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

GISO Version 1.3

GIAC Enterprises

- A Financial Services Company -

Kevin Agnew
May 19th, 2003

© SANS Institute 2003, Author retains full rights.

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

Table of Contents

Summary **3**
1. GIAC Enterprises Overview **3**
Business Services 3
IT Infrastructure 4
Retail Outlets 4
Head Office 4
Business Operations 7
2. Risks **9**
Transactional Data is compromised 9
Significance to GIAC 9
Impact to GIAC 9
Recommended Actions 10
Unauthorized access from a Retail Outlet 10
Significance to GIAC 10
Impact to GIAC 10
Recommended Actions 11
Denial of Service attack against Firewall 11
Significance to GIAC 11
Impact to GIAC 11
Recommended Actions 12
3. Evaluate and Develop Security Policy **12**
Evaluation 12
Purpose 12
Scope 12
Policy Statement 12
Responsibility 13
Action 13
Revision 13
4. Develop Security Procedures **16**
Appendices **18**
A. Network Diagram 18
B. Security Policy 19
References **22**

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

Summary

GIAC Enterprises is in the consumer foreign exchange business. Retail outlets are spread across the United States with site to site VPNs used to provide network connectivity. In addition to the public retail locations GIAC also provides an online offering for customers to conduct financial transactions.

Three specific concerns facing GIAC, the protection of transactional data, preventing unauthorized access from a Retail location and a Denial of Service attack against the corporate firewall will be evaluated. Details such as the relevance of the threat, consequences to GIAC and recommended actions will be identified.

An evaluation of an existing Secure Server policy will be discussed in terms of it's relevance to GIAC. It will be revised to more suit the GIAC environment with the purpose to mitigate some of the risks. A documented procedure outlining the necessary steps to obtain authorization to connect a server to the internal network is then derived in support this revised policy to ensure compliance.

1. GIAC Enterprises Overview

Business Services

GIAC Enterprises is a financial services company that has been providing foreign currency exchange, draft and wire services to the general public for the past eighteen years. There are six hundred employees in total, one hundred fifty of which work at the head office located in Washington D.C. The remaining staff is employed at the retail branches located throughout the United States. There are no branches outside the U.S.

The retail network consists of one hundred geographically dispersed branches located mainly at airports and shopping malls. There are anywhere from one to five employees at each site, dependant on customer volume and the necessary hours of operation of the respective location. Customers are able to purchase drafts, send wires, and convert currency at every location. Payment can be made by a number of methods including credit card.

As part of the due diligence in selling financial services, GIAC Enterprises is required to do an Office of Foreign Assets Control check for each transaction. If a positive hit is returned GIAC is not allowed to conduct the transaction and must report it.

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

> "The Office of Foreign Assets Control ("OFAC") of the U.S. Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. OFAC acts under Presidential wartime and national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze foreign assets under US jurisdiction." [1]

The USA Patriot Act[2] provides specific guidelines for the operations and reporting required by GIAC Enterprises with respect to Money Laundering. To support these requirements GIAC has Audit, Compliance, Finance and Accounting teams located at Head Office. Semi-annually members of the Audit group visit each Retail location to ensure company policies and procedures are being followed.

In addition to the walk up outlets, customers can also order foreign currency online for next day delivery. This web server is hosted at corporate head quarters.

The Information Technology (IT) department is located centrally but is responsible for the support and maintenance of the retail network as well. IT requires VPN access for remote support. Remote VPN access is also available to those authorized users.

.

IT Infrastructure

Retail Outlets

Communication from the retail branches is conducted through a site to site VPN tunnel. The workstations at the retail locations are Windows 2000 Professional. Each branch is networked, shares a laser printer and has Business grade DSL, with a dynamic IP, installed. A Nokia IP30, running a SOHO version of Checkpoint Firewall software, is installed at each branch to establish a VPN tunnel with the head office. As the IP is dynamic communication must be initiated from the retail site. Internet Browsing and any other related services are not allowed at the branch. The only accessible web site is the corporate Intranet. The site is used primarily for communication purposes but also provides financial details as to the profitability of each branch. The SOHO firewalls are configured to allow only traffic through the VPN tunnel to head office for the required services (Intranet, E-mail, Domain Controller, transaction processing).

Head Office

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

Head office uses a Cisco 2621 running IOS 12.3T, with a 10MB Ethernet Internet connection, as the border router. It has been configured to block any broadcast packets inbound or out, any IP packet with the source routing option set and ICMP. Egress and ingress filters are also in place.

