Interested in learning more about security?

SANS Institute InfoSec Reading Room

One Approach to Enterprise Security Architecture

This paper discusses an approach to Enterprise Security Architecture, including a security policy, security domains, trust levels, tiered networks, and most importantly the relationships among them. Rather than discussing the infrastructure of an information security program, this paper focuses on the architecture of an information security program. So what's the difference? The infrastructure refers to the supporting elements needed for functionality, and the architecture refers to the cohesive design of the elements....

One Approach to Enterprise Security Architecture

Abstract

The objective of enterprise security architecture is to provide the ***conceptual design*** of the network security infrastructure, related security mechanisms, and related security policies and procedures. The enterprise security architecture links the components of the security infrastructure as one cohesive unit. The goal of this cohesive unit is to protect corporate information.

This paper will discuss an approach to Enterprise Security ***Architecture***. It will describe an enterprise security policy, security domains, trust levels, tiered networks, and most importantly the relationships among them. Rather than discussing the infrastructure of an information security program, which numerous resources exist, this paper will describe the architecture of an information security program. So what's the difference? The infrastructure refers to the ***supporting*** elements needed for functionality, and the architecture refers to the ***cohesive design*** of the elements. While reading this paper, observe how the business objectives and management's security concerns are relayed to the users of corporate information via the enterprise security policy. Observe how the security domains inherit the policy, how the trust relationships are established between the security domains based on the policy, and how tiered networks are physically utilized to support the policy.

Introduction

As stated, "Most companies do not adopt published security management standards, but choose to write their own. This means that consistent, effective security standards are unlikely to be applied across different organizations." (Information Security Forum, p.1) There is not a one-size-fits-all policy that will suit the needs of all corporations. However, by accepting a recommended approach to enterprise security architecture, corporate security programs may become more consistent and effective.

Architectural Due Diligence

Every company implementing an information security program should perform due diligence regarding enterprise security architecture. The reason is that enterprise security architecture provides the concepts to ease the understanding and troubleshooting of security issues and to build structured, meaningful security practices. In addition, it may be used in the event of an audit or litigation. This structured approach saves time, resources, and money by providing guidelines to reduce the repeated security practices and processes that should be performed with each IT project. Unfortunately in smaller organizations, security architecture may come inherently as the enterprise security technology is deployed. The problem with this is that many security processes and resources are duplicated when the security department reviews similar projects. In addition, inconsistent decisions are made on similar projects resulting in an inconsistent security model.

The term "enterprise" used throughout this paper refers to multiple internal networks, multiple internal areas or domains, various internal devices and systems, numerous applications, and a diverse user presence as a collective unit.

Architectural Elements

The enterprise security architecture must ensure confidentiality, integrity, and availability throughout the enterprise and align with the corporate business objectives. The elements of the enterprise security architecture aid in the understanding of the enterprise security issues and isolate the vulnerabilities. "The enterprise security program must address all of the infrastructure elements in order to provide true protection of information assets. Failure to address even one element of the enterprise security infrastructure leaves large holes in protection and results in little security improvement." (Vance, slide 10)

Table 1 provides a brief comparison of the types of elements found in enterprise security architecture and in an enterprise security infrastructure. Only the major elements are given for comparison. There can be thousands of actual elements in a design.

Table 1

Elements of an Enterprise Security Architecture
Policy
Security Domains
Trust Levels
Tiered Networks
Elements of an Enterprise Security Infrastructure
Documentation = Policies, Standards, & Guidelines
Services = User Awareness, Guidance, Administration, Monitor, Respond, & Audit
Technology = Intrusion Detection Systems, Firewalls, & Host-based Protection

