Global Information Assurance Certification Paper

Twists in Security for Law Enforcement

Overview

Although computer security, at its base, is similar for businesses, government, home users, etc., there is a bit more that is involved for supporting law enforcement agencies. This paper is an attempt to not only briefly cover the basics of computer security that should be in use by everyone, but also an attempt to introduce to those unfamiliar with the extra challenges of supporting law enforcement what additional computer security precautions need to be addressed. This is by no means an exhaustive list, but an overview that includes some points of concerns, some ways they are currently being addressed, and a few insights into other ways to provide the needed computer security. As a person who was just recently given the responsibility of computer security in an environment that supports public safety after having been a server administrator, I too, need to learn the many additional challenges that I now face.

Many of the larger law enforcement agencies (the FBI, many major metropolitan police departments, etc) have their own direct computer support staff. This allows the computer support staff to have a limited user base that isn't quite as diverse as some other organizations may be. This also allows the staff to be more intimately involved and trained in the specifics of having to deal with the computer security challenges.

The Basics

Perimeter security between the internal network, the Internet and/or other organizations is a must. Although defense in depth is one of the "best practices", a firewall is a minimum. For larger organizations, firewalls between sensitive parts of the internal network is highly suggested. A benefit from this defense in depth will be the fact that even though an "unfriendly" may have gotten through the first line, there is still another that must be crossed before access to sensitive data, such as financial, human resource or other information is achieved. Having a proper configuration is also a must. It wouldn't matter if you had a firewall in place if your access rules permitted all traffic in both directions. This type of information can be found at various places on the web (see table 1), from the manufacturers documentation & from the many classes that are offered about firewalls at training centers & training companies.

Manufacturer/OS	Web site(s)
Cisco	http://www.cisco.com/warp/public/707/index.shtml
Linux	http://www.linux-firewall-tools.com/linux/
AS/400	http://www-1.ibm.com/servers/eserver/iseries/software/firewall/tech_tips/tech_tips.htm

IBM eNetwork	http://publib-b.boulder.ibm.com/Redbooks.nsf/RedbookAbstracts/sg245209.html?Open
CheckPoint	http://support.checkpoint.com/public/publisher.asp?hotid=55.0.4222079.2607206
Raptor	http://www.firetower.com/faqs/

Table 1

One of the areas that sometimes is a bit overlooked when dealing with perimeter security is the many entry points that need to be addressed. It isn't going to do much good to have all the security concentrating on the connection to the internet if you have multiple unguarded access points elsewhere. Do you really know how many modems there are within your network? Do you have rogue wireless access points? Does your VPN software allow network connectivity not through the VPN while the VPN is established? Do your remote users have personal firewalls & virus protection software installed on the PC(s) they are using to access your network? Do you have vendors who plug into your network when performing demos or other business related work? If a user has a laptop stolen while on travel, can it be used to access your network? Once you have the gotten a handle on all of these, you will be significantly closer to having a secure network.

Virus protection is becoming a significantly more important security item as time progresses. The number of viruses is beginning to rise exponentially. Running a virus scanner on e-mail entering and leaving your network won't stop the user who brings in files from home on a floppy. To be covered, you need to have a virus scanner running for e-mail, on file servers, on the desktop & encourage users to have virus protection at home. At a minimum, have virus protection at the desktop. Because of the constant threat of new viruses, you also need to either have distribution of the virus signatures automated, or be subscribed to the bulletins of your anti-virus software manufacture and have a simple distributions scheme. Without the ability to quickly get new virus signatures to all of the scanners as soon as another virus comes out, you will still be unprotected.

Since the infrastructure depends on the devices that connect the system & provide the services that the users depend upon, keeping these boxes secure is another issue. One of the hardest things to do is to keep up with the myriad of software patches that are continually being released to close the holes that are constantly being found. OK, so you patched your Microsoft file servers, but what about the Unix boxes, the NetWare servers, the routers & switches, the workstation Operating Systems, the Internet browser, the e-mail software and the endless list of software running on the desktops. Make sure you are subscribed to one or more of the many security bulletin services that exist on the web (see table 2).

Organization	URL for subscription information

SANS	http://server2.sans.org/sansnews
Bugtraq	http://www.securityfocus.com/cgi-bin/forums.pl
CERT	http://www.cert.org/contact_cert/certmaillist.html
Sun	http://sunsolve.sun.com/pub-cgi/show.pl?target=security/sec
Microsoft	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp

Table 2

Hardening an OS and closing all the holes that exist, even after you have applied the patches that are available takes a skilled person to do. Since most of us aren't quite that good by ourselves, we need some help. There are quite a few books on the market to help, such as Hackers Beware & Hacking Exposed, just to name a few. There are also many places on the web where similar information can be found (see table 3 for a few). At a minimum, make sure that all security related patches are applied and the number of services that are running is kept to a minimum. Access to services & files should be limited to only those that are explicitly require by the user. Password defaults for length should be maximized and expiration length should be minimized in accordance with the criticality of the information on the server.

OS	URL
NT	http://www.sans.org/infosecFAQ/win/harden_NT4.htm http://secinf.net/info/nt/hard/hard.html http://www.networkmagazine.com/article/NMG20000515S0091
NetWare	http://www.sans.org/infosecFAQ/novell/exposure.htm http://secinf.net/info/nw/novak/1120ws1.html
Linux	http://www.sans.org/newlook/projects/bastille_linux.htm
Sun	http://www.sun.com/blueprints/0601/jass_quick_start-v03.pdf
OpenBSD	http://geodsoft.com/howto/harden/OpenBSD/services.htm

table 3

Even after all of this is in place, having an intrusion detection system (IDS) is important. Do you know if someone has beaten your perimeter defenses? Do you have a user within the network that is engaged in inappropriate activities? Although having an IDS is important, it will need someone to check it and follow up on what appears to be inappropriate activity. Be wary of the initial results, because many, if not all of the systems produce False Positives. You haven't got one yet and you're not sure what's out there? Check out http://www-rnks.informatik.tu-cottbus.de/~sobirey/ids.html. It lists 92 different systems and a

URL to access for more information.

You can have all of the above in place and somehow users still find a way to either circumvent the system or just plain mess things up. Having a security policy in place is important, but if the user community doesn't know what it is and it doesn't have the backing of upper management, it may be useless. User education is always an important part of a basic security plan/policy. Make sure that management buys into the security plan and that enforcement comes from the top.

Information Groups

As the number of computer related incidents (Denial of Service, Viruses, Hacker attacks) has risen, the need for the sharing of information has risen too. Groups like CERT,[1] SANS,[2] Bugtraq,[3] etc. have been formed to try and meet that need. The FBI came to realize that without a better way to share information, there wouldn't be easy ways to deter the incidents. The FBI also decided that this sharing of information needed to include private as well as public sector security professionals. This effort gave birth to InfraGard.[4]

> InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a cooperative undertaking between the U.S. Government (led by the FBI and the NIPC) and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States critical infrastructures.[5]

The FBI is working to provide not only a place that incidents can be reported, but also a forum to allow knowledge to be quickly passed and utilized. Many of the chapters now are bring forensic labs on-line. These will be made available to local law enforcement agencies to provide a location and controlled environment where forensics on hard drives can be done as evidence is gathered in preparation for prosecution.

Now for the twist...

---

[1] http://www.cert.org/faq/cert_faq.html#A2

[2] http://www.sans.org/aboutsans.htm

[3] http://www.securityfocus.com/

[4] http://stlouis.fbi.gov/contact/fo/sl/origins.htm

[5] http://www.infragard.net

To help law enforcement communicate better with each other and consolidate the locations where information is kept, the FBI created the Criminal Justice Information Services division (CJIS). One of the systems under this umbrella is the National Crime Information Center (NCIC). NCIC has consolidated the query of many databases and includes an enhanced name search, fingerprint searches, probation/parole information, mugshots, convicted sex offender registry, SENTRY file, information linking, other images, delayed inquiry, improved data quality, on-line manuals, & an on-line ad-hoc query capability.[6] NCIC, because of its sensitive nature requires additional security measures to safeguard. These include: physical security of the computer room that houses the servers accessing NCIC; screening of the personnel that will have access to the computer room or terminals/computers that have NCIC access; limitations of what terminals/computers can access NCIC; and logging of NCIC transaction with regular review of the logs.[7]

To address the additional security requirements of limiting what terminals/computers can access to NCIC, rather than just being protected with a username/password combination, many agencies are also requiring a registered TCP/IP address to access the system. Unfortunately, an IP address is easy to spoof. Security could be tightened by requiring either a token or some other key that would be specific to an individual, such as a hardware token that plugs into a USB port. Administrative controls should also be in place and followed up with training to all who may have physical access to terminals/computers that have NCIC access. Regular audits should be performed to verify that these security measures are properly in place and being followed. The security addendum referenced at http://www.capitolcitypublishers.com/news/jtech/FBIInfo.htm specifies that the FBI will perform bi-annual audits of each agency having NCIC access to certify that all security measures are consistent with guidelines.

Making these same services available to the officers in the field without always getting a dispatcher involved can significantly improve the efficiency of NCIC transactions. There are different methods for delivering these services to the patrol cars. One of the popular ones is a product from Aether Systems called PacketCluster which is deployed through a cellular digital packet data (CDPD) network. AT&T is one of the supported providers of PacketCluster on CDPD. To make this happen, there must be a connection to AT&T's frame relay system. This then brings some additional security concerns because it adds another entrance into your network. The best method for handling this would be to have the AT&T connection terminate on a DMZ on the firewall. This will make sure that the firewall rules that you have in place can be applied. Many organizations are also putting VPNs in place to augment security. Still more are making sure that the nodes on the CDPD network can only access the PacketCluster server and nothing else through router access control lists.

---

[6]http://www.fbi.gov/hq/cjisd/ncic.htm

[7]http://www.fas.org/irp/agency/doj/fbi/is/ncic.htm

Anyone who has to support a dispatch center is aware of the extra load that this brings because of the 24x7 operation. Imagine yourself as a dispatcher who is taking calls, guiding officers or other public safety personnel to a scene, looking up a criminal history on someone just taken into custody, and working the radio to keep in contact with everyone at the same time. It takes a special kind of person who can multitask well to be a dispatcher. All of the security needs to be combined because of the sensitive nature of the information handled. Imagine the damage that could result to public safety as a "Denial of Service" brings everything to a screeching halt. Separating the dispatch center network from the rest of the network and providing either duplicate paths to the NCIC server(s) or having another method for a backup way of accessing the NCIC information is important. These types of alternatives should be covered in a disaster recovery plan.

Freedom of Information Act

The Freedom of Information Act guarantees access of governmental records to the general population. Thanks to September 11, 2001, many hearty proponents of this act have taken a second look at the consequences. How much information do we want to readily publish that might be used by terrorists, or hackers for that matter?

Summary

If all of the measures discussed in this paper are in place, then most of the security requirements are already being met. Focus on the security of the terminals/computers with NCIC access can then be more easily achieved. Having a security plan in place that addresses all security measures required, along with regular audits that are performed internally before the FBI audits, will greatly reduce the chances of unauthorized access.

Resources

InfraGard
http://www.infragard.net/
http://www.iwar.org.uk/infragard/
http://usinfo.state.gov/topical/pol/terror/01010802.htm
http://stlouis.fbi.gov/contact/fo/sl/origins.htm

National Crime Information Center (NCIC)
http://www.govtech.net/magazine/reseller/1998/march98/product_watch/productwatch1.phtml
http://www.fas.org/irp/agency/doj/fbi/is/ncic.htm
http://www.njsp.org/tech/ncic2000.html
http://www.securitymanagement.com/library/000152.html

Criminal Justice Information Systems (CJIS)
http://www.fbi.gov/hq/cjisd/about.htm

PacketCluster
http://www.cerulean.com/wireless/patrol_info.htm
http://www.mobic.com/news/2000/03/cerulean.htm

Freedom of Information Act

http://foia.fbi.gov/
http://www.aclu.org/library/foia.html

Security Policies
http://www.sans.org/newlook/resources/policies/policies.htm
http://www.information-security-policies-and-standards.com/

Forensics
http://www.ddj.com/documents/s=881/ddj0009f/0009f.htm
http://www.porcupine.org/forensics/column.html
http://www.guidancesoftware.com/html/

Disaster Recovery
http://www.techrepublic.com/briefingcenter.jhtml?id=b975&fromtm=e019