Global Information Assurance Certification Paper

Security Issues Your Company Faces When Storing Data at an ASP

By Kim Hughes

Today there is a growing desire from businesses of all sizes to house intranets, websites and data at Application Service Providers, ASP. "ASPs are service firms that provide a contractual service offering to deploy, host, manage, and lease what is typically packaged application software from a centrally managed facility. Customers gain access to the applications through the Internet or dedicated leased lines". (" High-End Application Service Provider Market Will Reach $2 Billion by 2003") Regardless if ASPs popularity continues to grows or fails tomorrow, companies need to assume that their data living on their ASP is not secure.

Let us assume that the ASP's perimeter security is top notch and all the proper defense in depth measure have been practiced such as firewalls, intrusion detection, policies and procedures, and limited access to locked server rooms. The focus of this paper will be on the security of data in transit, data in waiting and the confidentiality of data from employees at the ASP. We will also be discussing paths to resolution that your company may wan to explore in order to secure you data and protect your company when choosing an ASP.

Industry

The barriers into the entry of the ASP market are very low. "Gartner Group, at Stamford, Conn., industry research firm, said of the 480 retail ASPs operating today in the $3.6 billion industry, only 20 would survive as enterprise-class, full-service retail ASPs by 2004". (Gonsalves) The impact of an ASP failing and shutting down could be detrimental to a company. As the trends in the ASP community rise and fall, today's market is interested in the solutions ASPs have to offer. ASPs are appealing to large and small companies who are interested in low maintenance of servers, low cost of hardware and software, yet are ASPs secure? Protecting your company's data should be your number one concern when choosing to go with an ASP.

Risks

If your company chooses to go with an ASP, you should outline all the potential security hazards. When sending sensitive data across an open network such as the Internet, there is a very high risk of a hacker snooping the HTTP connection. There is risk of a hacker capturing your data in transit to the ASP. If the connection is not encrypted between the client and the ASP, data is susceptible to being captured by a third party.

Valuable data such as proposals, trade secrets, competitors information, financial information, sales information and customer data are all only a click away from prying eyes at your ASP. There is the potential risk of a corrupt ASP employee selling your companies data to competitors, modifying your data, deleting your data, or viewing valuable information such as root passwords and IP addresses to customer's networks. On intranets, housed by the ASP, you may have calendars that show in detail where your employees are and what their tasks are or customer's sites they may be working at. You may have a company phone list housed on the ASP, which could be a click away from an ASP employee handing it off to a recruiter. You may have client lists or partner lists with contact names and numbers that would make things all to easy for the wrong hands to call

upon your customers and partners and take away your business or violate a privacy agreement between you and your client. Taking proper security measures to protect your company's data can keep your company thriving and separate you from naive ASP customers. It is reassuring to your clients to let them know that even though you are storing their sensitive data at an ASP you are taking proper precautions to help reduce their data from being public knowledge.

Evaluate the Situation

First, check to make sure the session between the client and the ASP is encrypted use a tool to view the packets as they leave your network to the ASP to verify that the session is encrypted and secure. Using a Secure Socket Layer, SSL, connection can resolve the problem of hackers capturing your data in transit. A Virtual Private Network, VPN, between your ASP and the client is necessary to ensure all data traveling is encrypted. When choosing an ASP it is important to check the strength of the ASP's secure connection. What level of encryption are they using? What level of encryption is your personal web browser using? Have you upgraded your web browsers to allow higher negotiation of encryption between your client and the ASP?

Solving the problem of confidentiality between the ASP and your data in waiting is more complex and requires polices and procedures. Key things to look for while shopping for an ASP are to, "Examine a privacy policy's wording to understand what constitutes a sale or transfer of data. Keep the "what-ifs" in mind: what happens to the data if providers go bust or are acquired. Do a background check on the provider and check references. Look for seals of approval. Prevent your data from being sold up front by making them sign a contract that says they can't sell it". (Torode) Just because the idea of selling data is unethical does not mean that it won't happened to your company, it does happen

Pradeep Singh, a principal at Management Information & Technology Consultants, New York reported an astonishing 30 percent of 30 ASPs were mining customer data. "Singh, uncovered data pilfering while conducting background checks on hosting providers on behalf of his clients. He used a method called "seeding," in which he fed the hosting companies false information. If he started receiving mail under those false names, he knew they were selling their customers' data". (Torode) Even more shocking most of these companies have policies and procedures in place. More than likely most ASP employees that will be handling your data are not highly certified security professionals and the numbers prove that more than few can be swayed to act unprofessionally and sell data.

Collaboration also needs to be taken into consideration. A hostile former employee with the key to your encrypted files could team up with an employee of the ASP and successfully mine data from your site. Can this happen? Yes, it can but collaboration reduces risk, convincing a second person to buy into the idea of a scheme is more than usually less likely to happen rather than an individual working alone on a scam.

Encrypting all files can prevent your ASP from viewing your data. There are variations of how your company can go about encrypting data with different uses of various keys, which are discussed below. Proper policies and procedures must also be in

place when an employee leaves so the data cannot be compromised, which significantly reduces the confidentiality of your page hosted at an ASP from being violated.

Importance of Policies and Procedures

Proper policies and procedures are important for management to have in place to reduce risk of security related issues and insure secure consistent development of business. In today's corporate America many companies lack a formal well-defined security policy. Information security is a social and technological concern, it is important for upper management to be involved in the policy writing process to insure success.

It is important to have polices and procedures in place when implementing encryption into your company. Having a policy in your company for your employees to follow holds up in a court of law and can be beneficial when dealing with unethical issues. A company should have a complete policy designed for their daily business needs, not only if they are using encryption with an ASP.

Securing Data in Transit

Maintaining a secure connection over the Internet to your ASP is a must. The SSL, Secure Socket Layer Protocol, provides an encrypted connection-oriented communication session between client/server applications with a cipher and short-term session key. The encrypted data is scrambled in a way that it appears to be nonsense to persons viewing the packets. The nonsense text is called ciphered text and the original data is called clear text. There are different intensities of encryption. The strengths depend on the ease of an attacker breaking the key. There are a number of minor flaws in the SSL protocol that make it vulnerable to attacks, but as a whole it provides confidentiality and authenticity over a reliable connection such as TCP.

The SSL Protocol is divided into two layers. Each layer uses services from the layer below and gives functionality to the layers above. Through the record layer a handshake takes place between the client and the server, then initialization and synchronization of an encrypted session taking place at each end point. Next negotiation of a key exchange takes place and sensitive application data can be sent across the record layer.

Your HTTP session should be encrypted with SSL. This reduces the risk of hackers sniffing the line and capturing your data in transit. Currently this is the only way to secure data in transit. This function is set up through the web server at the ASP as a service.

Securing Data in Waiting

Option 1

This solution involves each employee be assigned an individual key. Each member of a group working on a project signs the document with each member of the team's public key and sends the document up to the ASP for storage. This works very well if you can remember who all was on what project for your entire company's existence. What happens if an employee out side the team needs to view the document? One of the existing members of the team has to download the file and add the new

employee's key to the signature and he/she can now view the document. This may be painful and time consuming, but it is all in the name of Security.

Policies and procedures need to be in place to make the functionality of this solution work.

1. *Handling of Sensitive Information*: Highly Sensitive documents should not leave the office. If sensitive documents have to leave the office via a public network such as the Internet from the office or from home to a remote site, documents must be encrypted with the company encryption standard. (Encryption solution name, i.e. PGP)
2. *Key Selection*: Users will provide a seed or a key for access to encryption standard. Users must select a strong seed and must not disclose the seed to unauthorized users.
3. *Theft of Equipment*: Users should not store passwords, user-IDs, or remote login information on their systems or home systems in the event of theft. Any password information or remote login information should not be placed in the same case as a portable system. Users should report theft immediately.
4. *Third Party System Access*: Users connecting to a third party system, such as an Application Service Provider, ASP, should use a user name and strong password. The company reserves the right to terminate user access of users upon termination or disrespectful acts to the site on the ASP. All files placed on the ASP and downloaded from the ASP will be encrypted. (See Handling of Sensitive Information section)

There are potential problems and risks involved in situations such as termination of employees, stolen laptops and compromised keys. First, if an employee leaves the company immediately removal of his/her access from the ASP. This is the first step to limiting his/her accessibility to entering the site. Management may store a copy of his/her key for ease of reading documents signed by this employee. As a company, you do run the risk of the employee still having a copy of the key on a disk or on a home computer. Proper removal of his/her access to the ASP reduces the risk of access to new or existing files. Collaboration with an ASP employee is still possibility to gaining access to the page and obtaining information.

If a laptop is stolen, a new password should be issued in case the employee's user name and password is saved in their web browser, to a local file or written down on paper somewhere in the bag. A new key should be generated for that employee and time taken to resign all the documents signed by the old key to ensure the thief couldn't gain access to sensitive company data. Also a new password to the ASP should be generated.

If an employee feels that their key has been compromised via a hack from the Internet, a friend, a foe or lost media, proper steps to remove the old key and produce a new key are necessary. As before, measures will need to be taken to resign all old docs and generate a new key.

Option 2

If you do not want to manage individual keys and worry about who was on what project in order to view documents, another option is to encrypt all documents with one company wide key. Each employee would have the same public and private key to encrypt and decrypt documents. Individuals will import the key into their key manager. The company will still benefit from the same security as the first solution with out the headache of key management.

Policies and procedures need to be in place to make the functionality of this solution work.

1. *Handling of Sensitive Information*: Highly Sensitive documents should not leave the office. If sensitive documents have to leave the office via a public network such as the Internet from the office or from home to a remote site, documents must be encrypted with the company encryption standard. (Encryption solution name, i.e. PGP)
2. *Key Selection*: Users will be given a company wide key to encrypt sensitive documents. Users will not disclose the key to any unauthorized users.
3. *Theft of Equipment*: Users should not store passwords, user-IDs, or remote login information on their systems or home systems in the event of theft of the equipment. Any password information or remote login information should not be placed in the same case as a portable system. Theft should be reported immediately.
4. *Third Party System Access*: Users connecting to a third party system, such as an Application Service Provider, ASP, should use a user name and strong password. The company reserves the right to terminate user access of users upon termination or disrespectful acts to the site on the ASP. All files placed on the ASP and downloaded from the ASP will be encrypted with the company key. (See Handling of Sensitive Information section)

Many of the same problems and concerns are still present with this solution as with the previous option. Termination of an employee, laptop theft, and compromised company keys are still valid concerns. Upon termination of an employee you will still need to revoke their access to the ASP. Access control lists will need to be in place and alerts will need to be activated if a new member tries to apply for an account. Terminated employees may have a copy of an invitation email at their home email account and may try to gain access to the ASP.

A business decision must be made if your company is going to keep the same key or generate a new key and re-encrypt all the data at your site once an employee leaves. The employee may have a back up copy of the key on disk or at a home computer. Your company may decide that removal of access into the ASP is fine and to leave the company key as is.

Upon theft of a laptop immediate action should be taken to re-password the users access to the ASP and evaluate if a new company key should be generated.

Recommendation

If you do decide to go with an ASP, securing data in transit with SSL should be a requirement no matter how you decide to manage the site. As which way you should go with data in waiting depends on your company. My recommendation would be Option 2 from because of ease of key management. There are many products that are available on the market for this, such as PGP. PGP has a user-friendly interface and was fairly simple to use. Distributing and installing the software internally is simple, the install is very straightforward. Then company key can be easily imported into PGP. Most importantly PGP makes encrypting and decrypting documents easy for all users even not technically inclined users. Finally don't forget to put proper policies and procedures in place to enforce use of security standards among employees.

Bibliography

"Desktop Security for Windows 95, Windows 98, Windows NT, Windows 2000 & Windows ME User's Guide". Version 7.0.

"High-End Application Service Provider Market Will Reach $2 Billion by 2003: New IDC Report Defines Emerging ASP Market and Vendors." March 26, 1999. URL:http://www.idc.com/Data/Internet/content/NET032699PR.htm (21 Feb. 2001).

Gonsalves, Antone. "Analyst Predicts Major Shakeout Among ASPs" TechWeb News August 9, 2000. URL: http://www.techweb.com/wire/story/TWB20000809S0023 (24 Feb. 2001).

Krause, Micki and Tipton, Harold F. Handbook of Information Security Management Boca Raton: CRC Press LLC, 1998.

Schneier, Bruce and Wagner, David. "Analysis of the SSL 3.0 protocol"

Torode, Christina. "DATA HANDOFF -- Are ASPs and hosting providers selling customer information? It happens more often than you might think." Issue: 906. August 07, 2000. URL:http://www.techweb.com/se/directlink.cgi?CRN20000807S0013 (21 Feb 2001).

Wood, Charles Cresson. Information Security Policies Made Easy . Sausalito: Baseline Software, Inc., 1999.