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
"Intro to Information Security (Security 301)"
at http://www.giac.org/registration/gisf

GIAC Enterprise Security Policies for an ASP with Hosted Production Network

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

Iztok Umek
GIAC-GISO Basic
Practical Assignment (v1.1)
27 December 2001

© SANS Institute 2000 - 2005 Author retains full rights.

Introduction

GIAC Enterprises is a leading provider of collaborative commerce solutions for logistics delivering the next level of competitive advantage and cost improvement in supply chain management. GIAC Enterprises offers this value through its Internet-based GIAC Enterprises Network application and Logistics Consulting Services. GIAC Enterprises optimizes logistics activities across supply chain networks by enabling cross-enterprise asset utilization, providing complete supply chain visibility and automating inbound and outbound transportation and distribution management activities. GIAC Enterprises delivers its solution via an ASP model.

IT Infrastructure

GIAC Enterprises IT infrastructure is divided into two primary areas; the Corporate Office network and the Production network. Additionally, the Corporate Office network is divided and consists of a demilitarized zone (DMZ) and an internal (private) network (see attached GIACenterprises.PDF diagram for details).

Secure connection between the Corporate Office network and the Production network is provided by a network-to-network VPN connection using VPN-1. A VPN client-to-network connection is also used to connect remote developers, sales and support personnel to the Corporate Office network.

The Corporate Office internal network includes an Exchange e-mail server, a Windows 2000 file and print server, as well as application and database servers for development and QA environments. Application and database servers are UNIX servers (Linux and SUN Solaris 8) and run WebLogic, webMethods and Oracle software. Development workstations run Windows 2000 Professional.

The Corporate Office DMZ network includes a primary DNS server (Linux), an Outlook Web Access (OWA) server (Windows 2000) for web e-mail interface for employees and a training application server (SUN Solaris 8).

There is a network intrusion detection server with probes in DMZ and the Internal network installed at the corporate office.

The Corporate office is connected to the internet through a firewall and router with two T1 lines for redundancy purposes.

© SANS Institute 2000 - 2005 Author retains full rights.

GIAC Enterprises hosts a production network with a managed hosting provider that has multiple connections to Internet backbone providers. The hosting provider manages firewall (with VPN), routers and Cisco CSS 11000 layer 7 switches (used for load balancing of the web application). They also manage Oracle dynamic fail over (DFO) cluster database servers for the production application. GIAC Enterprises is responsible for maintaining applications on application servers.

Business Operations

GIAC Enterprises Information Technology (IT) needs are primarily divided into two main categories. First is the support of basic corporate functions including IT support for HR, Client Services, Financial, Development, and other corporate departments and needs. Second is the support of the production environment for clients. GIAC Enterprises does its main business as an Application Service Provider (ASP).

GIAC Enterprises customers use web interface and EDI interfaces (http/https/ftp, depending on client needs) to send and receive information and use the GIAC Enterprises Network application in the production network. They also access the same application located in Corporate DMZ network for training purposes. This ensures their production data is protected while they train on new or existing features of the network application. There is no direct network connection between the customers' networks and with any of the networks of GIAC Enterprises, all connections are done on the application level. Access to the data stored in database servers is also only done through application servers on the application level, as customers don't need direct access to the database.

Maintenance of the application is conducted remotely from the Corporate network through server-to-server VPN-1 connections with Production network as well as using ssh protocol.

GIAC Enterprises employees use general office network resources (Exchange, Windows 2000 file and print server, printers) as well as their Windows 2000 Professional workstations. Developers, database, network and system administrators additionally use other servers that are predominantly UNIX (Linux, SUN Solaris 8) for application development and support.

Employees can use Outlook Web Access (OWA) to read mail while not in the office. Additionally some remote employees have client-to-network VPN connection to the Corporate network to access other network resources. Remote employees include sales associates, telecommuters as well as support personnel that need remote access in order to support production application and other corporate services based on external and internal Service Level Agreements (SLA).

Because the majority of employees work in the development area, GIAC Enterprises decided to use a liberal outbound traffic policy and only restrict access from DMZ and the Production network. All inbound traffic policies are based on business needs. Access to

© SANS Institute 2000 - 2005 Author retains full rights.

production and training web interface is controlled by username/password as customers can use the application from anywhere on the Internet. Access to EDI interfaces is additionally controlled by the Access Control List (ACL) on firewalls.

