Global Information Assurance Certification Paper

Security Issues for Application Service Providers

Achim von Neefe
November 2000

Security – A business issue for Application Service Providers

Working with an ASP stretches the client's security boundaries, increases inherent risk and might create legal issues.
Prudent clients will seek positive assurance to all security related questions. According to a Zona Research report, 96% of current or likely ASP customers "rated security as either 'extremely important' or 'very important' when considering a service provider". [1]
For ASPs these fears about security are one of the biggest barriers to their growth. "Demonstrating that they are addressing all of the security issues, both technical and policy-oriented, in an open manner is a needed catalyst to their market acceptance." [2]

Overview

The following text tries to touch all the relevant security related issues that an ASP faces and has to be prepared to answer. The areas covered in this paper are:

- Connectivity – SSL, Firewalls, VPN
- Applications and Infrastructure Software – web server, database, OS and applications
- Authentication and Authorization – certificates, passwords, role based access and data separation
- Auditing and Logging – what events are getting logged
- Administration – security policy, staff, physical access
- Miscellaneous – legal issues, disaster recovery

Connectivity

SSL
The Secure Sockets Layer is used to secure a communication channel. While application independent, it is optimized for HTTP and usually used for secure communication with a web server. A short introduction to SSL is available at http://www.rsasecurity.com/rsalabs/faq/5-1-2.html. [3]
An ASP should enable SSL for all HTTP based communication.

Virtual Private Networks
A VPN securely transports IP packets across the Internet backbone by establishing tunnel endpoints that negotiate a common encryption and authentication scheme prior to transport. It is used as an additional secure communication link between ASP hosting

facilities and customers' locations.

Firewalls
They are a standard for every ASP. A usual setup is having an outer firewall, a DMZ with web servers and an inner firewall (maybe from a different vendor) that protects the applications, databases etc. Of course an ASP could have a much more complicated firewall setup, for example compartmentalize applications or customers.
If each customer has a different port assigned the firewall can be configured to only allow connections from specific IP addresses to go through the firewall.
The correct setup is very important and has to be done by trained personnel. Maintenance is important: it shouldn't happen that each firewall administrator creates her/his own set of rules on top of the old ones.
A firewall can never be the only defense against outside intruders.

Routers
Because of the important role that a border router plays on the connectivity of the whole network it must be carefully configured and secured. Some of the standard configuration settings for a Cisco router should be changed to improve security and prevent unauthorized access.

Applications and Infrastructure Software

Hardened OS
All Operating Systems used by the ASP have to be hardened. Hardening simply means to remove all unnecessary services like FTP, telnet, finger etc. from the machine.

Secure OS
A secure or trusted OS is a special version of off-the-shelf operating systems that are enhanced to be more secure. An example is PitBull from Argus Systems. It can seal applications into unbreakable compartments without an all powerful superuser for the whole machine. Trusted operating systems are usually harder to learn and administer than standard versions. They are used for servers that conduct financial transactions over the Web or perform other highly critical functions. [4]

Database issues
Usually all the important data reside in a database. It should never be exposed to the Internet. All default accounts have to be deleted if possible and all passwords have to be changed according to the security policy. Sensitive information in the database should be encrypted. An access control mechanism has to be in place.

Securing the Web server
Securing a web server consists mostly of configuration issues like removing all unused CGI scripts, restrictive file access permissions, turning off automatic directory listing, no use of Server Side Includes, configuring client hostname and IP address restrictions etc.

Consider starting the web server on a non-privileged port so the server doesn't have to be started as root. If the web server is started from a superuser account, switch the ownership of all subsequently created server processes to a different account.

Designing more secure software
If an ASP develop its own software for a hosted service it should consider the security implications of the programs. Examples are the careful handling of input data and program execution with a minimum of privileges. [5]

Virus protection
Viruses have to be controlled at the file server, the gateway, and on e-mail servers. Server anti-virus applications allow for a virus scan and detection on an on-going and periodic basis, as well as each time a file is downloaded or a computer is booted. To protect networks, monitoring attachments at the e-mail gateway is just as important.

Intrusion detection
Just like virus protection intrusion detection software is a must for an ASP. The software has to be closely monitored and regularly updated.

Authentication and Authorization

Authentication can happen through a lot of different means. Certificates are considered one of the more secure forms of authentication. Others are fixed and dynamic passwords. Once authenticated authorization provides role based access.

