ASP Security Standards

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Overview

This document defines the minimum security criteria that an Application Service Provider (ASP) must meet in order to be considered for use by <Company Name>. As part of the ASP selection process, the ASP Vendor must demonstrate compliance with the Standards listed below by responding in writing to EVERY statement and question in the six categories. InfoSec will closely review the vendor responses, and will suggest remediation measures in any areas that fall short of the minimum security criteria. Corporate Information Security (InfoSec) approval of any given ASP resides largely on the vendor's response to this document.

These Standards are subject to additions and changes without warning by InfoSec.

2.0 Scope

This document can be provided to ASPs that are either being considered for use by <Company Name>, or have already been selected for use.

3.0 Responding to These Standards

InfoSec is looking for explicitly detailed, technical responses to the following statements and questions. ASPs should format their responses directly beneath the Standards (both questions and requirements) listed below. In addition, please include any security whitepapers, technical documents, or policies that you may have.

Answers to each Guideline should be specific and avoid generalities, e.g.:

Examples:

Bad: "We have hardened our hosts against attack."
Good: "We have applied all security patches for Windows 2000 as of 8/31/2000 to our servers. Our Administrator is tasked with keeping up-to-date on current vulnerabilities that may affect our environment, and our policy is to apply new patches during our maintenance period (2300hrs, Saturday) every week. Critical updates are implemented within 24 hours. A complete list of applied patches is available to <Company Name>."

Bad: "We use encryption."
Good: "All communications between our site and <Company Name> will be protected by IPSec ESP Tunnel mode using 168-bit TripleDES encryption, SHA-1 authentication. We exchange authentication material via either out-of-band shared secret, or PKI certificates."

4.0 Standards

4.1 General Security

1. <Company Name> reserves the right to periodically audit the <Company Name> application infrastructure to ensure compliance with the ASP Policy and these Standards. Non-intrusive network audits (basic

portscans, etc.) may be done randomly, without prior notice. More intrusive network and physical audits may be conducted on site with 24 hours notice.

2. The ASP must provide a proposed architecture document that includes a full network diagram of the <Company Name> Application Environment, illustrating the relationship between the Environment and any other relevant networks, with a full data flowchart that details where <Company Name> data resides, the applications that manipulate it, and the security thereof.

3. The ASP must be able to immediately disable all or part of the functionality of the application should a security issue be identified.

4.2 Physical Security

1. The equipment hosting the application for <Company Name> must be located in a physically secure facility, which requires badge access at a minimum.

2. The infrastructure (hosts, network equipment, etc.) hosting the <Company Name> application must be located in a locked cage-type environment.

3. <Company Name> shall have final say on who is authorized to enter any locked physical environment, as well as access the <Company Name> Application Infrastructure.

4. The ASP must disclose who amongst their personnel will have access to the environment hosting the application for <Company Name>.

5. <Company Name>'s Corporate Asset Protection team requires that the ASP disclose their ASP background check procedures and results prior to InfoSec granting approval for use of an ASP.

4.3 Network Security

1. The network hosting the application must be air-gapped from any other network or customer that the ASP may have. This means the <Company Name> application environment must use separate hosts, and separate infrastructure.

2. How will data go between <Company Name> and the ASP? Keep in mind the following two things:

    a. If <Company Name> will be connecting to the ASP via a private circuit (such as frame relay, etc.), then that circuit must terminate on the <Company Name> extranet, and the operation of that circuit will come under the procedures and policies that govern the <Company Name> Partner Network Management Group.

    b. If, on the other hand, the data between <Company Name> and the ASP will go over a public network such as the Internet, appropriate firewalling technology must be deployed by the ASP, and the traffic between <Company Name> and the ASP must be protected and authenticated by cryptographic technology (See Cryptography below).

4.4 Host Security

1. The ASP must disclose how and to what extent the hosts (Unix, NT, etc.) comprising the <Company Name> application infrastructure have been hardened against attack. If the ASP has hardening documentation for the CAI, provide that as well.

2. The ASP must provide a listing of current patches on hosts, including host OS patches, web servers, databases, and any other material application.

3. Information on how and when security patches will be applied must be provided. How does the ASP keep up on security vulnerabilities, and what is the policy for applying security patches?

4. The ASP must disclose their processes for monitoring the integrity and availability of those hosts.

5. The ASP must provide information on their password policy for the <Company Name> application infrastructure, including minimum password length, password generation guidelines, and how often passwords are changed.

6. <Company Name> cannot provide internal usernames/passwords for account generation, as the company is not comfortable with internal passwords being in the hands of third parties. With that restriction, how will the ASP authenticate users? (e.g., LDAP, Netegrity, Client certificates.)

7. The ASP must provide information on the account generation, maintenance and termination process, for both maintenance as well as user accounts. Include information as to how an account is created, how account information is transmitted back to the user, and how accounts are terminated when no longer needed.

4.5 Web Security

1. At <Company Name>'s discretion, the ASP may be required to disclose the specific configuration files for any web servers and associated support functions (such as search engines or databases).

2. Please disclose whether, and where, the application uses Java, Javascript, ActiveX, PHP or ASP (active server page) technology.

3. What language is the application back-end written in? (C, Perl, Python, VBScript, etc.)

4. Please describe the ASP process for doing security Quality Assurance testing for the application. For example, testing of authentication, authorization, and accounting functions, as well as any other activity designed to validate the security architecture.

5. Has the ASP done web code review, including CGI, Java, etc, for the explicit purposes of finding and remediating security vulnerabilities? If so, who did the review, what were the results, and what remediation activity has taken place? If not, when is such an activity planned?

4.6 Cryptography

1. The <Company Name> application infrastructure cannot utilize any "homegrown" cryptography – any symmetric, asymmetric or hashing algorithm utilized by the <Company Name> application infrastructure must utilize algorithms that have been published and evaluated by the general cryptographic community.

2. Encryption algorithms must be of sufficient strength to equate to 168-bit TripleDES.

3. Preferred hashing functions are SHA-1 and MD-5.

4. Connections to the ASP utilizing the Internet must be protected using any of the following cryptographic technologies: IPSec, SSL, SSH/SCP, PGP.

5. If the <Company Name> application infrastructure requires PKI, please contact <Company Name> Information Security Group for additional guidance.