

Secure Your Web Sites!

What You Need to Look For in a Provider

Many universities outsource some or all of their alumni relations web sites to application service providers (ASP's). Outsourcing this activity has many potential advantages including:

- Lower cost
- Better functionality
- No need to manage web servers and web applications

These benefits accrue from the fact that the ASP is providing the same service to many customers and therefore can share development and hosting costs among them. Additionally, because the ASP deals with many customers they develop a great deal of domain expertise that allows them to develop best of breed applications.

When evaluating a provider many people tend to look first and foremost at cost and functionality and overlook security. When outsourcing your web, ignore security at your own peril. There are two major security issues that you should concern your self with: defacement of the web site and theft of confidential data.

- Defacement can occur when a hacker breaks into a web site and changes the pages on the site. This has happened to web sites of organizations as influential as the New York Times.
- Theft of confidential data can occur when a hacker breaks into a web site and downloads confidential data stored on the site. For an alumni relations site, data that might be stolen includes the alumni directory database or even worse, credit card information for sites that process online donations.

You should consider three important aspects of online security when choosing your provider: physical security, network security and application security.

Physical Security

Security starts with physical protection of the servers and network hosting the applications. All servers and network equipment should be in a secure facility with access granted only to those who need it. This prevents tampering with equipment or even worse the theft of a server and all the data on it.

Alums Online servers are located at a data center in Chicago that has key card access to the facility, electronic logging of entry and exit, 24/7 security camera surveillance and 24/7 security guards.

Network Security

Network security is important because web servers connected to the Internet are vulnerable to electronic attack from just about anywhere in the world. Hackers and their automated tools may start probing a computer within minutes of it being connected to the Internet.

There are several important features of good network security:

- Firewalls should be placed in front of the servers that allow only required traffic to pass through.
- Servers should have been hardened/locked down using best practices for the operating system and application that are installed on them.

Contents

Physical Security

Network Security

Application Security

Summary

- Servers must be proactively patched with security patches for the operating system and applications when patches are released.
- Servers should be regularly audited using automated scanning tools for patches and other security settings that may have been overlooked.
- Server passwords must be changed on a regular basis, hard to guess, given to only those who need to know them, and changed immediately when an employee who knows them leaves the company.
- Remote server management should be done using encrypted protocols such as SSH, Secure FTP (SFTP), SSL and IPSEC/VPN.

At Alums Online, our servers fulfill each of these standards for network security.

Application Security

Application security is perhaps the most overlooked aspect of online security and is responsible for the majority of web site break-ins. Programmers are frequently not trained in best security practices before developing applications or do not take the extra effort that is required to create secure applications.

The most frequently overlooked application security vulnerability is SQL (pronounced sequel) injection. SQL is the query language that is used to manipulate most databases. SQL injection is accomplished by embedding SQL commands in a form or URL. SQL commands that are "injected" can be used by a hacker to manipulate a database in ways that were not intended by the programmer of the application, such as deleting data, changing data or even uploading/downloading data. Fortunately, SQL injection can quite easily be prevented by type checking of all form fields and URL parameters (making sure that a numeric field really contains numbers) and by inspecting fields for special characters that might cause unexpected results.

Most ASP's provide a web-based administrative application that allows customers to publish and change content. Session hijacking is an application security vulnerability that needs to be carefully considered when building these applications. When a user logs into the administrative application, a session is started that tracks who the user is and what permissions they have. Usually that session is tracked using session keys that are stored in cookies. If these session keys are easy to guess, a hacker can potentially put the keys into their browser's cookies and "hijack" or take over someone else's administrative session. Therefore it is essential that your provider uses hard to guess session keys and understands what is required to make sessions secure against hijacking.

Poor error handling can also lead to security vulnerabilities. A well-programmed application will never reveal highly technical information in an error message because this information may be useful to a hacker planning an attack. Unfortunately, the default behavior of most web servers when an application error is not anticipated by the programmer is to reveal all sorts of technical details. Fortunately most web server programming environments also give the programmer the ability to catch unexpected errors and display a generic error message such as "an application error has occurred." If you are using your provider's application and you see detailed error messages, you should be asking why.

Above all it is important that your application provider have a program in place to train their programmers about security, develop programming standards that enhance security and regularly audit application source code to make sure that standards are being followed.

Summary

Poor security practices by your alumni relations web site provider can compromise the integrity of your web site. If you have not evaluated your current provider's security, you should. If you are evaluating a new provider, security

should be one of the important criteria you use.

For more information about Alums Online security practices or security in general, feel free to contact me at the email address below or visit our web site at <http://www.alumsonline.com/hostingsecurity.html> .

Tom Parker
Founder and COO
Alums Online Inc.
tom@alumsonline.com