Best Practice Checklist Series - Issue 19

Website Security and Oversight

Understanding the basics: A layperson's guide and checklist for overseeing IT.

Best Practice Checklist Series
An exclusive publication of Sandbox Technologies, Inc.

3868 W Carson St, Suite 316
Torrance, CA 90503
Tel. (424) 207-5130
www.sandboxtech.com

SANDBOX TECHNOLOGIES

Small Business Solutions
Enterprise GrowthPath®
EGP Secure®
EGP Cloud™
ConstructIT®

Website Security and Oversight

Website development, maintenance, security, and management are highly specialized professions. Other than the management of our own Web properties, Sandbox Technologies does not engage offer the aforementioned services.

Given their importance, it is recommended that clients engage knowledgeable and well-vetted Web professionals with the highest standards of security and respect for best practices for maintaining their Web properties.

Notwithstanding the foregoing, as IT generalists, it is our goal to help guide and educate our clients in basic protections that may prove beneficial in promoting the stability and security of all technical systems they employ. For this reason, the brief list that follows consists of basic measures we recommend for owners of Web-based properties as applicable.

Should you have additional questions, or desire assistance with the identification of potential third parties to aid in your Web-related efforts, your Sandbox Technologies Engineer, Account Manager, or Consulting CIO will be happy to answer any questions you may have.

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Table of Contents

Website Security and Oversight.....4

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Website Security and Oversight

Security Standards

Does the organization have a formal set of standards governing the secure development, maintenance and updating of its Web properties?

Websites are sometimes overlooked as a critical security vulnerability. Whether an organization's Web presence(s) link to sensitive data like credit cards and personal information, or merely serve as an online brochure, there are a myriad of ways that a breach can cause damage to an organization.

If compromised, even the most basic of websites can be altered in such a manner as to expose visitors to malware, viruses, or other malicious code. As such, it is important to secure websites and other public facing systems aggressively and routinely have code professionally inspected to ensure integrity.

Status ☐ ☐ ☐

NOTES: _____

_____

_____

Employ the use of TLS/SSL Certificates

Do the company's Web properties employ the use of TLS/SSL certificates?

An SSL (Secure Sockets Layer) certificate is a two-part key pair used to encrypt communication, including traffic to and from a publicly accessible website. TLS (Transport Layer Security) is the next generation of SSL and differs from SSL by the protocol used to establish a secure connection.

SSL and TLS utilize the same certificates; however, the protocols are different, and availability is dependent on the environment hosting the Web property. At the time this was written, a minimum of TLS 1.1 should be enabled on Web properties when using secure certificates.

Status ☐ ☐ ☐

NOTES: _____

_____

_____

Web host security

Has the organization's Web host been thoroughly vetted to verify its commitment to security best practices that extend beyond the website individually and to the practices of the host itself?

Web host security is a key consideration. While organizations engaged in e-commerce or other revenue generating activity generally attend to this requirement, those with only basic publicity sites often overlook its importance.

Status ☐ ☐ ☐

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Code Integrity

Is Web code inspected periodically by a knowledgeable professional, and are Web platforms routinely updated in keeping with best practices?

Older Web technologies and sites that have not been kept current can often be exploited with relative ease. When a website is compromised, hackers can potentially insert malicious code, copy the site, and post dummy sites, collect user data, infect users with viruses, replace text or photos with malicious images, etc.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SPF and DKIM implementation

For applicable websites leveraging communication functionality, have SPF and DKIM been implemented when appropriate?

SPF (Sender Policy Framework) is a public list maintained as a DNS entry that lists servers authenticated as senders for a particular domain. SPF mitigates the ability of spammers to "spoof" legitimate email addresses or domains.

DKIM (Domain Key Identified Mail) is a technology used to authenticate particular emails with a public/private key pair. This, in essence, certifies that an email originated from an authorized server.

(DMARC (Domain-based Message Authentication, Reporting and Conformance) provides a mechanism for how email from another domain that fails SPF or DKIM mechanisms is to be handled. DMARC can be configured to reject or quarantine messages that fail SPF or DKIM checks, and then it can be configured to deliver reports of messages that have failed the above authentication checks.)

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

This document is protected by US and International copyright laws. Reproduction or distribution of this document for commercial advantage and without written permission from Sandbox Technologies, Inc. is strictly prohibited. Any distribution must retain attributions and this notice.

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.