Architectural Priorities

When developing an enterprise security program, a good practice is to prioritize security concerns in the following order: people, policy, and then technology. This order of priority considers job functionality and business needs as the highest priority. Security should not have a negative impact on production or the business. Policies need to be supported and enforced to provide a secure foundation for the business. Technology is the tool to provide the desired level of security. However, in many cases this order of priority is not established, or if initially established, changes over time. Unfortunately, the following order of priority is common: technology, policy, and then people. The reason for this is that technology can be overwhelming forcing security personnel to spend more time researching and supporting various devices, which results in loosing site of the business objectives. In addition, security personnel get heavily involved with urgent projects and relay detailed security information based on the policies, but often stray from the true business objective. Security personnel want to ensure that they do their job. It is very embarrassing to have your system compromised. The security person

responsible for approving a project may be willing to sacrifice some business objectives to ensure that they are not held responsible for a security breach. In general, this is not good practice, but is a tradeoff in many risk assessments. This is another reason for performing due diligence. Clearly stated policies within the enterprise security architecture will help avoid these types of decisions.

Technical & Social Architectural Challenges

A strategic and effective enterprise security architecture of today needs to be based on "Defense in Depth" which is a concept used to describe layers of defense strategies. The components at each layer work in tandem to provide one cohesive security mechanism. This layered approach will also help localize the impact if one element of the mechanism is compromised.

In addition to the technical challenge, information security is also a management and social problem. The type of security technology that is used depends on how the enterprise security architecture is designed, implemented, and supported via corporate security standards. Information security is partly a technical problem, but has significant procedural, administrative, physical, and personnel components as well. In some cases, specific technology may not be available. This is where well-designed procedural controls may be used until a technical solution is found.

"Social engineering bypasses cryptography, computer security, network security, and every thing else technological. It goes to the weakest link in any security system: the poor human being trying to get his job done, and wanting to help out if he can." (Schneier, p.266)

Enterprise Security Policy

This section will describe the role of an enterprise security policy as it relates to the enterprise security architecture. This section will not give detailed instructions on how to create an enterprise security policy.

"A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide." (Aronson, p.6)

The creation of enterprise security architecture begins by defining an enterprise security policy that everyone in the corporation accepts and supports. This starts at the top. The CEO must endorse, support, and abide by the policy. The policy must be enforced through all levels of management on down to every user. In many cases this results in an information security user awareness program that educates the users and ensures user acceptance. This program should include all users of the enterprise network, including non-employees. The main objective of the enterprise security policy is to provide confidentiality, integrity, and availability throughout the enterprise.

"Only 9% of employees indicated that they understood what security policies were intended to accomplish." Two thirds of responding companies do not keep policies up to date on a regular basis." (Vance, slide 15)

To develop an enterprise security policy, a thorough understanding of the environment is necessary. This is achieved by analyzing the security threats, risks, vulnerabilities, and countermeasures. Define the problem before defining the solution. Define what needs to be protected then balance the needs of security versus cost and business objectives. The business and IT strategies must be incorporated into this policy. The evaluation of the information generated by this analysis will help determine the classification of information and define the enterprise security domains.

A security policy is normally a brief, high-level document that uses general terms to express executive management's security concerns on the entire enterprise. It is a communication tool that allows management to communicate corporate security concerns. The policy also serves as a plan that is referenced during the creation of an enterprise security program. Standards are derived from the policy, and are the requirements that need to be met to implement the policies across the enterprise security technology. Based on the standards, are guidelines that consist of recommended procedures and checklists that provide users with a method of the meeting security compliance requirements. A major consideration of any policy, standard, or guideline is that it must be written in a manner such that the reader will clearly understand the objectives.

In general, the enterprise security policy provides guidance in making strategic, architectural security decisions. The standards and guidelines provide more detailed guidance for implementation and application in most situations.

The phrase "enterprise security policy" used in this paper refers collectively to policies, standards, and guidelines of an enterprise.

Here is an example of how policy, standards, and guidelines work together. A corporation has the following statement in it's policy, "Corporate information must be protected to an extent and for a period commensurate with its value and the degree of damage that could result from its unauthorized disclosure or modification, misuse, destruction, or non-availability." The message here is that corporate information must be protected, but does not state any standards or mechanisms that should be used to protect the information. The corporation has several standards. One standard states, "Corporate information accessed by an external, remote site, must be encrypted using the Triple Data Encryption Standard (3DES)." This statement clearly defines the standard to use for encrypting the data, and enables an auditor to check for this standard during a review. The corporation also has several guidelines for remote access, one of which describes how to configure virtual private networking (VPN) using 3DES to access corporate

information. This guideline can be followed to meet the security compliance requirements.

The enterprise security policy is enforced upon all information in the enterprise. A sub policy or guideline is used to classify the security level of each data element. This data classification eases the decision on where to place the information within the enterprise. The reasoning used to place data into various security domains, represents an interpretation of the policy at the domain level. The selected domain and placement in the tiered network is also based on data classification.

Data Classification
All information is not created equal. Classification of information into categories is necessary to help identify a framework for evaluating the information's relative value. The identification of this relative value will facilitate the establishment of cost-effective controls that will preserve the information assets for the corporation.

Data needs to be classified to determine the level of protection needed for each element, and what security domain to place it in. Data classification and risk management techniques should be balanced, thus resulting in a cost-effective mix of security disciplines and technologies. By classifying all data that enters the enterprise into categories, consistent and effective risk mitigation will prevail.

Levels of data classification will vary, but should be kept to a maximum of three or four levels to avoid confusion. In the event that data cannot be classified before entering the enterprise, a default classification should be applied. This default classification should be the most restrictive category to ensure confidentiality. Some information classification may change over time, and may need to be reclassified. Here is an example of data classification using three levels.

Public information is information that can be shared with anyone, the public. There are no restrictions on this information. A good example is a sales brochure on a corporation's most well known product. Another example is a retail price list.

Proprietary information is information that must be kept within the corporation and not shared with outside business partners because of its sensitivity, value, or criticality to the corporation. The corporation may be under legal or contractual obligation to protect this information. A good example is a corporation's customer information. Another example is a corporation's detailed network diagrams and firewall rule sets.

Private information is information that must only be shared with and accessible by selected individuals within a corporation. If this information is disclosed, it could violate an individual's privacy, cause significant damage to the corporation, or violate the law. Private information is often time-sensitive. Timeliness of delivery and use may determine the value of this information. A good example is the information stored in the

personnel files in a human resource department. Another example is information regarding a corporation buying one of its competitors.

Security Domains

The intent of using security domains is to standardize a corporation's information security program to eliminate the costs, user delays, and administrative overhead of redundant security procedures. Data classification of the security domain elements and domain certification of the entire security domain encourages security architects to limit access to security domains to elements with equal or more heightened security. By authenticating at a perimeter security domain, systems may not need to authenticate users a second time. User access to multiple systems should also be simplified.

Security domains separate the enterprise network into *logical*, discrete entities. The enterprise security policy is applied to each domain in a unique way. In other words, different standards and guidelines may be used in different security domains to accommodate the type of enterprise security infrastructure elements that reside in a security domain. As with data classification, many levels of security domains may exist, but it is best to simplify with three or four levels.

Domain Classification
Nearly all enterprise networks can be logically separated into the following security domains:

- A ***user domain*** consists of the physical location of the user and the type of network equipment used to access corporate information.
- A ***transport domain*** consists of the public and/or parts of the enterprise network used to provide connectivity to other domains. The other domains are normally bastion or data domains.
- A ***bastion domain*** consists of web servers, mail gateways, and application gateways. Separate bastion domains consist of VPN concentrators and network access servers.
- A ***data domain*** consists of mainframes, database servers, and application servers.

As stated earlier, data classification should be used to determine which security domain to place corporate information assets. Public information can be stored in any security domain. Proprietary information should be stored in a data domain, but a case can be made to store proprietary information in any domain, as long as it is not accessible to the public. Private information should be stored in a data security domain. One variance is that a corporate executive may store private information in a user domain.

Resources from multiple security domains can be virtually connected to provide access to corporate information. Consider a remote user accessing corporate information from home. The user resides in a *user* security domain. The user accesses the enterprise network over a virtual private network, which is in a *transport* security domain. The

connection is authenticated by a VPN concentrator and authorized by a network access server in a *bastion* security domain. Once authorized, the connection is permitted to a server in a *data* security domain without going through a second authentication process.

Trust Levels

At first glance, it may seem black or white, either trust or do not trust a network element. Experience performing security risk assessments will reveal that there are several gray areas of trust, otherwise referred to as variances. A variance is a condition in which a domain is trusted under certain conditions, possibly due to residual risk. Residual risk is the remaining risk when all available and cost-effective controls have been applied to mitigate the risk. The residual risk is normally acceptable given that the cost to eliminate it far outweighs the threat associated with the risk.

The decision to grant access to corporate information and resources depends on the data classification of the element, user authentication, and user authorization. Information classified as private is more secure and requires more challenging security mechanisms than information classified as public.

The trust relationships provide confidentiality and integrity for the authentication and authorization processes used to connect users to resources in security domains. To clarify, authorization techniques are used to determine who has rights to the resources and data in the security domain, and trust levels establish a standard level of authentication. The authentication method is related to the requesting user's user domain, transport domain, and if applicable bastion domain to reach the desired domain.

Trust levels are used to evaluate the security needs of each domain and determine what kind of authentication and authorization must be performed to permit connections to a domain. Elements in one data domain may have the same trust level as elements in another data domain, thus eliminating the need for a second authentication and authorization process. An entire security domain may trust another entire security domain. Trust levels enable a security domain to request additional authentication, or use the existing authentication at the required trust level. The reason for a trust relationship should be supported by the standards and guidelines that accompany the policy. The policy should also define the criteria required by each trust level in each domain. The user domain criteria depend on a user's physical location and type of equipment. The transport domain criteria depend on the authentication process used to access the enterprise resources. The bastion domain criteria depend on the resources accessed in the bastion domain. Bastion domains containing of web servers require less authentication than bastion domains that contain network access servers. The data domain criteria are based on the defined data classifications: private, proprietary, and public. A corresponding trust level exists for each data classification.

Trust Level Classification
Trust levels specify the minimum requirements for authentication and authorization based on the requested information or resource and the transport path from the user domain to the requested domain.

- ***Level three*** is considered **not** to be trusted. No authentication or authorization is needed. This layer relates to public information.
- ***Level two*** is considered trusted with variation. The variation may be due to a residual risk. User ID and password are required for authentication and authorization. This layer relates to proprietary information.
- ***Level one*** is considered to be trusted. Strong authentication methods such as tokens with personal identification numbers or digital certificates are required for authentication and authorization. Many times the data is encrypted before being transmitted. This layer relates to private information.

Domain Certification
All security domains must be certified to determine a level of trust. Domain certification is the process of verifying that all elements of the domain meet the requirements of the certification process for the assigned trust level. Domain certifications will vary depending on the enterprise security policy. The domain certification level, or trust level, is determined by reviewing all the elements in the domain, but the least secure element in the domain decides the level of trust. The reason for this is that access to this weakest link may enable an exploit to other elements of the domain. The domain certification process should be performed on a periodic basis. Depending on the guidelines, this may be a semiannual review process. Also, assigning trust levels to network elements eases the decision of which security domain to place the network element. The certification process results in a structured approach to ensure security for rapidly expanding enterprise networks.

Resources from multiple security domains with different levels of trust are virtually connected to provide access to corporate information. Again, consider a remote user accessing corporate information from home. The user resides in a *user* security domain that has a trust level of three, meaning that the domain is not trusted. The user accesses the enterprise network over a virtual private network, which is in a *transport* security domain that has a trust level of two. The connection is authenticated by a VPN concentrator and authorized by a network access server in a *bastion* security domain that has a trust level of one. Once authorized, the connection is permitted to a server in a *data* security domain that has a trust level of one. Since the data security domain has a trust level of one, the connection is passed without going through a second authentication process. This trust exists between the bastion domain and the data domain. Trusts are more common among domains of the same classification.

Tiered Networks

The tiered network model is a way to *physically* partition the enterprise network as specified in the enterprise security policy. Tiered networks allow the enterprise to physically protect corporate information from unauthorized access. Enterprise security infrastructure elements are placed between the tiers to manage access to corporate information. Each network tier may consist of several network segments, but must not include any network segments that are part of another tier. The reason for this is that a shared network segment may bypass the security controls.