In addition to the application access, inbound SMTP is allowed access to the Exchange e-mail server (firewall does SMTP queue/de-queue so direct access is not possible) and DNS queries are permitted to the DNS server in DMZ.

Security Policy

Areas of Risk

Remote Access

Remote access is a major security concern of GIAC Enterprises as it practically extends its network beyond its physical boundaries. Remote employees using VPN extend the network to include the computer with which they are working. In some cases this is their home computer; thus, outside the immediate control of GIAC Enterprises Systems Group.

Having their computer virtually appear in the GIAC Enterprises Corporate network (behind the firewall) exposes the network to many risks. Those risks include introduction of viruses and other malicious code (such as trojans) in the network. Remote computers can act as a gateway between the Internet and the internal network and, if compromised, can be used to retrieve sensitive information as well as destroy the information on the network servers.

With successful exploit of remote computer using VPN to GIAC Enterprises, an attacker would gain access to the network and possibly gain further access to network servers. If this exploit was not detected, an attacker could further compromise some of the network servers. From compromised servers one could retrieve (or destroy) sensitive documentation such as sales information, financial information and even source code for the GIAC Enterprises Network application. In the worst case, if such information (i.e. source code) was compromised (sent to competitors, introduced with backdoors) it could, in effect, force GIAC Enterprises out of business. The damage could be measured in millions of dollars in lost revenue and opportunities.

At least three steps can be taken to mitigate this risk.

1. Up-to-date anti-virus software must be run on all computers that have access to the

© SANS Institute 2000 - 2005 Author retains full rights.

network (even through VPN). This will minimize the risk of introducing viruses to the network.

2. Personal firewall software must be run on remote computers. This will minimize the risk of compromising the remote computer itself and using it as a staging point to attack other network resources.

3. Prohibit so called split-tunneling when using VPN. Doing this will restrict the remote computer to only allow connections to internal network while using VPN and prevent the remote computer from acting as a gateway between the Internet and the internal network.

The cost to successfully implement these three steps to mitigate the risk with remote access would be:

1. Anti-virus software: approximately $50 per remote computer (if the computer is a personal computer, as corporate computers already have licensed ant-virus software)

2. Personal Firewall: there are free solutions, but most are approximately $40 per remote computer

3. Introduction of VPN client that allows installation of security policies: approximately $2000 per 25 users.

Information Leakage

Information leakage is another large concern for GIAC Enterprises. It is a problem that is hard to solve with technical solutions. GIAC Enterprises heavily relies on its employees to protect its most valuable asset – information. Sensitive information can be found in various forms such as time sensitive documentation, financial documentation, source code, etc. Employees with access to such information can knowingly or not knowingly disclose this information to the outside.

Employees (or others trusted with such sensitive information) can expose such information in various ways including sending e-mail, leaving their local (or even remote) computer unprotected (sometimes even during a VPN session to corporate network), leaving sensitive documents on their desks, throwing documents in the garbage without shredding them, etc.

If such sensitive information would be exposed by an employee (or other person trusted with it) the damage could be substantial. Leaking of sales and financial information could cost GIAC Enterprises tremendously in lost opportunities.

The major mitigation factor for this risk is sufficient security awareness and training for users.

© SANS Institute 2000 - 2005 Author retains full rights.

Weak authentication

As with many enterprises this is substantial concern. Users need to authenticate before they can use their computers and other network resources. Most systems at GIAC Enterprises support at least username/password method of user authentication. Upon successful authentication, users are granted permissions to use various network resources (including access to source code and other documentation).

If the authentication method is not strong enough, (i.e. weak password) an attacker can pose as a legitimate user and gain access to all resources of that particular user as well as to other resources.

The consequences of successfully exploiting this vulnerability would allow the attacker to gain access to all resources that the compromised username has. An attacker could also use this compromised account to gain further access to other systems (perhaps even accounts such as root or administrators account). By gaining access to an account with sufficient privileges an attacker could possibly gain access to sensitive information.

To mitigate such a risk, systems administrators should implement a certain degree of complexity to their passwords. Furthermore, an alternative method could be used (such as one-time passwords). Introducing additional methods of authentication improves this system as combination of "what I know" (username/password), "what I have" (SecureID cards), "what I am" (retina scan, fingerprint) is introduced.

While introducing complexity into passwords and using one-time password methods are fairly cheap (largest requirement is the time to implement as many modern operating systems already support it), introducing additional levels (SecureID cards, retina scanners, fingerprint scanners) can be quite expensive.

Server Security

Network Servers are actually the place where most of the information in possession of GIAC Enterprises is stored. Therefore, it is logical that the security of such servers is very important for the corporation.

Exploiting various bugs on servers could allow an attacker to gain access to the information stored at compromised servers. Stored information varies from source code of the GIAC Enterprises Network application to financial and other vital corporate information. In addition to bugs there are other ways to compromise servers (password guessing etc…)

As with the previous risks, the consequences to the company could be catastrophic,

© SANS Institute 2000 - 2005 Author retains full rights.

especially in conjunction with information leakage risk.

To minimize the risk of compromised servers several steps could be made, most notably:

- Installation of up-to-date anti-virus software on the servers
- Installation of host based intrusion detection software
- Installation of some sort of access control list (ACL) software such as tcp-wrappers
- Installation of latest OS security patches
- Disabling services that are not used
- Adequate monitoring of server logs for anomalies

Risk of Computer Viruses

The latest outbreaks of malicious viruses and worms on the Internet has caused concern for every organization. Because of the widespread use of Microsoft e-mail products (such as Outlook) and their included vulnerabilities, the spreading of viruses and worms on the Internet can quickly get out of control.

Various viruses and worms might compromise sensitive data by destroying it or spreading it to other people. There have been several examples of malicious software sending out documents from the "My Documents" folder.

As with the previous risks, the consequences to the company could be catastrophic, loss of data can cause major delays in the release of new products, certain documents can migrate outside of the network of intended recipients, etc.

To mitigate this risk, all workstations and servers (e-mail and file servers) should run the latest up-to-date anti-virus software. Users should also be aware of the potential danger of clicking e-mail attachments and downloading files from untrustworthy sources.

Security Policies

The Remote Access Policy, Information Sensitivity Policy and Server Security Policy are found in appendices and address some of the areas of risk presented above. I found that SANS web page with security policies is an excellent source for start up companies that among other things battle with establishing security policies and procedures. Policies there are written so generic that it fits majority of companies that heavily depend on IT.

© SANS Institute 2000 - 2005 Author retains full rights.

Security Procedures

Server Security Procedure is found in appendices.

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

© SANS Institute 2000 - 2005 Author retains full rights.

Appendices

- GIACenterprises.pdf – network diagram of GIAC Enterprises
- Remote Access Policy
- Information Sensitivity Policy
- Server Security Policy
- Server Security Procedure

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

© SANS Institute 2000 - 2005 Author retains full rights.

References

Yusof, Asmuni. "Ways to Become an Effective Information Security Professional – from a GIAC Wannabe's Perspective." 1 October 2001. http://www.sans.org/infosecFAQ/start/professional.htm (10 December 2001).

SANS. "The SANS Security Policy Project." http://www.sans.org/newlook/resources/policies/policies.htm (27 December 2001).

SANS "Remote Access Policy" http://www.sans.org/newlook/resources/policies/Remote_Access_Policy.pdf (27 December 2001).

SANS "Information Sensitivity Policy" http://www.sans.org/newlook/resources/policies/Information_Sensitivity_Policy.pdf (27 December 2001).

SANS "Information Sensitivity Policy" http://www.sans.org/newlook/resources/policies/Information_Sensitivity_Policy.pdf (27 December 2001).

SANS "Server Security Policy" http://www.sans.org/newlook/resources/policies/Server_Security_Policy.pdf (27 December 2001).

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

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: May 1st, 2017

Upcoming Training

Click Here to {Get CERTIFIED!}

SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
Community SANS Chattanooga SEC301	Chattanooga, TN	May 15, 2017 - May 19, 2017	Community SANS
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Atlanta 2017	Atlanta, GA	May 30, 2017 - Jun 04, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Raleigh SEC301	Raleigh, NC	Jun 19, 2017 - Jun 23, 2017	Community SANS
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
Community SANS Fort Lauderdale SEC301	Fort Lauderdale, FL	Jun 26, 2017 - Jun 30, 2017	Community SANS
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
Community SANS Toronto SEC301	Toronto, ON	Jul 10, 2017 - Jul 14, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Boston SEC301	Boston, MA	Jul 24, 2017 - Jul 28, 2017	Community SANS
Security Awareness Summit & Training 2017	Nashville, TN	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio Fall 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Network Security 2017 - SEC301: Intro to Information Security	Las Vegas, NV	Sep 11, 2017 - Sep 15, 2017	vLive
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced