backups

- Modern data storage methods (storage area networks/network attached storage (SANs/NAS)) can help improve the survivability of your data by automatically mirroring it across multiple locations, but backups, particular backups of data on desktop systems remains a major problem at many sites. Most users simply don't bother backing up their desktop systems! Do your users? Are you sure?

Some Backup Suggestions

- "Hard Drives: Bigger, Faster, Cheaper-- and Less Reliable" http://cc.uoregon.edu/cnews/winter2004/hdrives.html
- Be sure backups are actually usable! When you need 'em is not the time to find out there's been a systematic problem for "some time!"
- Keep as many versions as you can afford
- Keep at least some backups off site.
- Guard backups the way you would original online media (watch privacy issues)

11. Physical Security and Survivability

- One of the reasons why you want backups is so that you have the ability to recover in case of a catastrophic event, like a data center fire.
- Are you protected against even trivial physical threats (like a disgruntled former employee equipped with a can of gas and a sledge hammer or pry bar)?

Major Fires Have Happened At Large Data Centers

- "[Update 20/11/2002 12:30]
  At this moment the ICT-heart of the university of Twente is burning. The so-called TWRC-building houses the central systems of the university, all servers and PCs will be lost and various affiliated institutes are without Internet connectivity."
  http://www.merit.edu/mail.archives/nanog/2002-11/msg00535.html

Some Physical Security Considerations

- Do you have a real (rather than just *pro forma*) disaster recovery plan?
- Do you have the ability to log who's coming and going from your building after hour, and from your machine room? Do you check those logs and investigate any anomalies?
- Do you have security cameras in place?
- When was the last time your building was rekeyed? Have any masters or submasters been lost since that time?

Some Physical Security Considerations (cont.)

- Have you tested and serviced your main UPS and emergency generator?
- The fire suppression system?
- How is surplus equipment disposed of? Are hard drives removed and destroyed?
- How is your trash disposed of? (See "Dumpster-Diving For Your Identity" http://www.nytimes.com/2003/12/21/magazine/21IDENTITY.html?pagewanted=all -- note that story is written about Eugene!)

12. SCADA Security

- One area we don't have time to get into today is SCADA (supervisory control and data acquisition) security.

- "Of particular concern to the task force, however, is the existence of direct and remote links between corporate networks used at utilities and the real-time SCADA systems used to manage the power grid. Until now, the electric industry has refused to publicly acknowledge these linkages and the vulnerability they pose. But the task force report puts SCADA system security at the center of the industry's most pressing security challenges."
  http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,87400p2,00.html (November 20, 2003)

Some SCADA Readings

- "21 Steps to Improve Cyber Security of SCADA Networks" http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf
- "Critical Infrastructure Protection: Challenges in Securing Control Systems" http://www.iwar.org.uk/cip/resources/gao/d04140t.pdf
- http://modbusfw.sourceforge.net/

Conclusion

- Thanks for the chance to talk today!
- Are there any questions?