GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Practical Assignment Submission
Teresa Kelly
GIAC certification – GSEC, Version 1.4b
November 23, 2002

Security Policy Harmonization in Extranet Connection Projects

Introduction

Nothing strikes fear into the heart of a network administrator than the words we need to allow a partnering company access to our trusted network. In today's world of the Internet and the ease of establishing all kinds of connections, management is pushing to interconnect systems and create extranets to meet a variety of business and economic mandates. The inherent security risks associated with moving from a trusted, stable environment to an unknown and therefore, untrusted environment demands a new set of tasks of management and system personnel. For that reason, it's important to introduce early in the connection project a concept of security policy harmonization. This process attempts to bring together the participants in the partnering organizations and attempt to establish some ground rules prior to any of the connections being made. The process of security policy harmonization is an important task on any project designed to make an extranet connection. This paper will show the importance of this harmonization process and how failure to identify security risks and controls for both or all parties can result in a myriad of security breaches. It will also identify risks that cannot be mitigated through technology alone. Policies and contractual agreements specific to security may be your only method for protecting your assets and resources. If nothing else, they will add a layer of additional protection to any technological controls put in place.

What is an Extranet? Essentially it allows a corporation an opportunity to extend to its partners or other third party users access to proprietary information. The concept of the Extranet is fast becoming a reality as companies look for new ways to meet customer needs, setup more efficient processes and reduce expenses. There are significant benefits to linking your internal network with a partner, a vendor, a supplier, customers or other third parties. They include:

- Sharing corporate systems and data (often mission critical)
- Provide access to specific customer services
- Development of new products
- E-commerce
- Data and File Query
- Transactional processing

The new economic reality now requires the once stable, traditional and wholly owned structure to acquire new organizations; to set up strategic alliances and partnerships and to outsource all kinds of services. For many years, organizations have been concentrating on ensuring that their own networks are secure, private and protected. The firewalls were built to keep the 'bad guys' out.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The concept of the extranet changes the definition of your security perimeter. An extranet has been described as “basically an intranet communication system that is open to select customers, suppliers and partners.” (Hameed) If you think of your organization as a trusted entity, your organization now opens its doors to those it knows nothing about, and therefore, an untrusted entity. Now management must not only be concerned for security controls within its own boundaries but security controls of those its allowing inside.

It’s obvious that extranets make business sense but it cannot be overstated, the risks it adds to your network, business applications and data. It’s important to understand the reason for the connection and who exactly will be connecting. You must learn as much about the risks both companies face as they interconnect their systems. The security policies at both sites must also be communicated, reviewed and harmonized in some fashion. Which policies will take precedence? Does one of the connecting organizations need to adjust their security stance to some extent? In many cases this may not be an option. Some extranets exist to extend services to another organization who happens to be a customer. It may not be feasible or advisable to expect your customer to change their security policy to meet your needs. Once the connection is made, “the participating organizations have little or no control over the operation and management of the other party’s system.” (Hash, p 4) The sooner in the connection project you can begin to identify these risks, the sooner you can begin to identify the solutions. You can begin to decide on the “rules of engagement” or the acceptable behavior that will be tolerated by those “untrusted” entities.

One of the biggest risks that faces a third party connection is the realization that security will be reduced to the level of the organization with the weakest security. Despite the connection type deployed (ie. leased lines, VPN, dial up, etc), your security may be compromised. An example of how this may work is in the situation where a VPN is deployed. A Virtual Private Network (VPN) is designed to create secure, encrypted tunnels through public networks. The VPN tunnel once created provides network to network access from one site to another or from one organization to another. However, if the VPN tunnel is not specifically terminated in a segregated area of your network, then essentially the VPN establishes one large network with a pipe directly connecting both ends. The security of the VPN will essentially adopt the security of the weakest end point.

Management is often under a misconception that if you have a firewall, your security risks are solved. After all, the firewall’s job is to stop all malicious traffic and protect the corporate assets. “A good firewall will faithfully do exactly what you’ve told it to do through its filter rules. But how do you know what the rules should be in the first place?” (Crume, p. 81) Firewalls are only as good as the security policies that are configured into their setup. In addition, some corporations have built systems that have a level of trust built directly into their architecture. Technology solutions reflect this trust. You may have a relatively flat

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

network that allows employee's access to almost any server in your domain. Opening the doors to third parties in an extranet means you may now be giving this same level of access to users in this partnership. You may also be unintentionally granting access to their customers and their partners and maybe even to your own competitors.

Even though this paper is concentrating on the policy aspects of connecting in an extranet, one technical aspect that is also affected by your policy is the architecture of your network. Consideration should be given to dividing up large or flat networks into separate network domains. These domains can then contain controls designed to segregate groups of services, data and users, specifically partners. Generally, a segregated section of the domain is referred to as a Demilitarized Zone (DMZ). The DMZ creates a portion of your security perimeter. Based on the business services that have been identified in the connection project, the systems that supply those services should be placed in a "partner DMZ". This is a special area of the network designed to control access to a dedicated secure zone.

This is a network issue that should be managed by effective policy. Since firewall rules are often defined by policy, it is useful to assist your firewall administrators and educate the project team involved in the connection project to identify some of the rules required for the setup of partner DMZ. An effort needs to be made where the business partners sit together and decide on the exact services they can expect; No more than what is absolutely necessary to accomplish the task should be allowed. Sample rules may include:

Rule #	***Source IP***	***Destination IP***	***Service***	***Action***
1	*Partner Network*	*Partner DMZ*	*Appropriate for partnership*	*Accept*
2	*Partner Network*	*Any*	*Any*	*Deny*
3	*Partner DMZ*	*Partner network*	*Appropriate for partnership*	*Accept*
4	*Any*	*Partner network*	*Any*	*Deny*

(Maiwald, p. 165)

Even if your firewall is configured appropriately, there is still need to ensure that your partner's security culture is in line with your security culture. Firewalls are limited in what they can do. Firewalls can only do what they are configured to identify. They cannot:

- Protect against attacks not made through the firewall
- Protect against an authorized user's malicious behavior
- Protect against viruses and Trojan horse programs
- Protect against completely new threats
- Protect against bad or nonexistent policies

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Protect against your own errors (e.g. incorrect filter setup)
- Act as an effective single point of defense
  (Crume, p. 82)

The inability of a firewall to entirely protect against the risks that exist in an extranet, points to the need for a 'marriage' between the technology and the policy. Despite your best technological efforts to lock down your security perimeter, there needs to be a realization by management that throwing money at expensive hardware and software solutions may not meet the need in its entirety. We need to develop a comprehensive approach that recognizes the need to implement both human and technical components and controls.

Need for Security Policy Harmonization

If we adopt the premise that security is primarily a human and management problem as opposed to a technological problem, then it becomes paramount that you enter into a dialogue about security policy harmonization early on in any network connection project. When considering the concept of policy harmonization, some of the security policies of relevance in any network connection implementation include authentication and access control policies, encryption practices, access privilege assignment and revocation, privacy issues, change management and availability of resources, including contingency planning. There may also be issues to resolve around remote maintenance, incidence response and auditing. In every organization, there may be radically different approaches to these practices. Some by their very culture will grant much more trust to their staff than another organization. In a closed shop, trust may mean that those on the inside are granted far more freedom and access to data, systems and networks. Security policies, if one exists at all, may reflect an organization that has a high degree of loyalty and reliance on staff to do the right thing. A company that has very low turnover may not have well-defined procedures for ensuring that a terminated staff member's id is disabled. Another company may allow their staff more freedom in their system usage. For example, they may have a more lenient position with respect to how much personal use of systems is allowed. Staff may be freer to surf the Internet for personal reasons. Downloading programs, music and other materials may not be regulated. As you prepare to connect your network to another corporation, these details become important. Charles Cresson Woods says, "It is critical that the participants in this new network agree on certain fundamental security policies. If the security policies are incompatible, then there is a possibility that lax security at one organization could lead to security compromises at the other." (Wood)

The organizations should identify the security policies that govern each organization and which set of policies will govern or take precedence during the duration of the connection. "The intention of harmonizing security policies is to establish a "baseline" or a standard of due care" to which all parties to the arrangement must abide. This baseline must define the minimum information security requirements that must be maintained in order to participate in the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

networking arrangement. Not being willing or able to meet these requirements should be sufficient justification for exclusion from (or expulsion from) the multi-organizational networking arrangement" (Wood, p 645)

Need for Third Party Contract

Once project teams can agree to the policies that will govern the network connection, the process should then look to documenting those agreements and standards of due care. There should be a shared expectation of services and controls on those services. The services that will be provided and the controls that will be in place need to be documented in a contract with the third parties in your extranet. The ISO 17799 standard proposes that:

> Arrangements involving third party access to organizational information processing facilities should be based on a formal contract containing, or referring to, all the security requirements to ensure compliance with the organization's security policies and standards. The contract should ensure that there is no misunderstanding between the organization and the third party. Organizations should satisfy themselves as to the indemnity of their supplier. (ISO/IEC 17799, p 6 section 4.4.2)

Many of the new data protection laws may soon require that partnerships provide evidence of the security measures in place at the partnering site.

The International Organization for Standardization 17799 (ISO17799) is one of the most widely recognized publications on security standards in the world. This standard was formally referred to as the British Standard 7799. These standards identify a significant number of control requirements, including a list of important things to include in a third party contract. In this paper, I will identify a number of these inclusions and expand on reasons why these should be covered off in third party agreements.

Items for Inclusion in Third Party Contracts/Agreements

1. **Data Owner**

   In Third Party contracts (often called agreements), it's important to define the "Data Owner". The "owner" has the responsibility to specify the data protection requirements and to audit those who have access to administer security procedures on their behalf. Ultimately, the owner is responsible for ensuring that the data is protected and secure. If company politics get in the way of defining ownership, use network and data flow diagrams to identify how the data is moving across the connection. Often both organizations will feel the need to be responsible for a component of the information. It may mean that data ownership is transferred from the transmitting party to the receiving party. In other instances, the transmitting party may retain ownership and the receiver merely becomes a custodian of the data. (Hash, p 8)

   Specifying an owner and the value of the information they control is not always readily apparent to those who will eventually be caring out the day-to-

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

day tasks of participating in the network connection. Once a connection is set up and operational, the flow of data over time should be cause for concern. Data classification becomes an additional requirement and the "owner" should make this clear. It's important that employees of your organization are educated about the acceptable content and the value of that content that has been agreed to in the exchange. The data owners need to recognize the effect of errors in exchanging data incorrectly or inappropriately. "Once information has arrived at a partner there is little guarantee-beyond expensive legal recourse-that prevents the information from traveling further. Also, there is no way to "take back" information." (Collin)

2. **Change Management**
   A process of change management must be identified. Impacts of change now affect more than one organization. Any authorization requirements and procedures should also be included. These authorization requirements extend to who is responsible for hardware and software installation and maintenance. If there needs to be modifications to software, hardware or network configurations it should be clearly stated who authorizes these changes, when the changes will occur and what the backout procedures will be, if something were to go wrong.

3. **Data Protection laws**
   Data protection laws within the jurisdictions of all parties to the connection need to be examined and considered to see what impact and/or restrictions exist with respect to the exchange or passing of data over the interconnection. Some of the regulations that need to be considered include the new Privacy Laws (Bill C6) in Canada; Health Insurance Portability and Accountability Act (HIPAA) regulations for the healthcare industry in the US; and the European Union's Data Privacy directives. For example, within the new Canadian privacy laws, an individual must give written consent for all uses of their personally identifiable information. "Each organization should consult with its Privacy officer or Legal counsel to determine whether such information may be shared or transferred. Permission to exchange or transfer data should be documented along with commitment to protect such data." (Hash, p 6)

   Another aspect closely affiliated with data protection laws includes data retention requirements. Limitations on the retention of data should also be spelled out in agreements and contracts to ensure it matches any legal requirements and policies that are practiced within your organization. It would not be wise to purge and destroy data per a retention schedule within your own organization, only to discover that the data still exists at your partner's site.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4. **Description of Services Offered**

As your organization prepares to establish an extranet, you need to evaluate the types of services you will be offering. Common services might include Web services, FTP, Email, Kerberos, data and file queries, transactional services, and the list goes on. You will also want to identify the applications associated with those services. You'll need to determine the network protocols that will be used. It's important to list these services to ensure that there is no misunderstanding about what the partner can expect.

Identifying the services should also force your organization to take the time to consider your own organization's security and how well you implement security best practices. For example, do you only run minimal services on your own servers? Do you patch vulnerable services on a consistent basis, and how well do you monitor those services and their use? Once you decide the types of services you will offer in your network extension and once you decide what ports need to be open and who will have access, you'll have a sense for the risks you are going to face. In IP networks you'll want to be alert to risky protocols in use such as UDP, ICMP, SNMP, etc. (Harris)

You can look to vulnerability lists for risks associated with a variety of services and protocols. The SANS/FBI list of the top 20 Internet vulnerabilities is one example of these vulnerability lists. To mitigate those risks you need to address all of the weaknesses within a service you want to offer. (Campione) Then, identify the services to be offered in your contract. All new services and protocols that might be added in the future will need to go through a formal change management procedure.

5. **Access controls**

Identify all permitted methods for accessing applications and data. You will want to list the controls that will be implemented and adhered to throughout the network connection term. An example of a control might include your minimum requirements for password creation. Another control will include a definition of the authorization process for user access and privileges. It might seem easiest and convenient to provide a single username and password for the partnering organization to share when accessing your network resources. But this option should be avoided. As much as possible access should be specific to the user. This ensures a level of accountability is maintained. In addition, it allows you to audit user activity and movement at the third party site. A shared username or account may be compromised if employees at the partner site leave and the password is not changed.

Access control should identify any termination procedures and how they should be carried out. Make it a requirement to maintain a list or database of individuals authorized to use the services being made available and what their rights and privileges are with respect to such use. Document who has responsibility for maintaining the list or database and complete an audit of this

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

database on a periodic basis. And finally you'll want to maintain the right to monitor, and revoke users based on suspicious user activity.

6. **Liability**
   The respective liabilities of the parties to the agreement need to be documented in third party agreements and contracts. Contracts should specify the standards you expect with respect to treatment of the data. If the organization is negligent, then appropriate liabilities and consequences should be clarified in the contract. "Determine and agree on who will be liable for what and under what circumstances" (Harris)

   This is often a difficult process to determine appropriate consequences. Often it's not feasible or economically prudent to adopt the line "the connection will be terminated for violating the contract"; but failure to document some type of consequence will leave you without recourse in the worst case scenario. Ideally, the security harmonization process and resulting contractual agreements are aimed at educating your partner on what you consider important to a secure network. With a good relationship and awareness of your expectations laid out 'on the table', litigation can be avoided.

7. **Physical Controls**
   If your organization has a policy that all critical servers and data need to be locked and segregated in secured facilities, then these controls should be practiced in organizations where you are transferring or exchanging data. Similarly, if sensitive data is locked in cabinets and shredded when no longer needed, then these controls should be required of the third party.

8. **Malicious software**
   Controls to ensure protection against malicious software are an absolute necessity. Again it becomes critical to identify that each organization must take appropriate and frequent steps to ensure that the risk of transferring viruses, worms, Trojans and other malicious code is kept at bay. One thing to keep in mind is that an organization should never rely on a third parties security measures to protect their data. So in this specific control requirement, it's important that your own organization have its own virus protection controls at all connection points and gateways. This particular requirement of the third party simply adds another layer of protection.

9. **Incident reporting**
   The third party agreements and contracts should identify arrangements for the reporting, notification and investigation of any security incidents or security breaches. This may include the requirement that someone within your organization be notified within a specified and reasonable period of time when there is a security incident that involves your data. You may wish to establish and document escalation lists with names and phone numbers of people in both organizations which would be used when an incident occurs.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

10. Involvement of the third party with subcontractors

Companies that partner with you may have additional partnerships of their own. They may sub-contract their services and they may have relationships with your competitors. Michael Harris suggests that this is where you begin to extend your network into areas you may not have even considered or recognized.

> As you connect your networks with various outsourcers, partners, vendors, alliances and even consortiums you may, and probably will, connect with whom they do. The above connection scenario changes the established trust model from explicit and understood trust to one of transitive implicit trust. This is the "I may trust you but I do not necessarily trust who you trust" scenario. (Harris)

This being the case, non-disclosure and confidentiality agreements are critical to all third party agreements and contracts. Limits on how far your data extends must be spelled out.

11. Right to Audit Clause

And finally, a "Right to Audit" clause should be included in your third party agreements. This clause should include rights to examine contractual responsibilities and to ensure that the agreements made at the outset are adhered to. It is also appropriate to ask partnering companies to provide you with any existing audit reports they may have had completed recently on their operations.

In any new effort to create an extranet the project team will invest significant effort toward identifying items of relevance that need to be included in third party agreements. It would be a useful exercise to consider establishing a corporate network access policy. This would be a useful document for future projects designed to connect new third parties. A network access policy document could identify the networks and services that will be allowed access and the "rules" that should be applied for giving access to those proprietary services. It could further identify any management controls and procedures to protect the access to network connections and network services. (ISO/IEC 17799, p 37) It will be a good resource to identify and gather requirements for all new connection requests. This would provide a central source for identifying all sorts of partner connections and needs.

Once your Third Party contract or agreement has been developed, you will want a responsible agent within the partnering company to sign the contract and be accountable to the agreements. A debate exists as to whether everyone associated with your data within the partnering company needs to sign off on the security requirements of the contract or if it's up to the responsible agent to be held accountable for the requirements laid out in the agreement. Generally the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

debate can boil down to this question, “how can someone treat your data in the way you expect unless they know your expectations?” If it is a requirement within your own organization that all internal employees, contractors and temporaries sign off on your own internal corporate security policy then it’s reasonable to implement this practice with your partners.

In your initial discussions with the third party around harmonizing your policies and standards, you should get a feel for the security mindedness and awareness within your extranet’s user community. It may be entirely appropriate to require that staff in the partnering company is regularly made aware of security and how they play a role in securing the organization. Creating a modified acceptable use security policy specific to the third party employees and circulated among the user base may be appropriate.

Conclusion

When setting up an extranet or third party network connection, one of an organization’s many intangible assets takes center stage. Trust is an asset that is often taken for granted and its value underestimated. Trust is that reliance management has in the good intentions of its staff; it’s the knowledge that comes with knowing that your own internal policies are practiced faithfully, best practices and security measures are implemented and your network is effectively managed. When you open up your doors to the unknown and untrusted world, this asset of trust is put to the test. By opening the dialogue of policy harmonization and agreeing to follow a common set of practices that both parties can adhere too, you can hopefully proceed into interconnections with some measure of confidence.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References:

Campione, Jeff Webcast: "The Making of the 2002 SANS/FBI Top 20" SeachSecurity.com, held November 11, 2002 http://searchsecurity.com/r/0,,7581,00.htm

Collin, Barry C. "Extranet Security: What happens if your partner turns against you?" Reprinted from October 1997 issue of Computer Security Institute's monthly newsletter. http://internet.about.com/gi/dynamic/offsite.htm?site=http://www.its.state.ms.us/et/extranet/et%5Fextranet.htm

Crume, Jeff; Inside Internet Security: What Hackers Don't Want you to Know, Addison-Wesley, 2000.

Hameed, Imran. "Issues in Building an Extranet" http://internet.about.com/library/aa_extranet1_053002.htm

Harris, Michael, "Inherent security risks of outsourcing – what the CIO should know", November, 2002 http://www.gocsi.com/inherent.htm

Hash, Joan, "Guide for Interconnecting Information Systems", National Institute of Standards and Technology (NIST), November 2001, http://csrc.nist.gov/2001news.html

International Standard ISO/IEC 17799 First Edition 2000-12-01 http://www.cs.jmu.edu/common/coursedocs/CS4-580 InfoSec/ Daughtrey/ISO_IEC_17799.pdf

Lindner, Marty, "Securing Extranets", November 25, 2002 http://www.itaa.org/infosec/pubs/isarticle.cfm?ID=8

Maiwald, Eric; Network Security: A Beginner's Guide, Osborne/McGraw-Hill, Berkeley, CA 2001.

PentaSafe, Houston, Texas, "Using people assets to protect information assets: understanding the "human factor" of information security". 2001. www.infopackaging.com/brochures/humanfirewall.pdf

Techrepublic, "Secure Extranets: A Business Perspective", November 25, 2002 http://www.cio.com/sponsors/083099_secure.html

Wood, Charles Cresson, "Information Security Policies Made Easy" Version 8, PentaSafe Security Technologies, Inc. Houston, Texas, May 2001.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.