Certificates
One of the more difficult questions when dealing with certificates is how to deal with CRLs (Certificate Revocation Lists). Another question is who to accept as the issuer or whether to accept self signed certificates. For an excellent general introduction to certificates and public keys see http://www.rsasecurity.com/rsalabs/faq/4-1-3.html. [6]

Passwords
If the ASP relays on fixed passwords as the only way to authenticate users a strict password policy is absolutely necessary.
Dynamic passwords are much more secure and usually use a hardware or software token. An example is RSA's SecureID. If an ASP decides to use dynamic passwords it has to distribute the token to the customer.
The combination of certificates and fixed passwords for authentication is considered very secure, while allowing for easier implementation than dynamic passwords.

Authorization
Once authenticated the access level of the customer can be determined. This enables the ASP

- to offer some kind of self service for the customer, e.g. a customer can add users, change the password of existing users etc.
- to restrict the access to hosts and files.

Customer data separation
One of the most pressing questions for a lot of ASP customers is how to keep data of customers apart. There could be separate database accounts or even separate database instances. For additional security each customer's sensitive data could be encrypted with a different key (see Protegrity (http://www.protegrity.com) for an approach that uses this principle).
There are also fairly sophisticated 3rd party products like Netscreen-1000 (http://www.netscreen.com) that allow an ASP to configure a security domain per customer.

Auditing and Logging

Auditing and logging are important for finding out about possible security breaches, usage forecasts, billing, finding software bugs etc.
An ASP has to decide what type of events will be monitored, e.g. all unsuccessful login attempts, attempts to exceed authorized limits or actions, help desk calls etc. It also has to make some of these data available to the customer. Other changes, like expanded administrator authorization, also have to be communicated to customers.

Administration

Security policy
One of the most important things an ASP has to have is a Security Policy. All ASP operations are governed by its security policy. It deals with questions like which personnel is authorized to access a customers applications and data and under what conditions, it answers questions about qualified security staff and potential screening procedures.
Other areas covered by the Security Policy are procedures and processes for events like denial of service attacks, unavailability for other reasons, breach of data integrity, incident response strategy etc.
A big ASP customer might want to have a customized Security Policy.

Ongoing assessments
An ASP could use vulnerability scanners on a regular basis to find weaknesses in its network. Another possibility is to hire an outside company for a security assessment.

Physical access control
Most of the time an ASP actually uses a collocation provider like Exodus or AboveNet for

the services it is hosting. These companies have strict access controls to the cage where the ASP's machines reside and only authorized personnel can get there.
If this it not the case the ASP has to have strict physical access controls in place.

Miscellaneous

Legal issues
In case a dispute arises legal issues will be important. Here are just a few issues that might become important:

- How can damage be proved
- Negligence vs. reasonable measures
- Liability issues

Hardware setup
A customer might have certain hardware preferences or might insist on getting a separate subnet.

Outside vs. inside threats
Most threats are coming from insiders, not outside intruders. [7] The ratio is roughly 65 to 35. This underlines the importance of a Security Policy and strict access controls to critical systems and data.

Disaster recovery
An ASP should have a plan for disaster recovery. There could be a secondary site that gets updated and can take over in case of a failure of the primary site.

References

[1] Grzanka, Len. "ASPs Need Bite." Interactive Week. October 21 2000.
URL: http://www.zdnet.com/intweek/stories/news/0,4164,2647788,00.html (November 18 2000).

[2] "ASP – Application Service Provider, or A Security Problem." November 2 2000.
URL:http://www.securityportal.com/cover/coverstory20000327.html (November 18 2000).

[3] "What is SSL?" RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1. May 2000.
URL: http://www.rsasecurity.com/rsalabs/faq/5-1-2.html (November 18 2000).

[4] Scheier, Robert L. "Trusted Operating Systems: The Ultimate Defense." Computerworld. November 6 2000.
URL: http://computerworld.com/cwi/story/0%2C1199%2CNAV65-663_STO53293_NLTs%2C00.html (November 9 2000).

[5] Ghosh, Anup K. "E-commerce security: weak links, best defenses." Wiley & Sons, New

York 1998.

[6] “Public Key Issues.” RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1. May 2000.
URL: http://www.rsasecurity.com/rsalabs/faq/4-1-3.html (November 19 2000).

[7] Clyde, Robert A. “Enterprise Security: Built on Sound Policies.”
URL: http://axent.se-com.com/ (November 21 2000).