



National Webcast Initiative Performing a Cyber Security Risk Assessment: Why? When? and How?

October 19, 2004
Question and Answer Transcript

The following is a compilation of questions submitted to the presenters through the written Q and A tool during the webcast. The transcript has been edited for relevance.

Q: *Most of the community doesn't think that these guys ever get caught! Why aren't these publicized?*

A: Although they are reported in the media they typically don't make the front page. In some cases details about the individual can't be reported due to the hacker's age.

Q: *In what court was Lamo prosecuted? I want to some of the court docs.*

A: Manhattan Federal Court. See <http://www.cybercrime.gov/lamoPlea.htm> for more information.

Q: *You mentioned lad & lassie script kiddies. Traditionally hacking has been a male phenomenon. Are we seeing females starting to get into this?*

A: Within computer culture, and especially hacker culture, women are rare. The most famous female hacker went under the pseudonym Susan Thunder. You can read about her and other women hackers at:
<http://home.c2i.net/nirgendwo/cdne/ch14web.htm>

Q: *Are keystrokes recorded or must the hacker note them in real time?*

A: Keystroke Loggers in short, record all input or activity performed on from the keyboard generally dumped to a log file. There are software based keystroke recorders for almost every operating system.

Q: *Is one safer behind a NATed firewall and "always on" or on a dial up (temporary on) but not NATed?*

A: NAT'ing was really designed to allow multiple internal computers to share one external IP address because external IP addresses are getting scarce. As a side

benefit NAT'ing does help hide details of your internal network such as the number of computers.

Q: *For a home user...Is there a difference in protection when using Internet DSL or Internet cable service?*

A: No there is no difference. A firewall and anti-virus product, updated at least weekly, is strongly recommended in both cases.

Q: *Are Macs any safer than Windows?*

A: Modern Macs are Unix computers. Each time you install an application under Mac OS X, you have to give the operating system permission to do that. (You're told to type a password. Without the correct password, nothing can be installed.) When there are new security problems, the Unix code in OS X is open to inspection and relatively easy to change.

Q: *How often should we update our protective devices? Every time we turn the machine on?*

A: At least once a week

Q: *Do Zone Alarm and Ad-Aware in conjunction with one of the leading virus packages provide sufficient protection?*

A: Yes, as long as you update them and run them frequently. However, nothing is 100%. In addition, you should keep your software updated with the latest security patches.

Q: *I work in tech support for a university. Do you know of resource(s) for us to get credible speakers to present cyber security information to the campus community?*

A: You may wish to contact EDUCAUSE, a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology. Website: www.educause.edu.

Q: *What is the Best Anti-Virus Program?*

A: There are a number of good anti-virus software programs available. For some related links, you may wish to visit <http://www.cscic.state.ny.us/related.htm>. However, your individual or organizational needs will dictate the solution that is best for you.

Q: *Is there a way to stop spoofing?*

A: The vending community is currently working to address this issue.

Q: *If a home computer is not secure is the home user legally accountable?*

A: At present there are no specific Federal statutes which would appear to hold a home user to specific standards of care. However, all users benefit from strict adherence to best practices such as those suggested in today's presentations.

Q: *Is there a good website to look at for assistance in developing an IT security policy/plan?*

A: You may wish to visit the National Institute of Standards and Technology at www.nist.gov and the SANS Institute at www.sans.org.

Q: *Can a router block all activity from the outside?*

A: Yes, a router can be configured to block all inbound traffic. However, you should also consider blocking unauthorized outbound traffic too. If your computer is compromised through another means (e.g. email virus) it will try to connect to the Internet to allow someone to remotely control it.

Q: *Can you utilize more than one antivirus system simultaneously? For ex. Microsoft and McAfee?*

A: It is generally recommended that you use one since multiple versions may conflict with one another.

Q: *How can you check if malicious programs already exist on your computer?*

A: Run a complete scan of your computer using current anti-virus and spyware software.

Q: *Are other broadcasts, more specific to organizations such as Homeland security, going to be done? Or can we request such?*

A: The National Webcast Initiative will be offering webcasts on a variety of topics. Upcoming schedules will be posted on the web at:
<http://www.cscic.state.ny.us/msisac/webcasts/index.htm>

Please feel free to forward any suggestions for upcoming sessions to:
isac@cscic.state.ny.us.

Q: *Are all of the "online virus scanners" and "online system scanners" that are available on the internet today (and usually use ActiveX controls) helpful or harmful? Allowing remote code execution through a browser control is something that in my mind should be discouraged... not encouraged.*

A: These are just another "tool in the arsenal" but should not replace local anti-virus software. Not all activeX, JavaScript, etc. is harmful and turning it all off sometimes breaks legitimate web sites. Bottom line is only allowing it for sites you trust.

Q: *What about looking for backdoors?*

A: The best approach today is the use of spyware and anti-virus

Q: *What site is best for reporting violations? What about reporting hackers?*

A: www.ftc.gov is a good site for reporting scams and phishing. Your local police, state police or FBI should be able to assist you. You can also report incidents to www.us-cert.gov

Q: *I was looking for the Real time, this was after I had some serious computer problems. After seeing this program I realized that I had a nasty virus of some kind. My fear now is that even after formatting my hard drive, is it really gone.*

A: Formatting your hard drive will definitely remove a virus. However if the vulnerability that allowed the virus to infect your computer is not resolved, re-formatting will not guarantee that you won't get re-infected. Make sure your computer has updated anti-virus, anti-spyware, a firewall and the latest security fixes.

Q: *Any specific software that detects worms?*

A: A worm is a type of virus that spreads on its own. All the anti-virus software products also detect known worms.