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 (Security 401)"
at http://www.giac.org/registration/gsec

Building an Enterprise Security Architecture

Michael Roberti

Introduction

Large IT organizations face challenges not found in smaller companies.. In a small company it is not uncommon for the System Admin group to be responsible for maintaining the NT and Unix servers, account administration, network security and in their spare time maintain the company Web presence. In a larger organization it is common to have a group dedicated to each of the above functions and not even report to the same manager. While this improves quality and may be more efficient in many ways it also increases the risk of miscommunication, and inconsistent standards. This is especially true in the security arena. Building an Enterprise Security Architecture (ESA) can minimize this risk.

What is a Enterprise Security Architecture

MSN Encarta dictionary defines Architecture as "**structure of computer system:** the design, structure, and behavior of a computer system, microprocessor, or system program, including the characteristics of individual components and how they interact."

According to Ken Cutler, CISSP, CISA, Managing Director of Information Security Institute, "A well-defined security architecture links all necessary security controls to a combination of design, baseline administrative controls, business drivers, legal requirements, and threat scenarios. It ensures that all the necessary physical, administrative, and technical safeguards are in place and in sync with each other and with the overall IT architecture and business culture."

An ESA is a document that describes the security design, tools, processes and activities that are used to protect the enterprise and how they interact with each other. In many organizations the security structure was grown piecemeal as security issues became known. Rhonda Henning at a recent IMF conference referred to it as a band-aid approach to security versus defense in depth. Building an ESA is documenting current architecture, it's planned migration, and how the plans relate to the business objectives. The ESA should be considered a living document and updated as plans are accomplished, technology changes and new risks are discovered and improvements are made to the architectural structure.

Why have a Enterprise Security Architecture

As stated earlier as job functions become more distinct and distributed security is often overlooked. In one large organization when asked how data access request were currently authorized all the parties involved stated they didn't know because the other group handled the authorization piece. Although this organization had a policy requiring access

© SANS Institute 2000 - 2005 Author retains full rights.

authorization in fact access to these particular applications were given to anyone who requested it. Going through the process of building the ESA is almost more important than the actual final product. It may well bring to light weaknesses which would not otherwise surface.

Having an ESA also assists in the process of budgeting for security tools and personnel. CIO and IT Heads struggle with security spending because it is difficult to see any return on investment. Having a document that defines the current security architecture makes it easier to justify and communicate to non-security individuals what needs to be done and why. Using the common analogy of security being similar to a chain and only as strong as its weakest link, an ESA helps find and explain the weak link. Including business objectives associated with security within the document will also assist management in the understanding of the need for security in the enterprise.

Finally, having everything included in one major document has the added benefit of having one location to go to when addressing a security issue. Policies and procedures are very important and need to be a part of every organization but if no one knows they exist or where to find them then they are not worth the effort it took to write them. The process of building the ESA also builds agreement across functional areas and management acceptance. This will help with the compliance and enforcement of security practices.

Approach

There are many ways to build and architecture. Determine what your scope and approach is going to be is the first step. Utilizing knowledge groups your organization may belong to like Gartner, Giga or Metagroup can help formalize a process. Giga has provided the following guidance:

1. Gather current and emerging Security requirements from the divisions/business units
2. Perform a baseline analysis to determine "current state" of the Security effort
3. Identify gaps in the "current state"
4. Articulate an architecture in functional terms to address the gaps and incorporate emerging business requirements.
5. Identify and communicate a "desired state" environment
6. Craft architecture blueprints to evolve the environment from current state to desired state.
7. Select standards and develop policies to implement the Security program within the context of the chosen architecture.

Use the Team Approach

The most effective way to build and ESA is to have a cross functional team working together to address all the issues. The tendency is for security managers to want to

© SANS Institute 2000 - 2005 Author retains full rights.

maintain complete control of the ESA. Having other functional groups invited prevents issues falling through the cracks and creates a shared vision among the organization.

Including Operations, System Administration, Application development/support and possibly even non-IT employees will help in the distribution of the workload and also the ultimate buy-in from the rest of the organization. At the same time you must be careful not to make the team so large it is inefficient. Depending on your organizational structure it is wise to have one or two people from a group who then can be your liaison for areas under that groups control. For example if Exchange and NT administration is included in one organizational group you may decide to only include one person on the team from that group who may be an expert in NT but they then can go and get input for any Exchange related questions.

Identify the business objectives associated with the security focus.

Understanding what the business requires is a fundamental step in defining your architecture. Not taking a high level view of how security interacts with the business tends to lead to the band-aid approach to security. The first step is to identify some high level business objectives. Some possible example include:

1. Safeguard Company A information assets from unwarranted use.

2. Safeguard the proprietary information of our partners, vendors, suppliers and customers.

3. Provide efficient local and remote access to approved information.

4. Maintain a security architecture that is cost effective, fault tolerant and easy to monitoring.

5. Protect Company A from possible legal liabilities due inappropriate use of I/S resources

.

Once the high level objectives are defined,
add some lower level requirements:

The Company A security system shall safeguard Company A information assets from unwarranted access or corruption while providing approved access to the Company A user community.

i. The Company A security system shall provide a means to ensure access to Company A information assets is granted only to fully authorized individuals.
ii. The Company A security system shall provide a means to ensure timely removal of access to Company A information assets due to changes in employment,

© SANS Institute 2000 - 2005 Author retains full rights.

strategic partners or customer relationships.

iii. The Company A security system shall provide automatic alarms, alerts and lockouts against unauthorized attempts to access Company A information assets.
iv. The Company A security system shall be capable of withstanding probable security risks as determined by an annual independent threat assessment.
v. The Company A security system shall provide the ability to encrypt Company A information assets as needed.

The Company A security system shall safeguard the proprietary information and systems of our partners, vendors, suppliers and customers from unauthorized access or corruption.

i. The Company A security system shall provide an audit trail for all authorized and unauthorized access to partners, vendors, suppliers and customers systems or information through Company A assets.
ii. The Company A security system shall provide automatic alarms, alerts and lockouts against unauthorized attempts to use Company A assets to access partners, vendors, suppliers and customers proprietary systems or information.
iii. The Company A security system shall be capable of thwarting the use of Company A assets to compromise partners, vendors, suppliers and customers proprietary systems or information as determined by an annual independent threat assessment.

The Company A security system shall provide the Company A user community efficient local and remote access to approved information assets.

i. The Company A User community shall be capable of performing all of the functions and exercising all of the capability from their remote location that they were authorized to perform when on the Company A LAN.
ii. The Company A security system shall be designed to minimize impact to remote user performance.
iii. Company A security system shall include mechanism to identify unauthorized connection points within the network structure.
iv. Company A security system shall include procedures to authorize and maintain alternative entry points within the network. i.e. modems

The Company A security system shall maintain a security architecture that is cost effective, fault tolerant and easy to monitoring.

i. The cost of maintaining the security architecture and operations shall be comparable to the best-of-breed companies as determined by annual benchmarking.
ii. The Company A security system shall be capable of continuing to protect Company A assets and partners, vendors, suppliers and customers proprietary systems or information in the event of any single hardware or software failure.
iii. The Company A security system shall provide an audit trail for all authorized and

© SANS Institute 2000 - 2005 Author retains full rights.

unauthorized access to systems or information.

iv. The Company A security architecture shall be defined by an annual security roadmap that is created and controlled by the Security and Architecture Services Directorate.

The Company A security system shall protect Company A from possible legal liabilities due inappropriate use of I/S resources.

i. The Company A security system shall automatically detect and report any inappropriate use of Company A assets by the Company A user community .
ii. The Company A security system shall automatically terminate any inappropriate use of Company A assets by the Company A user community.
iii. The Company A security system shall address the need to inform employees, partners, vendors, suppliers and customers of the importance of security and their role in its implementation.
iv. The Company A security system shall enforce Federal guidelines in controlling access to Company A information assets as required.

Once the objectives are defined it becomes the driving force in deciding to implement a new security technology. Just because PKI technology is available doesn't mean your organization needs to go through the expense of implementing it. If it cannot be linked to a business requirement it probably does not need to be implemented.

Perform and document a baseline analysis and determine the desired state

It is important to document the current state of security within the enterprise. Without this step it is impossible to identify the gaps that may exist. This is a good time to have a third party do a security analysis of your systems. There are many companies who perform this function including ISS, Axent (now part of Symantec) and of course the big consulting firms. Axent uses al life cycle security model, which includes most of what, will be in the ESA and they do their analysis using this full cycle approach. It may be more cost effective to utilize a small local security firm but make sure you check their credentials before trusting your enterprise to them. The report you receive from an analysis can be use as the start of your baseline and more importantly the next step of identifying gaps.

Because of the overlapping nature of security the baseline should be looked at from multiple views. One approach is to document it by services, a service being defined as an application or infrastructure. Some examples would be the Network, financial systems, or possibly an ERP system. Utilizing a graphical tool such as Visio is a good way to present the devices that make up a service. Document the network infrastructure by having a graphical view of all the routers, switches and network security products (firewalls, intrusion detections systems) that are utilized. Document a PeopleSoft HR system in the same manner showing the network components as well as the host systems the citrix or web front-end systems etc.

© SANS Institute 2000 - 2005 Author retains full rights.

The next view is a descriptor view of the security aspects of each of the areas identified in the graphical view. To insure all areas are covered first list each major component of security that should be included by that area and then document each one. Below is an one example of the security aspects by area:

Network
Logging/Auditing of network devices
Firewall (types, management, procedures)
Remote Access
Passive intrusion detection

Services/Applications
Account authorization
Account termination
Accounts Lockout and Password Settings
Intrusion Detection
Data handling requirements
Application misuse protection – viruses, buffer overflows etc.
CM Controls
Logging/Auditing

Platforms/Servers/Devices
Patch levels and procedures to update as new ones are released
Account authorization
Account termination
Accounts Lockout and Password Settings
Intrusion Detection
Data handling requirements
Logging/Auditing

Data handling
Notebooks and laptops
VPN issues
Home workers
E-mail encryption
Anti-virus

Corporate image/liabilities
Internet monitoring
Email monitoring
Mail relaying
Spam

Other
Incident Response

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

DRP
Backups
Physical Security
As you document the states for each of the above, decision will have to be made on what level to go to. If you have 1000 NT servers in your enterprise you probably will not want to document the patch level for each one. You will want to document what the desired security build is and a process to insure each one is upgraded in a timely manner. You may also have to categorize servers if there are requirements for different levels of security due to the interaction of patches and applications. The important thing is to cover all areas and identify who has the responsibility in the process. Having auditing turned on for your servers doesn't do any good if no one is assigned to monitor the logs. Or in the earlier example of account administration document how authorization is granted for every application/service.

As you develop the above list and document the current state of each identified area, gaps in your security architecture should become evident. Some of the gaps may already have been identified and plans put in place to address the risks, others may not have had any thought given to them. The current state and the desire state can be included in the same document. Each document should have three parts, current state, current plans and future enhancements.

To determine future enhancements some research will be required. This is why the team approach works best. If the above areas are assigned to the functional representative then the documentation and research can be spread out and not overwhelm the security staff. For example, if you are not using email encryption but know there will be a requirement in the future for it, the expected enhancement should be included in this document. Your teammate who is an expert in email should be the person tasked to evaluate the possible options. There are many sources of information to determine possible options and best of breed solutions for the above areas. One of the best is the Sans organization. (www.sans.org) The new reading room area is a wealth of information and is in a format which is easy to understand and digest quickly. The security magazines, Information Security and InfoSecurity are free and also available on line (www.infosecuritymag.com & www.infosecnew.com). Another great place for research are the security portals now available on the Internet www.infosyssec.net & www.securityportal.com are two places with easily searchable security information.

Prioritize and develop plans to address gaps and future enhancements

Once you have everything documented it is necessary to determine what and when the enhancements should be done. As Rhonda Henning presented at the IMF conference to determine the optimum solution (security architecture) it is necessary to balance cost, performance and functionality. Most Security Managers would agree with unlimited budget for staff and tools security would not be as difficult to manage. But the reality is most security organizations are under strict budget constraints.

© SANS Institute 2000 - 2005 Author retains full rights.

This is another area the team approach is best utilized. The team should evaluate the proposed enhancements and rate them on functionality, costs, ease of implementation, and possible disruption to the business. An effective approach to utilize in this prioritizing process is to develop a matrix showing the enhancements with a rating for each area. Once the matrix is populated it easily facilitates the building of a blue print of projects their priority and scheduled deployment. The blue print becomes a important piece of the ESA and valuable while preparing budgets and strategic plans.

Policy and Procedures

Policy and procedures are the backbone of any good ESA. "Consistency in applying security safeguards requires the development of written guidelines for the secure configuration of operating systems, databases, Web servers, routers, and other software and hardware. Implementing software "bug" fixes and patches on a consistent, timely basis is also critical. To be effective, technical security guidelines must be developed by well-directed workgroups involving the affected parties (e.g., IT management, administrators and engineers) as well as security and audit practitioners." Ken Cutler, CISSP, CISA, Managing Director of Information Security Institute. Any organizational policies, which address security issues, should be included in the ESA. As you complete the ESA the current policy should be evaluated against the current and future state documents to determine if additional documents are required. A great resource for developing security policy is Information Security Policies Made Easy by Charles Cresson Wood, CISA, CISSP. Pentasafe (www.pentasafe.com) also has a tool available based on this book which is used to develop and manage an organizations security policies.

Conclusion

While building and Enterprise Security Architecture takes time and resources the effort is worthwhile. You will have a document that will help insure you know the security status of your enterprise and it also provides continuity if the organization undergoes personnel changes.

References and Resources

Information Security and IT Audit Edition of TransMISsion Online, the e-newsletter from MIS Training Institute 2/21/01

Developing an Enterprise Security Strategy and Keeping it Current Rhonda Henning, Information Management Forum, Toronto Canada 3/26/01

MSN Encarta Dictionary, http://dictionary.msn.com Apr '01

© SANS Institute 2000 - 2005 Author retains full rights.

Philip J. Rosch, Giga Information Group Dec. ‘00

Pentasafe Corporation web page (www.pentasafe.com) Apr ‘01

Information Security www.infosecuritymag.com Apr ‘01

InfoSecurity (www.infosecnew.com). Apr ‘01

INFOSYSSEC The Security Portal for Information Security System Professionals www.infosyssec.net Apr ‘01

Security Portal The Focal Point for Security on the Net. www.securityportal.com Apr ‘01

Information Security Policies Made Easy version 7, ISBn #1-881585-06-9 by Charles Crisson Wood, CISA, CISSP, Baseline Software, Inc. Oct. 1999.

© SANS Institute 2000 - 2005, Author retains full rights.