Technology plays a key role in the tiered network model. The infrastructure elements used between each network tier filter and control access to the other network tiers. These elements are typically routers and firewalls. The configurations and rule sets applied to these elements are based on the enterprise security policy, which states the type of information permitted to pass between the network tiers and the various methods used to access the information.

Tiered Network Classification

Nearly all enterprise networks with Internet connectivity can be physically separated into the network tiers listed below. Several network segments and security domains with different trust levels may exist in each network tier, but each network segment can be categorized by one of the three tiers.

- The ***Internet tier*** consists of the global Internet. The enterprise security policy does not control every device on the Internet, but does enforce requirements upon these devices accessing the enterprise network.
- The ***Extranet tier*** consists of a protected extension of the corporate Intranet. This extension is often protected by a demilitarized zone (DMZ). In some cases, the DMZ is the extranet tier.
- The ***Intranet tier*** consists of the private enterprise network.

The enterprise security domains may exist in different network tiers. The user and transport security domains are common to every network tier. The bastion domain normally exists in the extranet tier, and the data domain normally exists in the intranet tier.

Interconnectivity between network tiers must be validated. Thus a security domain should not span two network tiers since this would violate the security rule sets between the network tiers. Authentication and authorization controls inherited from the policy are implemented on the enterprise security infrastructure elements between the network tiers. The interconnectivity between network tiers is described below.

- ***Internet to Extranet*** – typically requires user ID and password authentication
- ***Extranet to Intranet*** – typically requires strong authentication such as tokens with personal identification numbers or digital certificates

- ***Intranet to Internet*** – typically requires no authentication, however user ID and password are recommended
- ***Intranet to Extranet*** - typically requires no authentication, however user ID and password are recommended

Conclusion

An important task that a network team should do before building an enterprise network is to consult with the information security team to develop enterprise security architecture before deploying technology. This should be the case with every IT project that has impact to enterprise security. The information security team should provide a conceptual design with accompanying policies, standards, and guidelines that can be implemented in a consistent, structured, and affective manner.

The approach to enterprise security architecture described in this paper provides that consistent, structured, and affective enterprise security model. It streamlines the decision process of security personnel deciding where to place information or network elements by suggesting standards for data classification and placement into security domains. It provides efficiency by suggesting levels of trust that may be used to avoid duplicate authentication and authorization processes, not to mention save the user time and aggravation. It also describes a model used to physically partition the enterprise network, which provides physical protection of corporate information from unauthorized access.

In closing, enterprise security architecture should be a dynamic process that consistently enforces enterprise security among all users to protect corporate information.

List of References

Information Security Forum. Information Security Standards. London: Information Security Forum, September 2001. p.1

Vance, Bill. "Employees are your greatest assets… in security too!" March 2001. www.techxans.org/resources/techxans.ppt

Schneier, Bruce. Secrets and Lies - Digital Security in a Networked World. New York: JohnWiley & Sons, August 2000. p.135-187, 255-317, 367-388

Aronson, Jules P. "Site Security Handbook." Request For Comment 2196. September 1997. p.6 http://www.ietf.org/rfc/rfc2196.txt?number=2196

Holbrook, Reynolds. "Site Security Handbook." Request For Comment 1244. July 1991. p.9-23 http://www.ietf.org/rfc/rfc1244.txt?number=1244

Convery, Sean, Trudel, Bernie. "Cisco – SAFE: A *Security* Blueprint for *Enterprise* Networks." 2001. http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm

King, Dalton, Osmanoglu. Security Architecture Design, Deployment, & Operations. New York: RSA Press, 2001. p.13-39, 41-65, 111-138, 141-175

Nichols, Ryan, Ryan. Defending Your Digital Assets Against Hackers, Crackers, Spies, & Thieves. New York: RSA Press, 2000. p.41-118, 393-434

Lescher, Anne B. IBM Security Architecture – Securing The Open Client/Server Distributed Enterprise. Poughkeepsie: Open Software Foundation, Inc. 1995. p.1-1 – 1-6, 3-1 – 3-8, 4-1– 4-7

Vilcinskas, Markus. "The Need for a Security Architecture." Security Entities Building Block Architecture. 2000.
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/secentbb.asp

Benson, Christopher. "Basic Risk Assessment." Security Planning. 2000.
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/secplan.asp

McGhie, Lynda. "A Model for a Secure Distributed Computing Environment." Computer Security Journal. Volume X, Number 2, 1994. P.27-36

Swanson, Guttman. "Generally Accepted Principles and Practices for Securing Information Technology Systems." National Institute of Standards and Technology. September 1996.
p.11-38 http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

Last Updated: October 2nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Seattle 2013	Seattle, WAUS	Oct 07, 2013 - Oct 14, 2013	Live Event
SANS Baltimore 2013	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SEC760 Advanced Exploit Development for Penetration Testers	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SANS Bangalore 2013	Bangalore, IN	Oct 14, 2013 - Oct 26, 2013	Live Event
GridSecCon 2013	Jacksonville, FLUS	Oct 15, 2013 - Oct 17, 2013	Live Event
Healthcare Cyber Security Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 24, 2013	Live Event
Securing the Internet of Things Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 22, 2013	Live Event
SANS Tokyo Autumn 2013	Tokyo, JP	Oct 21, 2013 - Oct 26, 2013	Live Event
ICS410	Sterling, VAUS	Oct 21, 2013 - Oct 25, 2013	Live Event
October Singapore 2013	Singapore, SG	Oct 21, 2013 - Nov 02, 2013	Live Event
SANS Dubai 2013	Dubai, AE	Oct 26, 2013 - Nov 07, 2013	Live Event
FOR572 Advanced Network Forensics and Analysis	Washington, DCUS	Oct 28, 2013 - Nov 02, 2013	Live Event
SANS Chicago 2013	Chicago, ILUS	Oct 28, 2013 - Nov 02, 2013	Live Event
MGT415 at (ISC)2 SecureSoCal 2013	Manhattan Beach, CAUS	Oct 31, 2013 - Oct 31, 2013	Live Event
SANS South Florida 2013	Fort Lauderdale, FLUS	Nov 04, 2013 - Nov 09, 2013	Live Event
SANS DHS Continuous Diagnostics & Mitigation Award (CDM) Workshop	Washington, DCUS	Nov 06, 2013 - Nov 06, 2013	Live Event
MGT415 at (ISC)2 SecureDallas 2013	Dallas, TXUS	Nov 06, 2013 - Nov 06, 2013	Live Event
SANS Pen Test Hackfest Training Event and Summit	Washington, DCUS	Nov 07, 2013 - Nov 14, 2013	Live Event
SANS Sydney 2013	Sydney, AU	Nov 11, 2013 - Nov 23, 2013	Live Event
SANS Korea 2013	Seoul, KR	Nov 11, 2013 - Nov 23, 2013	Live Event
Cloud Security @ CLOUD Expo Asia	Singapore, SG	Nov 13, 2013 - Nov 15, 2013	Live Event
SANS London 2013	London, GB	Nov 16, 2013 - Nov 25, 2013	Live Event
SANS San Diego 2013	San Diego, CAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
FOR585 Adv Mobile Device Forensics	Vienna, VAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
Asia Pacific ICS Security Summit & Training	Singapore, SG	Dec 02, 2013 - Dec 08, 2013	Live Event
SANS San Antonio 2013	San Antonio, TXUS	Dec 03, 2013 - Dec 08, 2013	Live Event
SANS Cyber Defense Initiative 2013	Washington, DCUS	Dec 12, 2013 - Dec 19, 2013	Live Event
SANS Oman 2013	Muscat, OM	Dec 14, 2013 - Dec 19, 2013	Live Event
SANS Golden Gate 2013	San Francisco, CAUS	Dec 16, 2013 - Dec 21, 2013	Live Event
SANS Forensics Prague 2013	OnlineCZ	Oct 06, 2013 - Oct 13, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced