Global Information Assurance Certification Paper

Integrating Security into Network Redesign

Marie Hubbard

GSEC v.1.3

Many businesses are discovering that the networks they built years ago are not capable of supporting the increasing requirements of today's electronic world. For the purposes of this paper, imagine that a security team has been directed to work with a larger team to combine all IT resources belonging to over 20 different departments. Each department had developed their very own network and most have highly integrated their business functions with custom designed cross application systems. There will be over a thousand servers involved with this consolidation, and that there are currently about 800 IT workers in the entire enterprise. It is up to the security team to make sure that any and all security issues are properly addressed during the redesign of a single department's network into a new IT network for the entire organization.

The following pages will briefly describe many of the issues needing to be addressed in such a situation. The logical beginning point is planning for the increased needs of the infrastructure. Then a process for integrating applications onto servers already on the IT network must be defined. The next step will be to ensure that application servers that will not be integrated with existing IT servers are securely configured before being integrated into the IT network. This will require a well documented testing and validation procedure. During this process the network intrusion detection system, if already in place, must be expanded to properly monitor the new network segments that will be added during this consolidation. There must also be a well-defined process for dealing with security incidences that may arise. Security policies must be developed to govern the operation of all servers on the enterprise, as well as to aid in enforcing the procedures on integrating servers onto the IT network. Last but not least, it will be very important to develop a good working relationship with all of the IT people who will be joining the consolidated IT department. Large network consolidations are not an easy task, and fairly important steps, like building security in from the foundation up, may be missed in the process.

Step one: Infrastructure Design and Network Management

Some resources state that network design should be decided from the top down, loosely following the IP stack. Business requirements dictate the applications that will be running the network, and the application requirements will drive the needs of the network infrastructure. Infrastructure decisions, however, are often said to be made from the bottom of the OSI model up. One must be careful not to let apparent business requirements force unsafe network practices. With that in mind, I propose that one must carefully attempt to predict the future business requirements in terms of types of applications, criticality of systems, and amount of network traffic generated by these systems. Then one must attempt to build a secure and scalable network infrastructure to serve as a foundation for your current and future network needs.

One way to think of designing a network is rather like designing a building. First, decide what type of building the business requires, a one or two story factory, or a skyscraper? The size of the business and the types of data it needs to work with can vary greatly. Once the building requirements have been identified, like how many floors (how large a network), what kind of layout for offices and divisions (VLAN/subnet strategy), whether to have exterior windows all around or thick solid walls (border router or hardened firewall peripheral defenses), these requirements will drive the kind of foundation (network infrastructure) that must be built. The foundation must also take into account the environment in which the building will be placed. Are earthquakes a concern (industrial espionage); is the building in a swamp (do hackers hold conventions next door)? There are many things that one must consider when building or re-designing a network, and to ensure that the network is as safe possible, security must be integrated from the ground up.

Network Design

In deciding what the network must support, it is important to analyze the current and future needs of the network. The future needs in the scenario described at the beginning of this paper would include the network needs and traffic of the departments that are to be absorbed into what will be called the IT department, and a best guess on how those needs will increase in the next few years. For any network re-design, the following bulleted topics should be considered before the network infrastructure is completely decided. Please remember that this is only a partial listing, and far more exhaustive listings will be included in my referenced materials.

- Types of Applications – Driven by business requirements

  Identify what the network will be expected to accomplish. The network should be capable of supporting the primary functions of the organization, not only at present levels, but it should be scalable to support the future expectations of the organization. If the organization provides educational resources over the Internet, it will likely need to be capable of supporting streaming video. Providing streaming video to large numbers of people at once requires a significant infrastructure investment, appropriate servers and storage facilities, and an absolutely reliable delivery mechanism. For instance, for Internet connections you would want extremely reliable Internet service.

- Identify the criticality and confidentiality ratings for the data on the network, and adjust the network design accordingly.
  It will be necessary to perform a risk analysis on the network systems. This consists of identifying the threats to the data, and how vulnerable the network is to those threats. After this analysis, adjust the network infrastructure plans and logical network design to build in heightened security where it is necessary, while allowing for necessary business functions to proceed without noticeable impact. For example, if the organization is a financial institution, and the future of the organization dictates the need to have

extensive interaction with customers over the web. It is a well-known fact that financial institutions that can be accessed through the web are prime targets for hackers. If there is not a firewall between the Internet and the data servers, the organization runs a very high risk of having the confidentiality, integrity, and availability of the data or any combination of these compromised. That makes for angry customers and bad press, both of which can prove very costly in addition to any direct monetary losses caused by the hack.

- Network Protocols necessary (Application requirements)
  Best security practices require that all unnecessary and unused services and protocols be disabled. After identifying what is necessary and what would not be appropriate in an entire network segment, many unnecessary protocols and services can be blocked at the networking level. For instance, http is not necessary on a router. It may be available for web-enabled management, but it is not necessary. Not allowing http on a management network can significantly reduce the vulnerability of routers to hackers. Another example would be SNMP. Many network and server management systems utilize SNMP, but the traffic need be only internal within that network. SNMP traffic should not be allowed in from outside your own network. It is necessary to have manageable network devices at the points where you would want to filter protocols.

- Security Requirements – design a secure model to address the needs of each type of system.
  Perform a risk analysis on each system or group of systems according to the criticality of the functions performed and the need to protect the data that is handled. A web server that holds nothing but pretty pictures doesn't need the kind of security measures that should be in place on a system that stores customer credit card numbers. A good way of addressing the security requirements on a large network is to create separate network segments connected with firewalls for each class of server. For example, for the financial institution network described in a section above, a recommended network design may include both a very carefully designed secure DMZ for the web servers, and a highly protected network VLAN for the database servers located behind another firewall that would only allow outside contact to be initiated by pre-determined web applications on specified servers, never by a user account or process that has not been pre-defined by port number. Non-critical web content servers could be placed in a less restricted DMZ with a more permissive firewall or border router at the outside perimeter, and no communication allowed to be initiated from those servers to systems in more protected network segments.

- Availability/Reliability requirements – driven by business requirements
  How important is it that a given system be available 24/7? How much down time is allowable when necessary, a week or less than an hour? If the

requirements are that the system be available 24/7 with no downtime allowed (this directive has been given in the past) then the administrator might wish to look into redundancy. This is a huge and very popular subject, and a thorough discussion is beyond the scope of this paper. Networking equipment manufacturers will be more than happy to help configure such a network, and they often have excellent information available on the web as well. Cisco and IBM have very impressive collections of documents on subjects ranging from network infrastructure design, the different LAN/WAN technologies, Quality of Service, multicasting, etc. Links to some of these sites will be provided at the end of this paper.

LAN/WAN considerations

Identify all categories of users and how they will interact with your network.

Employees
Partners
Customers
Physical locations of each type

The locations of those who need to have access to a network can have a tremendous effect on network design.

Network Management

While this may appear slightly off topic, it is included here because using these management tools greatly improves the administrator's ability to manage the speed, reliability and uptime of the entire network. These tools can be so integral to maintaining a network that if there is the possibility of replacing networking devices, one may want to take into account the management systems that can be used with the network equipment when making hardware decisions.

- Network device management tools can be platform specific, and help administrators fine-tune a network or identify problems before systems are affected.
- Server management systems can be platform specific, and allow the server administrator to be proactive in dealing with potential system failures. Some server management programs can also be used to manage centralized security logging, file integrity checking, and perform many other helpful security functions.

Budget – the final decision maker

There is a saying: "You can have it fast, cheap, or secure – pick two." (Notice that reliable and even functional are not mentioned.) Through very careful design planning and implementation, it is possible to do a lot more with limited funds than by just throwing things together and stopping when everything appears to work. Even when budget is not a limiting factor, it is important to note that if security requirements are not specified, then security will probably not be considered. This holds true for internal staff as well as outside contractors – if a contract does not specify all needs, then an organization may not get all that it pays for.

Step two: Application Integration
Even while the infrastructure is still being upgraded, work may begin on integrating outside department applications onto servers already on the IT network. The testing should actually be performed on a test network, which hopefully already exists as a resource in the IT department. It is actually best to have two separate test networks, an application test network and a security test network. An application test network can exist alongside the production systems, but simply not be in production. A good security test network will be completely separate from the production network, and contain enough servers and other networking equipment to allow careful configurations to mimic enough of the IT network to effectively test the security of an application or operating system. After the application is functioning properly on the application test network, it may be either transferred to the security test network or restored onto another server from a complete backup. Security vulnerability assessment tools should be run on the server as well as penetration testing to assure that the new application does not introduce unnecessary security risks to the IT network. Only after the application has received a certification from Security should the application be loaded onto the Production server. Be certain to verify that there is a good backup of the production server first! None of this work should have taken place on the original server, so if something goes wrong with the integration, the old server may be placed back into production.

