Global Information Assurance Certification Paper

Network Security on a Shoestring

While many magazine ads and glossy brochures tout the need for high buck, high end, cant live without security solutions, there are many small to mid-sized organizations, non-profit organizations, or as in my case, school districts that just cant afford to pony up that kind of money for the big shiny boxes with lots of lights, bells and whistles. The purpose of this paper is to introduce some simple, effective, cost efficient ways to implement basic network security practices. These basic steps should also be used as a starting point for organizations that are just beginning to roll out their security infrastructure.

The process can be broken down into three distinct areas:

1) What can *I* (or my department) do?
2) What can my *manager* do?
3) What can the *end user* do?

What can I do?

This is the area that you have the most control over. The first step is to gather information. What is at *risk* (data, physical assets, etc)?[1] What are the *threats and vulnerabilities* (exploits from the internet, internal sabotage, end user errors, etc)? What will it cost me in time to repair/restore damaged or lost data? What would it cost my company is lost revenue due to down time or lost business due to lack of confidence of customers? Could a loss or downtime result in a lawsuit? These are all questions that need to be answered and documented. These issues will help your case when trying to allocate more funds or resources to the security cause.

The second step is assessing and documenting your physical and logical network layout. How many entry points are there from the Internet? How many internal subnets? How are they separated?

Now lets get to work. Lets assume for a moment that you anticipate your greatest threat is from the outside. From this point, talk to your ISP and find out what, if anything, they do to protect *you* from the bad guys. Do they block incoming ICMP traffic or broadcast traffic? If not, ask why not. Check your own boarder routers – are the default login passwords changed? Are the default SNMP community strings changed? Are you blocking incoming ICMP traffic and broadcast traffic? Are you using access lists to only allow the traffic that needs to come and go through your router? Do you have any unnecessary ports open? Contact your vendor for more information on how to check these parameters. These are the first steps to keep the intruders off your doorstep.

Do you physically lock your servers and electronics in a room or closet? Physical security of network assets is a must, not matter what the operating system. Also lock the keyboard/console when not in use. Many exploits require that the attacker have access to the server console (either locally or remotely). Have you either changed or removed the

default Supervisor/Administrator user or password? Have you applied the latest patches for your hardware and OS? Have you checked for security updates to the IOS on your network electronics? Do you audit failed login attempts (and if so DO YOU CHECK THE AUDIT LOGS regularly)? Do you enforce intruder lockout on all your user accounts? Do you have any kind of security on dial in access (such as authentication, call back, etc)? Do you have periodic data backups? Do you have/use tools to check password strength (be sure to get permission from management before using!).[2]

There are several shareware and freeware programs available to assist you in tightening up your security[3]. You can get port scanners to run against parts of your network to see if either you have left open unused ports on servers, workstations or electronics – or maybe someone else has opened a port for a current or future compromise. Use them! (after getting permission from your superiors). There are also inexpensive host based firewall solutions that can be applied to servers and workstations to provide at least a basic level of protection. Use them! Some companies will let you download an evaluation copy to test and see how they can be used and configured. These can also give you basic intrusion detection (IDS) capabilities.

Although often overlooked in the smaller companies, a security policy will ensure that both *you* and *your network* are safer. Security policies should include such things as

- How often user passwords are changed
- Is there a minimum password length?
- Do you require hard to guess passwords
- What's the process for removing a user after leaving the organization
- How long does an unused user account remain until deleted
- Acceptable use of the network resources and email systems
- What's the procedure for reporting suspicious activity (possible virus, social engineering attempts, etc), both by end users and IT staff
- Who's responsible for virus updates
- Are users required to secure their workstations before leaving them (logging off, power off, etc)
- Are users forced off the network periodically (nights, weekends, etc)
- Does every user have their own unique network username and password

A good security policy is beyond the scope of this document, but there are many places on the web that offer assistance in this area[4]. A security policy is something that your management will have to buy into and promote.

Although you can do all these things mentioned above, enforcement of any policy or procedure is for naught if management doesn't buy into the reality of network security exploits. In addition to the above-mentioned items, part of your job (perhaps the most important part) may be having to convince upper level managers that network security needs to be taken seriously. This is where your risk assessment comes in handy. Use this

and some examples of common, highly visible, recent exploits to drive the point home (such as the Microsoft or EBAY hacks.).

What Can My Manager do?

Management buy-in of network security matters is crucial. They will be the ones leading the charge to the rest of the company about security, as well as the ones who put the teeth into and enforce the security policy. If they don't enforce the fact that users should change passwords periodically, or secure their workstations when not in use, then it's a useless policy. They can also assist you in setting up user awareness training and help you navigate the politics of the organization.

What Can End Users Do?

Some of the best, and cheapest, defenses against the hacker can be implemented at the user level[5].

- Don't share user names or passwords
- Don't open unsolicited or suspicious email without verifying from the source
- Don't leave the workstation open and unattended
- Use hard to guess passwords
- Change passwords frequently
- Keep the virus software updated
- Report ANY strange or unfamiliar behavior of the workstation.
- Don't succumb to social engineering! Verify identity before giving pertinent network information

The real key to getting the support of the end user is awareness. They need to understand that there is more at stake then just losing something in their user folder on the network. An "awakening" program that shows the users what can really be compromised or destroyed on the network with just their username and password helps to meet this goal. The end user needs to take ownership of their piece of the network and truly understand and believe that serious damage and loss can occur in the network, even through their doorway.

In Conclusion

Do whatever you can do on the piece of the network over which you have control and keep on top of it. Get managers to realize that network security is a real issue, not just paranoia. End user awareness will be your biggest ally in the war against the "black hats". In short, implementing effective network security everyone's responsibility, not just the IT staff!

Lastly, stay informed! Subscribe to online weekly and monthly reporting tools such as NTBUGTRAK or the SANS digests[6]. Get a monthly subscription to any one of a number

of network security periodicals. Join (or start) a local network security "users group". New exploits and hacks come out daily and we must attempt to keep on top of them.

SANS offers two very good documents on network security at this level. The URL's are http://www.sans.org/ddos_roadmap.htm and http://www.sans.org/newlook/resources/esa.htm

[1] Some information on risk assessment can be found in the SANS reading room at http://www.sans.org/infosecFAQ/risk.htm

[2] The Sans Institute. "Windows NT Security Step by Step" Version 2.15. July 30, 1999

[3] Some common scanning/hacking tools (and other "tools of the trade") can be found at http://www.hackingexposed.com/tools/tools.html

[4] Sans offers a guidline to creating security policies at http://www.sans.org/newlook/resources/policies/policies.htm

[5] http://www.sans.org/mistakes.htm

[6] http://www.ntbugtraq.com/ and http://www.sans.org/newlook/home.htm

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS