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

Guidelines for Security at the Application Service Provider and Hosting Service Organization

Introduction

Over the last few years, with the economic boom and post Year 2000 effects, we have experienced an unprecedented requirement for enterprise software products as well as supporting Information Technology(IT) skilled talents. Due to the soaring costs for IT, companies have found that it is more cost beneficial to outsource some of their IT functions. This has led to the upraise of the Application Service Providers(ASP) and Hosting Service Organization(HSO). (We will refer them as 3rd Party IT Service Organization in this paper.)

By engaging a 3rd Party IT Service Organization, the User company can transfer the system management to the 3rd party IT Service Organization. The User company can rely on the 3rd Party IT Service Organization to manage the system availability, performance and scalability. For all the benefits, there are however, operational risks involved when the system is out of the controls of the User company. Issues such as security and privacy need to be considered when a 3rd Party IT Service Organization vendor is selected.

Purpose

Given the increased computer related crimes, any User company considering a 3rd Party IT Service Organization should review their security related requirements with the 3rd Party IT Service Organization vendors. The purpose of this paper is to provide minimum-security baseline and standards to govern any application development outsourcing and hosting functions. By following these standards, the controls can be validated and a process instituted to monitor for continued compliance.

General Requirements

The Security Officer from the User company should be designated as the final security authority of all information services hosted at the 3rd Party IT Service Organization. This will eliminate any potential conflict as well as keeping the User company abreast of any pertinent security related changes.

Depending on the User company requirements and policies, there may be times that third party audits(CICA Section 5900, AICPA SAS 70, AICPA and CICA Systrust) are needed in order to ascertain security controls are in place and verifiable. Inclusion of such a clause in the agreement would be prudent.

Many companies do not have formalized hiring policies. As a result, personnel security procedures are often not in place. The importance of formalized hiring policies and procedures should not be overlooked as statistics often suggested that most security

© SANS Institute 2000 - 2005 Author retains full rights.

related violations occur internally. Hiring standards, performance management and termination practices should be consistent with the 3rd Party IT Service Organization's security needs.

Security Policies And Procedures

The purpose of the Service Level Agreement (SLA) is to contractually oblige the 3rd Party IT Service Organization to uphold certain requirements. It is, therefore, imperative for the User company to carefully review the SLA when choosing a 3rd Party IT Service Organization vendor. Specifically, the SLA should provide details on the 3rd Party IT Service Organization security policies and procedures. Any pertinent security policies and procedures should be reviewed and approved by the User company's Security Management and Operations prior to the signing of the agreement. Security policies and procedures typically include the following:

- Identification of all individuals responsible for implementing the security policies and procedures and what their roles and duties are.
- Identification of critical information to protect.
- Identification of enforcement procedures.
- Identification of steps to be taken if there is a security breach.

Security Architectural Requirements

Since the 3rd Party IT Service Organization manages the network infrastructure, they should be held responsible for the maintenance of current diagram of all servers, network maps, and protocols used for all services hosted. In addition, interdependencies and trust relationships required between servers comprising the application should be documented. The User company should require the 3rd Party IT Service Organization to perform such validation on a monthly basis.

In the event that systems hosted or application developed by the 3rd Party IT Service Organization are compromised from the Internet, depending on the SLA, the 3rd Party IT Service Organization may be held accountable. To minimize this exposure, the 3rd Party IT Service Organization should incorporate a layered approach to security, eliminating single points of failure that can allow unauthorized access to its network. This is good security practice that protects both the User company and 3rd Party IT Service Organization.

Additionally, in order to protect the network, administrative and privileged access should be sourced from a non-public network and any traffic traverse over the Internet should be encrypted using well known encryption standards. As well, all remote administrative and privileged access to the servers hosted by the 3rd Party IT Service Organization should be accompanied by two factor authentication techniques. Not having this policy will subject the network to potential violations.

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

Application and Code Review

Nowadays, web-based applications are often developed in a fast-paced environment where high-quality software development methods and configuration management practices are often ignored. For those web-based applications that are developed by the 3rd Party IT Service Organization, the User company should reserve the right to mandate an independent review of all code to ensure good coding standards are followed and that security weaknesses are identified and addressed.

Some of the components of an application and code review include:

- Evaluation of compliance with the User company security policies and guidelines
- Assessment of technical controls for authentication, authorization, administration, and user access to data
- Attempt of buffer overflow via login process or data submission
- Attempt of denial of service attack via process or data submission
- Attempt of administrative or Operating System functions via user input field
- Attempt to execute prohibited transactions
- Breaking of the user "shell" to achieve access of administrator or another user
- Verification of data storage and transmission encryption and key management
- Attempt of malicious code exploits via well known hacker information sites (i.e. www.securityfocus.com and www.securityportal.com)

In those cases where source code is not available or strictly proprietary, alternative approaches such as application focused penetration testing should be considered so that an acceptable level of assurance is achieved.

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

Change Management

In any IT environment, a documented and properly followed change management process is a necessity. In the case of 3rd Party IT Service Organization, change management process should be consistently applied to the web content, software, hardware components comprising the web site or application being hosted. Before any changes are implemented, a formal mechanism for identifying the security impact of changes should be established and evaluated by a qualified security professional.

For those approved changes, the 3rd Party IT Service Organization should ensure that changes applied to production services are made in accordance to a defined and documented change management process approved by the User company.

Authentication and Access Control

The 3rd Party IT Service Organization should have a standardized authentication and access control process. Any server hosted at the 3rd Party IT Service Organization should adopt a "Role-Based Access Control Methodology" separating system administrator, application administrator and anonymous/guest roles.

It is good security practice for authentication of all administrative and privileged access to those servers hosted at the 3rd Party IT Service Organization be used either the:

- two-factor authentication
- one-time passwords

  Or

- reusable password that is changed every 30 days and not repeated during the life of the server

Where remote traffic originating on the Internet accessing systems or networks within the 3rd Party IT Service Organization is necessary, an acceptable Virtual Private Network (VPN) solution requiring two-factor authentication should be used to provide maximum security.

Threat and Vulnerability Assessment

The 3rd Party IT Service Organization should conduct network and host vulnerability scans periodically. The frequency of these scans should be discussed and agreed upon by both the 3rd Party IT Service Organization and the User company. The purpose of vulnerability assessment is to test security modules and assess system attributes that allow threats to succeed such as poor password management, unconfigured firewalls or hub ports exposed to unauthorized users. Where in-house expertise is lacked, the 3rd Party IT Service Organization should engage third party security professionals to conduct such tests.

© SANS Institute 2000 - 2005 Author retains full rights.

Technical Security Controls

Server Security

Default configuration creates tremendous security risks. Any server hosted at the 3rd Party IT Service Organization should either be configured based on industry best practice(i.e. SANS Institute at www.sans.org, National Security Agency at www.nsa.gov etc.)approved by the User company or the User company's own specifications. Some of the best practices include:

- All user accounts except for the server account(s) and authorized administrator account should be removed
- Different root directories for the server and server document should be used
- Interpreters, shells, and configuration files should be located outside the server directory
- A dedicated host for the server should be used and all other unnecessary services, including Simple Mail Transfer Protocol (SMTP) and File Transfer Protocol (FTP) should be disabled
- Only a minimum set of client applications should be installed. If a browser must be installed, then downloading of active content (for example, Active X and Java) should be disabled
- Where appropriate, multiple server instances under different IDs should be run in order to provide different types of access to different users
- Packet filters, such as TCP wrappers, should be used to restrict connections from known hosts or services and to log incoming service requests

Vulnerabilities get discovered almost on a daily basis. The 3rd Party IT Service Organization should establish a process to receive notification of any newly detected security vulnerability. It is the responsibility of the 3rd Party IT Service Organization to ensure the server software in use incorporates vendor issued updates and patches to remove known security vulnerabilities.

Network Security

Network traffic should be actively monitored by the 3rd Party IT Service Organization. In addition, the 3rd Party IT Service Organization should ensure that all connectivity initiated from hosting server into the User company application server is restricted to either SQL access to database or other defined TCP-based access. To further protect the network, the 3rd Party IT Service Organization should also adapt a "default deny and implicit drop stance" that forces systems to fail closed and dropping all traffic not expressly permitted.

© SANS Institute 2000 - 2005 Author retains full rights.

Other good network security practices include:

- Run only services and protocols necessary. Where insecure protocols are used, i.e. FTP, Telnet etc. all sessions must be encrypted through a service such as "Secure Shell"
- Limit network access to the web-hosting systems by IP-address and meet service levels required for application performance
- Block any unauthorized usage of security discovery tools and protocols i.e. Port Scanners, Trace-route etc

Dedicated Firewall

The User company should ensure a process is in place to provide configuration, monitoring, auditing and active management of the firewall at the 3rd Party IT Service Organization. As in any other security platforms, maintaining the currency of the vendor issued updates and patches is critical. Should the firewall be compromised, an alert should be sent to the User company for immediate remedial actions.

Intrusion Detection Systems

Intrusion Detection Systems(IDS) is one of the critical security architecture components. It is the 3rd Party IT Service Organization responsibility to configure and manage the IDS as well as maintaining the currency of the patches and attack signatures. The User company should ensure that the applicable event logs for potential malicious attacks and probes are reviewed and analysed by the 3rd Party IT Service Organization on a daily basis. In the event of a successful intrusion, there should be a process in place so that the User company is alerted immediately.

Security Monitoring

Since the website and applications are hosted at the 3rd Party IT Service Organization, regular and frequent reviews must be conducted to ensure all components continue to adhere to the agreed configuration standards required for security. Some of the required security monitoring components include:

- Audit logs on all web-hosting systems and applications that have the capability
- Logs and events of web-hosting systems on a daily basis with ability to trace a user's actions for incident response purposes
- Process to obtain all new security alerts for operating systems, commercial applications and technologies that are in use by the User company
- Risk assessment and implementation plan for all applicable vulnerabilities from the appropriate security and virus alert sources i.e. Microsoft

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

Technet, Computer Emergency Response Team (CERT) at www.cert.org, etc. within 24 hours

Incident Response Handling

The 3rd Party IT Service Organization should have a formal incident response and handling plan to provide guidance to users in the event that a security incident occurs in the system hosted. The incident response and handling plan typically contain the following processes:

- Identification of incident and assignment of responsibilities
- Containment of incident
- Eradication of the cause and symptoms of the incident
- Recovery of system

Data Backup and Disaster Recovery Planning

The User company should ensure that a backup and disaster recovery plan(DRP) be developed and implemented at the 3rd Party IT Service Organization in order to safeguard its web-hosting systems or data hosted from disruption and suspension.

The DRP should contain the following phases:

- Awareness and discovery of possible and plausible threats
- Assessment of risks in relation to perceived threats
- Mitigation of risk exposures and possible losses
- Preparation of specific actions that must be taken should a disaster occur
- Annual validity testing of the current DRP
- Preparation of response and recovery

Backup should occur daily for servers and weekly for key files. Backup tapes should be stored off-site. Where the security of the User company information or data is of vital concern, a secure media vault at a storage facility maintained by an offsite media storage company should be engaged.

Physical Security and Environmental Controls

Physical security of the server is also of paramount importance. The User company should ensure that any server hosted at the 3rd Party IT Service Organization is located in a managed and secure physical environment in order to protect it from threats such as fire, accidental damage and vandalism.

The 3rd Party IT Service Organization should restrict physical access to the data centre in

© SANS Institute 2000 - 2005 Author retains full rights.

order to protect the User company hosted systems and other related supporting infrastructures against threats. Physical access to the server should be secured by a secure case. Identification badge, Card-key access, cameras and guards should be deployed at key entry points at the data centre.

Environmental controls are also critical and at a minimum should include the following:

- Installation and regular testing of fire suppression and preventive devices to protect the data centre from fire
- Implementation and maintenance of uninterruptible power supply (UPS) or backup generator to protect sudden loss of electric power. Should a critical business application be hosted at a 3rd Party IT Service Organization, it is desirable to have a redundant UPS system
- Regular maintenance of heating and air-conditioning systems
- Periodic review of the electric power distribution, heating plants, water, sewage, and other utilities for risk of failure
- Full time 3rd party security monitoring and CCTV
- Implementation of moisture and humidity detectors above and below raised floor environment.

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

References:

a) Zdnet India, "How to choose a Data Centre"
http://www.zdnetindia.com/biztech/specials/datacentre/stories/17769.html

b) JP Vellotti, "ASP Security Primer"
http://www.zdnet.com/pcmag/stories/reviews/0,6755,2692080,00.html

c) Ariel Kelman, "ASP Planning: A checklist for Security"
http://www.advisor.com/Articles.nsf/aid/KELMA02

d) Sue Hildreth, "ASP Security: Why Firewalls are not enough"
http://b2b.ebizq.net/asp/hildreth_2.html

e) Dr. Bruce V. Hartley, "ASP Security"
http://www.internetindustry.com/Interviews/aspsec.shtml

f) Tipton & Krause, "Handbook of Information Security Management"
http://secinf.net/info/misc/handbook/ewtoc.html

g) Information Security Forum, "Web Site Security: Workshop Report and Basic Checklists"

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

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

© SANS Institute 2000 - 2005 Author retains full rights.