Best Practice Checklist Series - Issue 8

Auditing & Verification

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®

Auditing and Verification

It is a common misconception that simply maintaining a network, applying security patches, and updating software and systems represents an adequate degree of effort to keep an environment secure.

While the foregoing measures are without a doubt essential, today's threat landscape requires a greater degree of attention and effort than ever before. In this issue of the Best Practice Checklist Series, we'll list a number of checks that should be performed periodically, along with various solutions that can be implemented to augment security.

Although no company should ever make the mistake of believing their network environment is 100% secure, by no means does that relieve them of the responsibility to aggressively safeguard the security of their data using every reasonable means available. And while some of the measures that follow may not be appropriate for your organization, they are all measures that merit attention and consideration.

Compiling the recommendations for this issue while keeping things brief was challenging given the complexity and associated questions that some of the implementations will evoke. Nonetheless, in keeping with our format, we have endeavored to do so. As always, if you would like to discuss any of the following recommendation further, 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

Auditing & Verification 4

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

Auditing & Verification

Firewall Configuration Settings

Are periodic reviews of firewall settings being conducted?

Reviewing firewall settings, such as port status, mappings, rules, VPN's, geographic communication restrictions and other critical settings helps to identify and eliminate unnecessary attack vectors. As technology needs change, inbound and/or outbound ports may occasionally need to be opened or closed to meet communication requirements. When such settings are no longer required, it is not uncommon for them to be overlooked and left in place. For this reason alone, reviewing ports is a particularly useful practice in environments with multiple administrators.

Additionally, given the potential for malicious actors to surreptitiously breach networks as a result of unknown third-party software exploits, periodic examination of firewall settings can often alert IT professionals to the existence of breaches that might otherwise go unnoticed for some time.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Firewall Firmware & Subscription-Based Security Services

Are firewalls being inspected periodically to confirm that subscription-based security services are active, and that the device is employing the most current stable firmware revisions?

New firewall firmware is released as bugs and/or security flaws are identified and resolved. Firmware updates are critical to maintaining the best available protections against newly discovered exploits, and system stability impediments.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Firewall Logs

Are firewall logs being reviewed periodically?

A periodic review of firewall logs can help to identify possible attacks, and sometimes even their place of origin. Although many log entries may not constitute actionable information, the heightened awareness that results from reviewing log enables security to be further tightened in various areas as deemed appropriate.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

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

Third-Party Audit Utilities

Have formal auditing utilities been deployed to augment built-in audit trail mechanisms with limited capabilities, or to provide audit trails for solutions that offer no built-in audit trails?

While many technologies feature built-in logging and/or auditing functions, simple and inexpensive third-party products can often bridge shortcomings and increase visibility by aggregating and parsing logs and data from multiple disparate systems, or by simply collecting data that is available but not being logged. Third-party auditing solutions can streamline management, aid in the identification of misconfigurations, help identify attack or breach vectors, and in some cases, even identify malicious or undesired behavior from authorized users.

Status ☐ ✓ ☐ − ☐ ?

NOTES: _____

_____

_____

Backup Verifications

Are regular verification checks and random file restorations being performed periodically to confirm backup viability?

Notifications that a backup has successfully completed should never be regarded as conclusive. It is possible for backup images or chains to become corrupted without the knowledge of an administrator. Corruption can cause irreparable damage to files and never be discovered until such time as it becomes necessary to restore from backup. Crypto virus infections can be contracted and encrypt some volumes and not others and go undetected for weeks or even months if the encrypted files are not accessed during the normal course of business.

Due to the foregoing and numerous other reasons, it is essential to regularly test backup data to confirm viability and integrity. Failure to do so can potentially lead to a situation where deletion, corruption, malware-based encryption, or other damage has unknowingly occurred, and backup data is not viable. In such situations, recovery options may be limited to restoring a version from an older backup or accepting a permanent loss.

Status ☐ ✓ ☐ − ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

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

Password Reviews

Are passwords to devices and systems being reviewed, changed, and tested periodically?

The use of default passwords on devices such as managed switches, WAPs (Wireless Access Points), printers, and other network hardware creates exposure that can be leveraged by malicious actors in ways that vary in severity depending on the network resource. Similar, failure to periodically change these passwords (especially when IT-related turnover occurs) can be a potential source of exposure.

Status ☐ ☐ ☐

NOTES: _____

_____

_____

Application Reviews

Are servers, user workstations and other devices periodically inspected for the presence of unauthorized software?

Unauthorized software installations can create system instability due to incompatibilities, and they can be the source of exposure to serious security risks. Even reputable software installed without authorization can create exposure because there can be no assurance that security patches and fixes are being deployed in a timely manner, or at all.

Even when users are denied local administrative privileges, occasional checks are recommended, as some administrators occasionally succumb to pressure from friendly co-workers or high-ranking executives to install unauthorized software, even when doing so constitutes a violation of company policies.

In addition to the potential for creating security vulnerabilities, unauthorized software can cause performance degradation on local workstations, effectively reducing lifecycles and necessitating premature replacement. Reducing equipment lifecycles for as little as six months can cost an organization thousands of dollars, given that workstations are typically replaced en masse, or in groups.

For maximized efficiency, application reviews can often be conducted using network maintenance scans that automatically inspect managed devices from a central location and produce reports listing applications installed.

Status ☐ ☐ ☐

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

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

Rights and Permissions Reviews

Are users accounts, folder access rights, user permissions, email distribution groups and other centralized network settings periodically reviewed and updated as necessary?

Most business network environments are highly fluid and constantly changing. This can make it difficult, if not impossible, for administrators to effectively track changes and keep pace with changes. It is not uncommon for users to change departments and require access to different folders and solutions, while maintaining access to folders required for their previous job function. But for how long? And who is tracking this and notifying IT when it's time to revoke that access? Similarly, supervisors may require access to a departed employee's email and other resources? Again, for how long and who is tracking this? Without periodically reviewing the foregoing and related settings with management, dormant accounts can potentially be breached and utilized by malicious actors without drawing attention to themselves because no one else is using them, or even aware of their existence.

As with the preceding recommendation, data for these reviews can typically be produced by conducting network maintenance scans that automate the collection of settings, permissions, user accounts and related information and produce reports that can be easily reviewed by IT and designated management personnel.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Breach Disclosure Checks and Dark Web Searches

Is the organization routinely checking for third party breach disclosures and Dark Web sources for evidence of compromises?

It is important to reset login credentials for services that have been hacked, so that malicious actors cannot gain access to a breached user's account. Depending on the service and scope of the hack, other personal information such as credit card numbers, home addresses, and social security numbers can be leaked as well. When organizations or individuals are quickly alerted that a leak has occurred, that knowledge can prove extremely helpful in mitigating damage and preventing identity theft.

Often users will ignore company policies prohibiting the use of identical email and password combinations for multiple online services. In such cases when a third-party website software solution is hacked and a person's login credentials are released malicious actors typically attempt to use the leaked credentials to access other services that the user has signed up for, which can include company-related systems. (Users should be advised to never use company email addresses for access to any websites or resources that are not authorized and required by the company for them to perform their job functions.)

Breach disclosures can be searched online via several free websites however it is recommended that organizations do not attempt to perform their own Dark Web searches for a number of reasons. Subscription-based services are available that conduct both Dark Web searches and disclosure searches for all domain users and provide monthly reports in a simple and easy to understand format.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

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

Web Activity Monitoring

Is a solution in place to facilitate the monitoring of Web use as needed for security and productivity purposes?

Web use monitoring is employed to aid in proactively identifying user misconduct, to protect proprietary data, and to encourage productivity.

While highly beneficial in some environments, the decision to employ Web use monitoring and controls warrants careful consideration. Although an organization's policies may (and typically should) stipulate that users have no right to or expectation of privacy, the use of aggressive monitoring can have an adverse impact on a company's culture if not introduced properly. Simple utilities can be deployed to collect user activity data for review when necessary and are deemed adequate for most organizations.

When appropriate, more aggressive solutions are also available that can facilitate daily time limits for non-business Internet use (online shopping, etc.). Limits can be imposed selectively by groups, and access can be permitted in full, or restricted entirely if desired.

Status ☐ ☐ ☐

NOTES: _____

_____

_____

LAN traffic analysis.

Is a system or solution in place to facilitate automated analysis of LAN traffic patterns and activity?

Because Trojans, botnets and other forms of malicious activity will frequently create outbound connections, the ability to review activity logs and reports can help to identify potential compromises to an organization's network environment. As an example, outbound connection attempts to IP addresses in nations the organization does not require remote access into the network from could potentially merit examination. This is one example of a myriad of indicators that can potentially point to a breach or attack.

To maximize visibility into potentially suspicious activity, organizations may elect to deploy what is known as a security information and event management or "SIEM" solution to automate the collection and analysis of activity-related data on a 24/7 basis. While large enterprises may assign the responsibility of conducting daily reviews of SIEM alerts, SMB's often elect to subscribe to third-party services that transmit alerts to third-party firms that monitor and analyze alerts around the clock and notify the organization's IT personnel or other designee(s) when an analyst believes an alert warrants further inspection and potential remediation and response.

Status ☐ ☐ ☐

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

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

Penetration Testing (Third party)

Are periodic penetration tests performed to proactively identify potential security vulnerabilities in need of remediation?

Penetration testing is the practice of conducting simulated attacks on an environment as a means of identifying weaknesses before they are identified and exploited by malicious actors. There are various types of penetration testing methods and protocols. Professional penetration tests are recommended, and in most cases, they should be performed by independent and neutral third-party professionals that are unassociated with the organization's internal IT personnel and outsourced IT providers.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Surveillance and Access Control Systems

If surveillance cameras and/or electronic access control systems are used, are feed recordings periodically reviewed and access logs inspected to ensure proper functionality and identify potentially anomalous activity?

As with all security systems and devices, surveillance cameras should be tested regularly to insure proper function and availability in the case of a cybersecurity or other event. Without testing or monitoring, it is possible for camera NVR or DVR devices to become suspended and cease recording without an organization's knowledge.

At the time of this writing, the most commonly used access control systems employ technology that enables access cards to be electronically read and duplicated in as little as seven seconds with the push of a single button using a device resembling an automobile key fob that costs less than $50.

Electronic access control system logs should be inspected for signs of anomalous activity, such as access at odd hours, and failed entry and/or exit attempts logged when the control system has already registered a cardholder as having entered or exited the facility.

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.

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