GIAC Enterprises deploys firewalls from two different vendors to protect the internal network and the transactional data. The Internet facing firewall is Checkpoint NG FP3 on Nokia IP650 platform. The operating system is IPSO version 3.6 FCS6. It is running the firewall and VPN service. The Checkpoint firewall is the VPN endpoint for all remote VPN connections. It also is configured to NAT internal IP addresses to provide further protection. A Cisco PIX 535 running the firewall and VPN service is used to protect the internal database server housing the transactional data.

The web servers in the DMZ are running Microsoft IIS 5.0 on Windows 2000 Advanced Server connected to a Cisco 2948 switch (IOS version 12.0) with 128bit SSL. The ISS RealSecure Server Sensors are installed on each web server. The ISS RealSecure Network Sensors are deployed on the external, internal and DMZ segments. DNS for the website is handled by the ISP.

The Rate server, located in the DMZ, runs Windows 2000 with F-Secure software installed. It connects through SSH to a third party service that provides foreign exchange rates. After download the rates have margins applied and are then sent to the retail branches. The RealSecure Server Sensor is running on this server.

The internal core switch is a Cisco 6509 running CatOS 12.1(8a)E3. There are three VLANs configured for the internal network. One is dedicated to servers and the other two split between the workstations.

GIAC uses three different vendors for its anti virus defense. McAfee is used on the servers, Symantec's Norton Anti-virus on the desktops and TrendMicro on the Exchange server. The deployment of virus definition files is centrally managed. Checks are done daily for new signature files.

GIAC Enterprises has two Windows NT 4.0 domain controllers to support user authentication. These servers also run the DHCP service, to handle the automatic IP configuration of the workstations, WINS and DNS for name resolution.

The Intranet server is a Windows 2000 server running IIS 5.0. It is used by the Retail branch managers to obtain their profit and loss statements on a daily basis. Access to this section is restricted to authorized users. Members of the specific Windows NT Global groups are granted read only access to the relevant reports. Other more generic material such as company communications, policies, and Human Resources forms can be found on the Intranet as well.

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

The File and Print server is a Windows 2000 server that allows departments within GIAC to share relevant information. Finance and Accounting, for example, have shared Excel spreadsheets for month end and year end reporting. All shares have restricted share permissions based on Global Group membership and also NTFS restrictions per folder or, if necessary, per file.

Microsoft Exchange 5.5 running on Windows NT 4.0 is used for e-mail. Users are not allowed to store their e-mail on the local workstation. Personal folders of any kind are not allowed.

The proprietary OFAC Database is located on the internal network at Head Office. GIAC subscribes to a 3rd party service that provides daily updates to the database. This requires only an outbound Internet connection only. F-Secure software has been installed on the server to facilitate the SFTP communication to the external server. It is an automated script that runs every night. GIAC does not consider this sensitive information as it is available to anyone with a subscription.

The transactional database is a Windows 2000, SQL 2000 server that resides behind the PIX firewall. In addition to the secure server lockdown, RealSecure Server software is also running. As this data represents GIACs 'crown jewels', GIAC uses 3DES encryption on the necessary fields.

Internal workstations are all running Windows XP. Each department manager has an approved suite of software that their staff requires to conduct the day to day operations. The IT staff has created the necessary images for each department so any workstation can be created consistently and quickly.

IT personnel are able to conduct typical health checks and troubleshooting from home. Home users must use a GIAC provided laptop, subject to the policies, procedures and security lockdowns of GIAC in order to connect remotely.

VPN access is only allowed from the retail branches and authorized home users. The VPN configuration for the retail locations is handled by the internal IT staff at GIAC. The Nokia IP 30 SOHOs are preconfigured at head office and shipped to the retail location. In order to prevent misconfigurations at the retail location a member of the IT staff is sent on site to setup the network. Branch employees have no access to the SOHO firewall. Laptops for home users are configured at head office. If there are any issues with the laptop, once it has left, that cannot be resolved over the phone it must be returned. Home users are never granted any enhanced privileges to assist in troubleshooting.

As GIAC is a Microsoft shop, Microsoft Baseline Security Analyzer is used in conjunction with the Software Update Service (SUS). This allows GIAC to keep all systems at the latest patch release. New patches are reviewed by the

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

Systems Infrastructure Manager. Upon approval they are applied to the test environment and if UAT is passed, deployed to production.

GIAC's IT Infrastructure team utilize tools from The Center for Internet Security [3] as follows,

- RAT for Cisco Routers
- Level-2 Windows 2000 Professional template
- Level-2 Windows 2000 Server template
- Level-1 Windows NT
- Top 20 Scanner

Any device deployed on the network must have the relevant security template and latest service pack applied. The TOP 20 Scanner is run on a monthly basis.

Business Operations

The crown jewel of GIAC Enterprises is the data held within the transaction database. This is contains sensitive details about customers including credit card information. The data is obtained either at the Retail branches or can be entered online by customers.

A typical day at the retail branch begins with the delivery of current exchange rates from Head Office. A server at Head Office is configured to take a rate feed from a data service, massage the data into text format, encrypt (using FileCrypt[4]) the file, and distribute it to the branches for use by the POS system. Rates are delivered to the branch before it opens and, depending on the volatility of the market, several more times throughout the day.

At the retail outlet customers are able to convert currency, purchase drafts and send wires. Transactions are entered throughout the day. Details of the transaction amount, the exchange rate, and customer particulars including payment method are all captured. There is no local database at the retail branches. At the close of business a process is run that creates a master file, detailing all transactions from all terminals for that day. The file is encrypted and sent to Head office transaction database via the VPN tunnel.

Customers also have the option of using GIACs online service allowing the convenience of ordering foreign currency online and having it delivered the next day. Customers sign up online for an account of which the details are sent to the client in two separate e-mails, one containing the username and the other the password. Once online, customers simply enter the amount and type of currency they require, a shipping address and credit card number. The Draft and wires service offered at the retail branches is not available online. The Windows 2000 IPSec service has been configured to encrypt any data sent from the Web server

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

to the back end database to protect the data in transit. Once the data is entered into the database it is processed similarly to the data from the retail branches.

The Audit department has the responsibility of protecting the assets of GIAC Enterprises from a business perspective. They make certain that the business is being run in a sound and profitable manner. This is done through periodic examinations of the branches in order to ensure that proper policies and procedures are being adhered to. Security, operations and customer service are all reviewed as part of the process. Investigations and reports on internal and external fraud and other crimes are also conducted when necessary. The auditing function is manual. Audit requires use of protected shares on the File server in order to share data with the necessary colleagues.

The Compliance Department is responsible for transaction reporting, as well as Bank Secrecy Act Audit Reporting (Anti-Money Laundering). They perform transaction analysis and suspicious activity reporting. Compliance runs reports against the database where all the transaction details are held. They are looking for trends such as small transactions conducted by the same individual at different locations, large international wire transfers and activities to high risk countries.

The Finance and Accounting departments also require access to the central database for the month end and require access to the file server to share data for items such as timesheets and expense reports.

The IT department is responsible for the support and maintenance for the retail branch locations, central servers, web servers, firewalls, routers, IDS, switches, and telephones. Onsite support at the central office is available during the business hours of 9:00 – 5:00pm. The retail branches receive telephone support and, if necessary, a technician would be dispatched for onsite issues. All IT staff have remote access to the corporate network from home so they can perform typical health checks or any necessary troubleshooting.

Employees working from home require Secure ID tokens to access the network. Outside of IT, access is restricted to e-mail and the File sharing server from home. Users can not access the operational systems that contain sensitive transactional data remotely.

In order to protect customer credit card numbers the following is a summary of what GIAC has in place,

- Cardholder data is not stored on front end systems
- Network traffic between servers is encrypted
- Firewalls configured to ‘deny all’ except for the protocols required by the business
- Latest patches applied on systems

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

- Up to date anti-virus signatures
- NAT on Internet facing firewall
- Each server in the DMZ is restricted to only one function
- Fields in the database with cardholder information are encrypted
- Unique identities for staff accessing the database

2. Risks

Transactional Data is compromised

Significance to GIAC

This data represents GIAC Enterprises crown jewels. Data could potentially be accessed by both external and internal individuals. Contained in the database are specific customer details including credit card numbers. This sensitive information must be made available to as few people as possible internally.

The article "Root of massive credit card threat found"[5] helps to convey the serious threat GIAC faces from external individuals due to GIACs online presence.

Internal to GIAC, local users require access to the same database holding the credit card information so the necessary security policies and procedures need to be in place. "Busted ID Theft Ring Part of a Growing Epidemic"[6] describes the damage internal employees can do given an insecure environment.

Impact to GIAC

In addition to the loss of the customer confidence in GIAC Enterprises, there would be financial liabilities and potential lawsuits if customer details were compromised and fraudulent charges appeared on credit cards.

The quote below provides more reason as to why GIAC needs to ensure security measures are fully enforced to protect customer information.

"With just your name, Social Security number and birth date, identity thieves are often limited only by their creativity. They can go on a shopping spree using credit cards in your name, take out large sums of money at the bank, and apply for health insurance, cell phone service or even a new job as your financially irresponsible clone. And it can take years to set the record straight."[7]

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

Recommended Actions

Mitigation of this risk would include the following,

- Protect data at rest - Relevant fields in the database are encrypted so anyone able to obtain a copy of the database would not be able to read sensitive information.
- Protect data in transit – Where possible use the Windows 2000 Server IPSEC service to encrypt any incoming and outgoing traffic between the relevant servers.
- The Cisco Pix, protecting the database, is configured to accept access from specific IP addresses only as well as only the necessary ports.
- Assign unique IDs to each person accessing the database, and restrict access to only those IDs.
- Audit database access by the Unique ID daily.
- Restrict physical access to the database.

Unauthorized access from a Retail Outlet

Significance to GIAC

In order for GIAC Enterprises to be successful in the retail market they must place their outlets in high traffic public locations, be flexible in payment methods and have currency on hand to meet the demands of customers. The combination of these items represents a vulnerability to GIAC. In addition each branch requires a connection to the corporate head office in order to receive the current foreign exchange rates and for submissions of day end files.

Intruders breaking into the site off hours would have access to the local cash supply, computer equipment and the internal network.

Impact to GIAC

There is obvious financial loss in terms of theft of the branches cash float and computer equipment as well as the lost revenue while systems are being replaced and the branch is closed.

In addition there is potential theft of financial information through use of the Intranet, or other network resources (e-mail, network shares).

Any printed material left by branch staff would be available to the intruder that may contain sensitive information.

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

Recommended Actions

Mitigation of this risk would include the following,

- Configure firewall rules to only allow VPN access from the branch during branch business hours.
- Configure the VPN tunnel to allow only the required ports.
- Video surveillance installed at all retail outlets.
- No data saved to the local machines.
- Clean desk policy be implemented. Employees are prohibited from leaving hard copies of any sensitive material of GIAC Enterprises and its operations in an open area.
- Strong password policy enforced with account lockouts after 3 attempts.
- User accounts allowed access only during business hours.
- Timed lock on local safe to prevent it being opened off hours.
- Limit the amount of currency on hand at the branch.

Denial of Service attack against Firewall

Significance to GIAC

As GIAC Enterprises is a financial company they may be targeted for an attack. The Internet facing Checkpoint firewall is critical to the business functionality so is a likely target. GIAC is vulnerable as the firewall is a standalone unit with a single connection to the Internet.

The business relies on the Checkpoint firewall for delivery of the foreign exchange rates to the retail branches and for receiving the daily transaction file. The firewall also provides access to the online web site where customers are able to conduct transactions.

Impact to GIAC

The communication to the Retail branches is based on VPN technology. If the central firewall is down, there is no communication to the branches. In this situation each site would use the last foreign exchange rates received. Depending on the fluctuation in the currency markets this could have significant impact to the profitability of GIAC Enterprises. This also prevents the daily transaction file from being submitted to head office, resulting in a delay in back office processing. The Finance and Accounting departments could not complete their work as scheduled.

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

A DoS attack would also take the web site down resulting in lost revenue, customer confidence and bad publicity.

Recommended Actions

Mitigation of this risk would include the following,

- Deploy a standby Checkpoint firewall
- Install a second circuit from a different ISP (due to cost considerations the bandwidth would be downgraded as compared to the primary connection but still sufficient to get GIAC Enterprises operational quickly).
- Configure a secondary DMZ with one web server to run the online Application.
- Modify the DNS record to point to the new website

GIAC Enterprises does have a fully tested Business Continuity Plan and, if deemed appropriate, it can be invoked.

3. Evaluate and Develop Security Policy

The crown jewel of GIAC is the transactional data residing on the database server at the corporate head office. Due to the criticality of this server, the Secure Server Policy (see Appendix B), available from the SANS Security Policy Project, will be evaluated and revised to suit the GIAC Enterprise environment.

Evaluation

Purpose

This section of the sample policy indicates that the intent of the policy is to establish standard server builds which will minimize the risk of unauthorized access to confidential information and technology. It identifies why the policy is necessary and the risk it is addressing.

Scope

The boundaries of the policy are clearly defined as it states the policy applies to servers that are connected to the internal network. It also makes reference to a different policy for DMZ server configuration which helps to further define the boundary.

Policy Statement

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

The policy section overall does a good job of providing guidance as to what has to be done in support of the policy. Some of the statements in the General Configuration Guidelines need to be stronger. The points where 'Operating System configuration *should* be in accordance …' and 'Access to services *should* be logged' need to be modified to provide less ambiguity.

Responsibility

The policy does outline responsibilities for the configuration guides and ensuring compliance however there is no mention in the policy as to who is responsible for modification, review, approval and implementation of the policy itself.

Action

The items mentioned under the Monitoring section detail the length of time security related events are to be saved. There needs to be a time frame put on the reporting of security related events to InfoSec. As it stands in the sample policy there does not appear to be the necessary urgency considering the criticality of the system.

The compliance section indicates that audits are to be performed regularly which is somewhat subjective. This should be modified to specify a specific frequency.

Overall the sample policy can be used for GIAC with the appropriate modifications. As the IT team at GIAC is small, there is not an InfoSec department. The Systems Infrastructure Manager is responsible for IT security. GIAC does not have individual operational groups, and since all servers are centrally located, the Network Operations team is responsible for the configuration, administration and maintenance of all servers. With respect to enforcement, any server found to be non compliant will be removed from the network immediately. It is important to GIAC to have the ability to recover servers in a short period of time therefore a statement will be added regarding a contingency / recovery plan. Finally, as GIAC uses the MBSA utility from Microsoft, a scan is run on the server before deployment and on a quarterly basis thereafter.

Revision

Server Security Policy

1.0 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by GIAC Enterprises. Effective implementation of this policy will minimize unauthorized access to GIAC Enterprises proprietary information and technology.

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

2.0 Scope

This policy applies to server equipment owned and/or operated by GIAC Enterprises, and to servers registered under any GIAC Enterprises-owned internal network domain.

This policy is specifically for equipment on the internal GIAC Enterprises network. For secure configuration of equipment external to GIAC Enterprises on the DMZ, refer to the *Internet DMZ Equipment Policy*.

3.0 Policy

3.1 Ownership and Responsibilities

All internal servers deployed at GIAC Enterprises are owned by the Network Operations group who are responsible for system administration. Approved server configuration guides must be established and maintained by the Network Operations group, based on business needs and approved by the Systems Infrastructure Manager. The Network Operations group should monitor configuration compliance and implement an exception policy tailored to the environment. The Network Operations group must establish a process for changing the configuration guides, which includes review and approval by the System Infrastructure Manager

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location, and a backup contact
    - Hardware and Operating System/Version
    - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

3.2 General Configuration Guidelines

- Operating System configuration must be in accordance with approved InfoSec guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services must be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

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

- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers must be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.
- Servers must have in place a recovery or contingency plan.
- Servers must have the MBSA report run and submitted to the Systems Infrastructure Manager before deployment

3.3 Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    - All security related logs will be kept online for a minimum of 1 week.
    - Daily incremental tape backups will be retained for at least 1 month.
    - Weekly full tape backups of logs will be retained for at least 1 month.
    - Monthly full backups will be retained for a minimum of 2 years.
    - MBSA report will be run on all servers on a quarterly basis by the Network Operations team
- Security-related events will be reported to the Systems Infrastructure Manager immediately, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

3.4 Compliance

- Audits will be performed, at minimum, twice annually by authorized organizations within GIAC Enterprises.
- Audits will be managed by the internal audit group, in accordance with the *Audit Policy*. The Systems Infrastructure Manager will present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

4.0 Enforcement

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

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Any server found to be sub-standard may be removed from the network at the discretion of the Systems Infrastructure Manager

5.0 Definitions

Term	Definition
DMZ	De-militariezed Zone. A network segment external to the corporate production network.
Server	For purposes of this policy, a Server is defined as an internal GIAC Enterprises Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

6.0 Revision History

This policy is reviewed and approved on an annual basis by the executive committee at GIAC Enterprises. The Systems Infrastructure Manager is responsible for the drafting and maintenance of this policy.

4. Develop Security Procedures

Server Authorization Procedure

Scope

The purpose of this procedure is to outline the necessary requirements for an individual in the Network Operations group to obtain authorization to connect a server to the network. It serves to prevent unauthorized and unknown servers connecting to the network thus minimizing risk to GIACs business.

Server Authorization

1. Network Operations group gathers the specifications for the server as follows,
    - Business Owner
    - Business Function
    - Services running
    - Hardware specifications
    - Operating System
    - Service Pack
    - Server Name
    - IP Address

© SANS Institute 2003, Author retains full rights.

2. Network Operations group e-mails specifications to Systems Infrastructure Manager

3. Network Operations e-mails MBSA report for this server to the Systems Infrastructure Manager.

4. Network Operations group e-mails the tested and documented backup, restore and recovery procedures for this server.

5. System Infrastructure Manager reviews the request within 5 business days.

6. If the server is in compliance with the Secure Server Policy and Server Recovery Policy the Systems Infrastructure Manager sends an e-mail to the Network Operations group and business owner authorizing deployment.

7. If the server is non-compliant in some facet, it is identified and sent back to the Network Operations group for correction. Network Operations will resubmit the required documentation to the Systems Infrastructure Manager within 5 business days.

8. As stated in the Secure Server Policy, audits will be conducted semi annually in accordance with the Server Audit Policy.

This procedure clearly assigns responsibility to the Network Operations for gathering the specifications, validating the security patch level and ensuring recoverability of a server before it can be deployed in GIACs environment. It supports the Secure Server Policy by requiring submission of the contact details, hardware and software specifications, security (MBSA) report to validate the patch levels, and the recovery procedures. By following this procedure only servers that are identifiable, secured and recoverable would be connected to GIACs network. This eliminates the possibility of having unauthorized and unknown servers on the network thus providing GIAC with a more secure environment. It also will reduce recovery time as documented procedures must be in place before server deployment.

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

Appendices

A. Network Diagram

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

B. Security Policy

Note: This policy was obtained from the SANS Security Policy Project and downloaded from http://www.sans.org/resources/policies/

Server Security Policy

1.0 Purpose
The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by <Company Name>. Effective implementation of this policy will minimize unauthorized access to <Company Name> proprietary information and technology.

2.0 Scope
This policy applies to server equipment owned and/or operated by <Company Name>, and to servers registered under any <Company Name>-owned internal network domain.

This policy is specifically for equipment on the internal <Company Name> network. For secure configuration of equipment external to <Company Name> on the DMZ, refer to the *Internet DMZ Equipment Policy*.

3.0 Policy

3.1 Ownership and Responsibilities
All internal servers deployed at <Company Name> must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by InfoSec. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by InfoSec.

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location, and a backup contact
    - Hardware and Operating System/Version
    - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

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

3.2 General Configuration Guidelines

- Operating System configuration should be in accordance with approved InfoSec guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

3.3 Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    - All security related logs will be kept online for a minimum of 1 week.
    - Daily incremental tape backups will be retained for at least 1 month.
    - Weekly full tape backups of logs will be retained for at least 1 month.
    - Monthly full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

3.4 Compliance

- Audits will be performed on a regular basis by authorized organizations within <Company Name>.
- Audits will be managed by the internal audit group or InfoSec, in accordance with the *Audit Policy*. InfoSec will filter findings not related to a

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

specific operational group and then present the findings to the appropriate support staff for remediation or justification.

- Every effort will be made to prevent audits from causing operational failures or disruptions.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	**Definition**
DMZ	De-militariezed Zone. A network segment external to the corporate production network.
Server	For purposes of this policy, a Server is defined as an internal <Company Name> Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

6.0 Revision History

© SANS Institute 2003, Author retains full rights.

References

1. "Mission", Office of Foreign Asset Control
http://www.ustreas.gov/offices/enforcement/ofac

2. Doyle, Charles. "The USA Patriot Act – A Sketch." CRS Report for Congress. 18 April 2002
http://www.fas.org/irp/crs/RS21203.pdf

3. The Center for Internet Security
http://www.cisecurity.com

4. Zimmermann, Philip R. FileCrypt
http://www.veridis.com/openpgp/en/index.asp

5. "Root of massive credit card threat found"
http://www.cnn.com/2003/TECH/internet/02/20/credit.hack.ap/

6. Marlin, Steven. "Busted ID Theft Ring Part of a Growing Epidemic". 7 January 2003.
http://www.banktech.com/story/BNK20030107S0001

7. "Identity Theft Survival Guide",
http://money.cnn.com/2002/11/26/pf/saving/q_identity/index.htm

© SANS Institute 2003, 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
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Toronto SEC301	Toronto, ON	Jul 10, 2017 - Jul 14, 2017	Community SANS
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