Step three: Full Server Integration
After a determination has been made that a server should be re-located with all existing applications onto the IT network, the server should be examined in the same way that all previously existing servers on that network should already have been tested, by undergoing a full vulnerability assessment. Begin with tools that automate scans for vulnerabilities in operating systems and applications. These tools provide reports of discovered vulnerabilities, which should then be verified if that could be done without risk to the system. Many of the free and fairly inexpensive tools really work quite well; the only category in which some are lacking is reporting capabilities. No matter how large the available budget, one tool that is highly recommended for everyone to use is a free tool, NMAP. It is not fancy, it requires knowledge of Linux and its reports are text only, but it is extremely fast and very accurate, which sometimes is more important than anything else. There are also vulnerabilities that cannot be safely tested by an automated tool, but can be discovered by using personal knowledge of the type of system or program.

After a full vulnerability assessment is performed and a report is created containing recommendations for configuration changes and operating system and application software updates, it is up to the server administrator to apply appropriate changes. Testing may need to be done before changes are made, and of course full backups created prior to altering the production systems. A

formal process, as in a form, should be in place for the administrator to report that either each change has been made or a valid reason given for why it can't be. Following is an example of what such a form may look like:

1. A. A full description of the vulnerability, possibly including links to more complete information available on the Internet.
   B. A complete and understandable description of how to address the vulnerability. Provide links to more complete information if possible.
   C. Provide a date by which the change must be completed.
   D. Change completed on: (date to be entered by Server Administrator)
   E. If the change is not made, provide a detailed explanation of why it was not feasible. (Completed by Server Administrator)
2. A. Next Vulnerability

After a predetermined time and before the server is allowed to be moved onto the IT network, the security team should validate that all necessary changes have indeed been made.

Similar testing and updating should be performed on the servers that cannot be integrated into the IT network.

Step Four: Implementation or Expansion of an Intrusion Detection System. There are two major types of intrusion detection systems, Network based and host based. For large networks like the one being discussed here, I recommend concentrating on a network based intrusion detection system first. There are many different systems available. There are appliance based, fully supported systems available from a variety of vendors. Be aware that they can be extremely costly, and often require the purchase of extra, also very expensive administration software to convert the data from their sensors into something easily usable by staff. If money is not a problem in the organization, then this can be a very good option, as it pretty much guarantees a good system with good support and lots of nice pretty graphic reports to show the boss.

If money is in short supply in the organization, and the available staff has the knowledge and interest in building their own system, it is quite possible to build an extremely impressive system using free or fairly inexpensive software. Such a system should be designed to be centrally manageable, the staff should be able to judge which publicly available signatures would be appropriate for the network as well as be able to write their own signatures, and the management program used should provide the level of reporting needed by the organization. Also be sure to harden the sensors' operating systems and applications; encrypt the traffic sent between the sensors and the management servers, use separate NIC's for traffic monitoring and sending alerts to the management server, place the sensors on a protected management network with ACL's on the router

defining all machines allowed to connect to that network, etc. In other words, lock down the system as tight as possible, because a compromised intrusion detection system can be more harmful than no IDS at all! If the available staff does not have the time and/or expertise to take these steps, a pre-configured and fully supported system should be purchased.

Another important consideration for an IDS is that it be scalable to the needs of the organization. Sensor placement is critical, but must be decided according to needs. Assume that the IT department performs NAT at several levels. This may mean that there would need to be sensors on both sides of certain firewalls and routers in order to allow for the identification of attacking systems. This can be a very important thing to identify early on – there may not be enough funding to purchase a $15,000 sensor for each network segment and/or firewall interface that should be monitored.

The most important network segments to monitor will be the ones that the critical servers occupy and those of the IT staff who have access those servers. It is important to capture the data before any NAT takes place. Once the core servers and any network locations that can easily access those servers are properly monitored by the IDS, and the perimeter defenses are monitored as well, and then if funding remains it may be reasonable to consider monitoring the remaining network segments. It is also advisable to place host based intrusion detection on the critical servers.

Step Five: Incident Response

It is imperative to have well defined processes in place to deal with different types of Incidences. An incident can range anywhere from an outbreak of a virus or worm on the network (remember Nimda) to the theft of confidential data or loss of administrative control of servers. Different types of incidents require different responses, but many similarities exist. NIST, the National Institute of Standards and Technology, provides a very nice summary of policies and procedures that should be in place. Please visit their web site for the up to date document: http://www.cert.org/security-improvement/practices/p044.html

There is a great deal of information available on the Internet explaining how to develop incident response procedures and I will include links to several of them in my references. There is so much to be considered and done that it cannot fit within the scope of this paper. To broadly summarize what many of these resources state, it is critical to have your incident response procedures well documented, and make sure that everyone who may be involved in dealing with an emergency know and understand them. It is also absolutely essential for these procedures to be supported by Policy, and you must be given the authority to enforce the necessary actions with full management support at all levels.

This is another area where it is best to develop official forms to help track and manage each major type of incident. There is a great deal of helpful material on the Internet for this, and SANS has step-by-step guides available for purchase.

Step Six: Security Policy
Having comprehensive and up to date security policies in place is critical to the success of any security initiative, and there is a great deal of information available on the Internet and from other sources on how to implement security policy. Since this paper is concerned with network redesign, it is important to note that the organization's existing security policy will need to be readdressed.

This will not be a comprehensive evaluation of the need for security policy, how to develop one or what must be in place to enforce it, but instead briefly explain the importance of identifying the appropriate structure for a policy. A security policy must be structured to be understandable, provide the legal foundation for the organizations security objectives, and be organized in a manner that is appropriate for that organization. Types of policies include:

Enterprise level policy
International policy
Division level policy
Local level policy
Program policy
Issue specific
System specific
Procedural policy
Standards
Guidelines
Procedures

This listing is a mixture of policy levels, policy types, and policy support devices. It is a long and daunting list drawn from many sources, and proves an important point – it is easy to become overwhelmed when attempting to develop security policies for any organization. It is important to realize that not all of these policy types are necessary for all organizations. A company employing only 5 people may need only an overall company policy and the procedures necessary to support that policy. A multinational corporation may need to conform to entirely different legal restrictions in specific locations and therefore require country specific policies that would necessitate the inclusion of specific issues in all lower level policies. An organization must base their security policies and policy structure on their business requirements, as security policy is intended to enhance the operation of the organization by managing the risks to its information systems, not by breaking system functionality.

The best way to prepare for the development of appropriate security policy is to carefully evaluate the organization, identifying its business requirements, the types of data on your network, the importance of securing each and the environment within which the organization exists. Understanding these things

will help to identify what information regarding security policy development is appropriate for developing security policies for this organization.

Step Seven: Developing functional working relationships
While all of the previous steps are very important to address, the success of a security strategy will ultimately depend upon cooperation between all individuals within the organization.

Before users will cooperate in almost any situation, they first have to understand what is being asked of them and why. Properly educated users may also serve the function of notifying appropriate individuals of situations that may indicate security breaches. Another argument for providing proper security training of the user community is to raise their awareness of corporate security culture and social engineering issues. This is why security awareness training is vital in securing your network. Another rather successful method for improving communication with the user population is publishing regular security newsletters, and even humorous weekly quick notes. The more comfortable users feel interacting with security staff, the more likely they are to bring potentially important issues to security's attention, or to comply with sometimes inconvenient requests during a security emergency.

Close cooperation between system and network administrators is essential for the successful and secure operation of any network. While it may not be necessary for these people to work closely together on a regular basis, it is advisable to maintain regular and cooperative contact in order to build relationships that will aid in communication and cooperation during crisis situations. Regular non-emergency communication also helps foster a better understanding of the other employees' jobs, which can be of tremendous help during a crisis.

The Security Operations staff must foster close relationships with all IT staff. For purposes of incident response, the relationships with Networking and System administration staff are critical. While there should be formal procedures for different kinds of incidences, the simple truth is that without both practice in dealing with such situations and well-founded relationships of trust, cooperation between the necessary individuals may fail when it is needed most.

