Security Considerations for Extranets

Karen Korow-Diks

Security Considerations for Extranets
Karen A. Korow Diks
December 18, 2001

Introduction

Increasingly extranets are being used by organizations to conduct e-business operations. However, an extranet must be properly planned, implemented and maintained to ensure that it does not pose an unacceptable risk to an organization's internal data and information systems. This paper identifies potential risks associated with extranets and the actions that can be taken to mitigate against them.

Why Implement an Extranet?

There are many definitions of an extranet. According to Norman E. Smith, an extranet is a networking environment set up so that a customer, supplier, consultant and anyone outside the company can access data and/or applications inside the company's network [Smith, p. 1]. An extranet is part of a company's Intranet that is extended to users outside the company [searchsecurity.com]. It is a business-to-business network operating over the Internet [Office.com, p. 2]. According to Richard Keeves, an extranet is an Intranet that is partially accessible to authorized outsiders [Keeves, IBC]. Only the extranet providers' suppliers, vendors, partners, and customers are allowed onto this network [King, p. 101].

Organizations choose to establish extranets for a variety of reasons including to:

- Promote the exchange of data and information among selected users
- Allow business-to-business and electronic commerce transactions between businesses and external customers
- Improve efficiency
- Provide a centralized access to data
- Expedite and speed up business transactions
- Be closer to customers
- Increase customer service and loyalty
- Collaborate with companies on development efforts
- Strengthen business relationships [Keeves, IBC].

Extranets enhance a company's ability to communicate and conduct commerce among employees, suppliers and customers. They also reduce the costs for businesses to communicate with external entities [King, p. 100]. For these reasons, it can be expected that the use of extranets will continue to increase.

Potential Security Risks Posed by Extranets

Although there are several advantages for organizations to implement an extranet, such an interconnection can expose businesses to increased security risks. Use of extranets can pose the following risks:

- By allowing extranet Web servers access to internal databases, businesses have to make an opening in their firewall. The more openings a company has in its firewall, the greater the possibility for the wrong people to get in and do damage to internal systems and data [office.com, p9].
- Too many extranet connections provide the potential entry points for computer viruses and other malicious code that can wreak havoc on information and information systems.
- An extranet connection often allows access to the company's proprietary data and therefore affords another avenue of access for unauthorized users to exploit sensitive or proprietary information.
- Because an extranet increases the number of network connections, it increases the risk of networking penetration. Once one network is compromised, an entry point for compromise of systems and data exists for all the other networks connected to it [Herold and Warigon, 35].
- Should the extranet crash or become compromised due to lack of adequate security, the extranet operator may be held liable for the loss of business operations at other companies [office.com].
- If connecting partners to the extranet have inadequate access controls or have a lack of understanding of extranet security policies and requirements, they could expose the interconnected networks to penetration [Herold and Warigon, p35].
- If connecting partners use modems to connect into the company, the potential exists for criminals to use war dialers or other means to dial into the network to access sensitive information or damage the network itself [Herold and Warigon, p35].

To mitigate against these risks, security measures must be identified and implemented which protect the extranet connection throughout its life cycle. The life cycle of the extranet involves planning, implementing, and maintaining the connection. Security measures also must address the changing and evolving security vulnerabilities and threats to the systems and data accessed via the extranet.

Measures to Mitigate Risks Posed by Extranet Connections

The following section identifies security measures that should be considered when planning, implementing and maintaining an extranet. These measures provide network and application security to protect data and resources from unauthorized access.

Establish a Forum for Planning, Implementing and Maintaining the Extranet. To ensure that the interconnection via the extranet is as protected as possible throughout its life cycle, organizations that are parties to the connection should work together to develop a coordinated and comprehensive approach to planning, implementing and maintaining a secure connection. These actions should be taken under the auspices of a formalized forum dedicated to ensuring the security of the extranet connection. Responsibilities of the forum should include, identifying security controls that should be implemented by

each organization to protect the interconnection and associated information assets; developing an extranet security policy; and establishing and implementing an extranet security contract. Establishing a forum can provide a channel for clear and regular communications between the parties involved in the extranet connection. Both managerial and technical staff should be members of the forum and involved in all aspects of the interconnection life cycle.

Develop and Implement An Extranet Security Policy. The forum established for planning, implementing and maintaining the extranet should develop the extranet security policy. The policy provides a common understanding and set of security standards for managing the risk associated with establishing and maintaining an extranet. The policy not only identifies security requirements for the extranet, but also assigns responsibility so that security measures are implemented. The security policy should be a living document that is modified as information security technologies change. The security policy must be agreed to and approved by all parties to the connection. According to Christopher King, the following statements should be included in an extranet security policy:

- The extranet must be securely partitioned from the company intranet
- Secure network connectivity must be provided using a dedicated line or using a virtual private network (VPN)
- Extranet users must be uniquely identified using adequate authentication techniques
- Authorization must adhere to the principle of least privilege
- Extranet managers will receive monthly access reports to verify the proper use of the network
- The extranet must not provide a routable path to the participant networks (i.e., the extranet provider's network should not allow packets to flow between partner networks)
- A real-time monitoring, auditing, and alerting facility must be employed to detect fraud and abuse [King, p 102].

Additionally, the policy should state that all parties to the extranet connection are responsible for ensuring only authorized users have access to the extranet and that these users comply with the extranet security policy.

Establish and Implement an Extranet Security Contract. The forum created for establishing, implementing and maintaining the extranet should not only develop the extranet security policy, but also the extranet security contract. This contract is a security document that specifies the technical and security requirements throughout the life cycle of the extranet. The contract documents the security requirements for connecting the information systems and identifies the security controls that will be used to protect the systems and their data. According to the Herald and Warigon, an effective extranet security contract should serve as a legally binding document and should:

- Provide a clear understanding of security standards to be followed by connecting partners

- Provide a description of the applications and information that will be accessible by the external partner
- Be reviewed and approved by the corporate attorneys prior to approval and signing
- Ensure that the connecting party agrees to comply with minimum security polices
- Ensure those signing the contract are authorized to do so
- Stipulate that intrusions will be investigated, reported to the other connecting party and that corrective measures will be implemented by the victimized party
- Ensure that each connecting party isolates their network from the other party using firewalls and other secure networking strategies and technologies
- Ensure that each connecting party agrees to audit their network and inform the other party of any situations affecting their mutual security
- Stipulate the date for start of service and a termination statement that takes effect if either party does not adhere to the contract
- Stipulate that those having access to the extranet or involved in maintaining the interconnection participate in a security awareness and training program to ensure their understanding of their security responsibilities in using the extranet
- Stipulate that each party agrees to continue attending forum meetings to discuss security issues of mutual concern [Herold and Warigon, p 38-39]

Conduct a Risk Assessment: It is critical that all parties to an extranet connection understand their systems and the security risks posed by establishing an interconnection; and have a common understanding and agreement on what security controls need to be in place to mitigate these risks. Understanding the network and identifying the threats and vulnerabilities associated with the interconnection helps to determine the level of risk associated with interconnecting to another system. Conducting a risk assessment of the network and system is a good way to learn the answers to these questions and to determine how secure the network is. The risk assessment can be carried out by a certified third party that examines the baseline security policy and the security architecture that it meets [King, p 104]. As part of the risk assessment process, the use of hardware vendor programs should be considered to test for holes in the network such as misconfigured routers or switch ports. Additionally, the results of the assessment should be documented and based on a set of predetermined security requirements approved by all organizations involved in the interconnection.

Provide Physical Access Controls to the Company's Network. According to the *Computer Security Journal (CSJ)*, a company should centralize the connection points of its network in secure locations [CSJ, p54]. These locations should provide protection for network assets against damage, loss, theft, or unauthorized physical access. Additionally, environmental controls should be put in place to protect against natural disasters and hazards such as fire, excessive humidity and flooding. Requiring the use of access badges, cipher locks and biometric access control devices should be considered to protect against unauthorized access. Only those individuals with a need for access should be allowed to enter areas where the company's computer hardware is located.

Securing the Network. Securing the network involves ensuring that all components connecting to the company network comply with the company's and the extranet security policy. A common and effective practice for securing the network when connecting an internal LAN to an external network, such as an extranet, is to install a network Demilitarized Zone (DMZ). The DMZ provides a tightly managed network buffer between the internal network and the external network [Smith, Part 5, p.2]. The DMZ can be set up by installing a firewall on the incoming external line and one at the connection to the internal network. The systems installed on the network between the two firewalls are in the network DMZ [Smith, Part 5, p.2]. The DMZ provides a secure partition between the extranet and the provider's Intranet [King, p 101].

Securing the network also involves using additional security software and hardware that provide capabilities for intrusion detection, virus scanning, identification and authentication, and encryption. Installing intrusion detection systems provide the capability to detect breaches in the security of the interconnection. Virus scanning software scans the information that is transmitted from one information systems to another and eliminates malicious code before it can cause damage to the system. Using strong identification and authentication (I&A) mechanisms helps ensure that only those who are authorized have access to the interconnection. Such I&A mechanisms include user identification and passwords, digital certificates, biometrics and smart cards. Encryption of data during transmission and storage protects the confidentiality and integrity of the data.

Conduct Extranet Auditing. To help control risks, parties to the extranet should install auditing mechanisms to record activities occurring across the interconnection. To be effective, the security audit should be thorough in addressing vulnerabilities and it should be repeatable to provide a consistent perspective on the company's security practice [secinf.net/info, p 5]. Types of activities to be audited include event type, date and time of event, user identification, the success or failure of access attempts and security actions taken by the system administrators or security personnel. The audit logs should be analyzed on a regular basis.

Conclusion

Businesses will continue to use etranets to increase their productivity and efficiency, and to meet customer service requirements. However, using an extranet exposes the organization to increased security risks. To address these risks and minimize the chances for unauthorized access into their information systems, businesses can implement a number of security measures. Such measures range from developing a comprehensive extranet security policy and extranet security contract to implementing physical and logical security measures to control user access and ensure network, information system and information security.

References

Christopher King, "Extranet Access Control Issues, " in Harold F. Tipton and Micki Krause, ed., *Information Security Management Handbook,* Vol. 2, 4th edition (New York: Auerbach, 2000), 99-114.

"Comprehensive Enterprise Network Security Assessment: A White Paper for Enterprises in an Internet Environment," ISS. (http://secinf.net/info/ids/censa/CNSWP.html)

"Establishing an Extranet: Overview" http://www.google.com/search?q=cache:CHZB5CEFvZI:www.expertengines.com/dev/obtinclude/technology/establishing_extranet.asp+%22And+according+to+a+1999+Booz-Allen%22&hl=en

Herold, Rebecca and Slemo Warigon, "Extranet Audit and Security," *Computer Security Journal*, Vol. XIV, No. 1, 1998, 35-44.

Keeves, Richard, "Overview of Extranets," IBC, 2001. **http://internet.business.com.au/May%20IBB.pdf**

Ling, Raymond Rihao and David C. Yen, "Extranet: A New Wave of Internet," *S.A.M. Advanced Management Journal*, Vol. 66, No. 2, 39-44.

Smith, Norman E., Extranet Planning Guide," September 27, 1999. (**http://itmanagement.earthweb.com/article/1,,616141,00.html**)