Conclusion:
This paper is not intended to be an all inclusive checklist of issues to be addressed during a network redesign, that would be far to broad a topic to effectively cover in one paper. Instead this is intended to help organizations recognize that there are a lot of issues that need to be addressed in order to develop a secure and effective consolidated network. The steps that have been listed are also not intended to be taken consecutively, but in most cases must be continuously addressed throughout the entire reorganization. Since this paper is essentially an outline of subjects that an organization should consider during an

IT reorganization and has not included in depth analyses of any particular issue, the references used in researching this material are organized in the order of the main issues addressed. This organization is intended to assist the reader in further research of the individual topics.

References

Infrastructure Design

1. Martin W. Murhammer, Kok-Keong Lee, Payam Motallebi, Paolo Borghi, Karl Wozabal. "IP Network Design Guide". June 1999.
URL: Http://www.redbooks.ibm.com

2. Department of the Army, TRADOC Pamphlet 25-73 "TRADOC Plan for Reengineering Information Systems Modernization (TPRISM)", 13 December 2000.
URL: http://www-tradoc.army.mil/tpubs/pams/p25-73/p25-73a.htm
URL: http://www-tradoc.army.mil/tpubs/pams/p25-73/p25-73b.htm#10

3. United States Department of State, "Information Technology Architecture" April 16, 1999. http://www.state.gov/www/dept/irm/it_architecture/it_vol1.html#_Toc452433037

4. Cisco White Paper, "Gigabit Campus Network Design--- Principles and Architecture", July 2, 2000.
URL: http://www.cisco.com/warp/public/cc/so/neso/lnso/cpso/gcnd_wp.htm

5. Cisco IOS Release 12.0 Security Configuration Guide
URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/index.htm

Application Integration

6. Karen Boucher, "Application Servers on the Front Lines", Software Magazine, Dec. 1999.
URL: http://www.findarticles.com/cf_dls/m0SMG/3_19/59329321/print.jhtml

Full Server Integration – Vulnerability Assessment

7. NIST Special Publication 800-42, "DRAFT Guideline on Network Security Testing", Feb. 2002.
URL: http://csrc.nist.gov/publications/drafts/security-testing.pdf

8. Stuart McClure, Joel Scambray, George Kurtz. Hacking Exposed: Network Security Secrets and Solutions, Third Edition. New York: Osborne/McGraw-Hill, 2001.

Intrusion Detection

9. Rebecca Brace, Peter Mell, "Intrusion Detection Systems", NIST Special Publication, Nov 2001.

URL: http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf

10. NSS Group Report, "Intrusion Detection Systems – Group Test (Edition 2)", Dec 2002.

Incident Response

11. RFC2350, "Expectations for Computer Security Incident Response", June 1998.
URL: http://www.faqs.org/rfcs/rfc2350.html

12. Laura Taylor, "Incident Response Planning and Management", January 28, 2002.
URL: http://intranetjournal.com/articles/200201/se_01_28_02a.html

13. Sans Institute Publication, "Computer Security Incident Handling Step-by-Step".
URL: http://www.sans.org/newlook/publications/incident_handling.htm

14. New Technologies Inc., "Computer Incident Response Guidelines" May 7, 1999.
URL: http://www.secure-data.com/guidelns.html

15. National Infrastructure Protection Center, "Cyber Threat and Computer Intrusion Incident Reporting Guidelines", September 11, 2001.
URL: http://www.nipc.gov/incident/cirr.pdf

Security Policy

16. Cisco publication, "Identifying Security Risks and Cisco IOS Solutions – Security Overview."
URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scoverv.htm#xtocid12467

17. Thomas R. Peltier, "How to Manage a Network Vulnerability Assessment" training materials, Netigy Corporation, 2000.

18. Peter Morrissey, " The Interactive Network Design Manual; How To Secure Your Network", November 1996.
URL: http://www.networkcomputing.com/netdesign/security1.html

19. NIST 800-12 "Introduction to Computer Security: The NIST Handbook, Chapter 5 Computer Security Policy."
URL: http://fas.org/irp/doddir/other/nist-800-12/chapter5.htm

20. B. Fraser, Editor, SEI/CMU, RFC 2196. "Site Security Handbook" Section 2, Security Policies, September 1997.
URL: http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2196.html#sec-2

Working Relationships

21. Richard Bartley, "Corporate Information Security Strategy – how to avoid giving free information to attackers", March 26, 2001.
URL: http://online.securityfocus.com/guest/5144

22. Louis Lehman, "Cooperation – The Foundation of Network Security", May 1, 2001.
URL: http://rr.sans.org/incident/cooperation.php