Best Practice Checklist Series - Issue 5

Authentication Security, Network Traffic & Activity Analysis

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®

Authentication Security, Network Traffic & Activity Analysis

The purpose of this guide is to provide non-technical personnel a brief overview of authentication essentials, and traffic analysis solutions to enhance security. Because no two networks are identical, it is recommended that you discuss the topics that follow with your IT professional(s) to ascertain the applicability of each recommendation and agree upon each measure's importance within the context of your particular environment.

At a time when threats to information security are at an all time high, asking the right questions and ensuring you're receiving optimal protection has never been more important.

Should you wish to discuss any of the information that follows, your Sandbox Technologies Engineer, Account Manager, or Consulting CIO will be happy to answer any questions you may have.

Authentication Security

Although no environment is 100% secure, strict authentication controls, such as Multifactor or Two-Factor Authentication (2FA) have become a must have for businesses. Other practices, such as requiring password complexity and periodic password changes are also essential.

Network Traffic & Activity Analysis

Ongoing analysis of network activity has similarly become an important component of establishing a proactive security posture. The ability to detect threats in real-time can oftentimes provide an opportunity to thwart attempted attacks before serious damage has been done. And when the inevitable breaches do occur, the ability to identify attack vectors and take immediate action can mean the difference between success and failure for a business.

SANDBOX TECHNOLOGIES

© 2017-2021, All Rights Reserved. Sandbox Technologies, Inc.

Table of Contents

Recommended Practices – Authentication Security 4
Recommended Practices - Traffic and Activity Analysis 8

SANDBOX TECHNOLOGIES
© 2017-2021, All Rights Reserved. Sandbox Technologies, Inc.

Recommended Practices – Authentication Security

Enforce Password Complexity & Minimum Length Requirements

Do all systems require that passwords consist of upper and lower-case characters, numbers, and special characters, and it is recommended that they be no less than 14 characters in length?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Educate Users Regarding Acceptable Password Selections

Have all users been suitably educated in proper password selection practices, including the avoidance of popular phrases, single dictionary words, and the use of common substitutions (e.g., “@” in the place of “a”, “1” in place of “i”, etc.)?

It is often helpful to explain to users that failure to adhere to these basic principles can lead to passwords being easily compromised using simple and widely available hacking tools.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Unique Passwords

Are unique passwords being used for for all solutions and services?

Users should be advised that employing the use of the same password can create serious security exposure. Hackers are aware that users commonly ignore this recommendation for convenience, and upon breaching one solution, device, website, or cloud-based resource, they will often attempt to use the same password to access other services, including those of the company. The use of identical passwords for different purposes should be avoided at all costs, especially for administrative credentials and core networking devices where the breach of one credential can lead to a cascading effect and amplify adverse consequences by an order of magnitude.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

© 2017-2021, All Rights Reserved. Sandbox Technologies, Inc.

Mandatory Periodic Password Changes

Are periodic password changes being required and electronically enforced in keeping with the minimum recommendations of applicable third-party compliance requirements?

Recommendations for the frequency at which passwords should be changed vary. Expert studies have shown that too frequent changes lead to dangerous user habits, such as recording passwords on sticky notes attached to displays or making only small incremental password changes with each new iteration. Conversely, it has also been demonstrated that requiring frequent password changes forcibly reduces the occurrences in which users select the same password for use with different services – A serious problem described in the previous recommendation. It is recommended that organizations carefully weigh the pros and cons of different password change frequencies, follow the guidelines of any applicable regulations they are subject to, and select a reasonable password change policy of not less than once every 90 days.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Third-Party Vendor Access

Is access to network resources by third-party vendors limited to only those that require unassisted remote access to perform their required function(s)?

Vendors of various third-party software and technologies sometimes require access to server resources to provide maintenance, support, and upgrades. Unfortunately, access by any party increases exposure to security risks. It is recommended that third-party vendors requiring only occasional remote access be required to submit written requests before being granted access on a manual, per-use basis.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Unique Administrative User Logins & Passwords

Are administrative users assigned unique logins and passwords?

When multiple administrative users exist, each should be assigned unique administrative accounts and passwords. The use of shared administrative credentials not only increases the risk of disclosure, it also renders it difficult to undertake auditing efforts and forensic investigations with any degree of certainty because audit logs do not reflect the actions of individual users. Shared administrative credentials also necessitate additional labor effort when terminating administrative users, because all accounts known to them must be changed, along with any attendant services, automated tasks, etc. Additionally, administrative accounts should be separate from normal user accounts for the same individual. The purpose of this practice is to mitigate the potential for damage if an administrative user should inadvertently become breached or disclose his or her credentials in the course of conducting normal work activities (e.g., accessing email, etc.)

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

© 2017-2021, All Rights Reserved. Sandbox Technologies, Inc.

Administrative Credentials Maintained by Designated Management Representative(s)

Does a designated and trusted, non-technical staff member maintain a secure and comprehensive list of (unique wherever possible) administrative access credentials to company systems?

Administrative credentials should be maintained at all times by a designated executive entrusted with their care. All executives of equivalent rank or higher should be aware of who the individual vested with this responsibility is, and the associated ramifications. This practice is key to preventing company systems from being held hostage by disgruntled IT employees or vendors, and can help avoid uncomfortable requests for password information in the event a personnel change or third-party inspection is required.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Secure Password Repositories

Are passwords stored in secure password repositories only?

Storing passwords in emails, instant messages, spreadsheets, documents, contact databases, accounting software, low-cost browser-integrated solutions, and even some well-respected cloud-based password repositories can create significant exposure for organizations, especially those that must routinely share passwords among staff. Password-protection on spreadsheets and documents can often be easily overcome and should never be used.

While organizations may wish to weigh the risks of using various well-respected and largely secure cloud-based password repositories, it must be remembered that their adoption places a high degree of trust in the ability of the provider to keep these very high-value hacking targets safe.

For optimal security, it is recommended that organizations host their own repository internally behind a multifactor-protected VPN and using enterprise-class software that requires secondary multifactor authentication for access. Optimally, the solution selected should include audit trail functionality that enables an administrator to produce reports detailing all dates and times that a password was accessed along with the username of the individual accessing it.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

© 2017-2021, All Rights Reserved. Sandbox Technologies, Inc.

Multifactor Authentication

Is multifactor authentication required for access to all company resources?

In addition to a password, multifactor authentication (also sometimes referred to as 2FA or Two-Factor Authentication) requires the entry of a unique security code generated by a token or a mobile device application to authenticate to protected systems. MFA greatly increases security by not only requiring the knowledge of a valid password (1st factor), but also the security code (2nd factor) to gain access to resources.

Because each user's security code changes frequently (administrators often opt for every 60 seconds), multifactor authentication lessens the likelihood of a data breach in the event a user unwittingly allows their username and password to become compromised. It is strongly recommended that all organizations implement multifactor authentication to protect all supported information technology systems, including cloud-based solutions.

The types of multifactor solutions vary and are often dictated by the platform(s) in use (Mac and/or PC), and by what solutions are supported by the applications in need of protection.

Implementation methods range from simple and inexpensive configurations requiring manual entry of a mobile phone generated code for each protected solution, to more friendly “Push Based” solutions. More complex configurations also exist, such as SSO (Single Sign On) which can further lessen user burden by unifying credentials and thus allowing authentication to multiple systems at once.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Automatic Screen Locking

Are computers configured to lock their screens automatically after a designated period of inactivity, and are users instructed to manually lock their workstations whenever they will be unattended?

Leaving workstation logged while unattended creates exposure to unauthorized access if a malicious actor uses this opportunity to gains physical access.

It is recommended that a centralized measure be implemented causing workstations to lock after no more than fifteen minutes of inactivity, and less, if possible. While such policies can be established on a workstation-by-workstation basis, centralized control provides proper visibility and aids organizations in ensuring ongoing compliance. Users should also be instructed to manually lock their workstations whenever they will be unattended.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

© 2017-2021, All Rights Reserved. Sandbox Technologies, Inc.

Recommended Practices - Traffic and Activity Analysis

LAN Traffic Analysis/SIEM Solution

Does the organization employ the use of a LAN traffic analysis or SIEM solution that alerts administrative personnel to anomalous and/or potentially nefarious activity?

SIEM (Security Information and Event Management) solutions are a valuable tool for proactively identifying possible security threats and enabling organizations to take rapid remediatory actions. SIEM solutions work in many ways. Because Trojans, botnets and other forms of hacks/exploits will frequently create outbound connections, SIEM activity logs and reports can help identify potential compromises to an organization's network environment. As an example, outbound connection attempts from the United States to IP addresses in foreign nations could potentially merit examination unless the company is conducting business in those nations or has executives traveling there need for person(s) there to connect to the organization's network.

Unusually large offsite data transfers are often flagged by SIEM solutions and can be indicators of internal corporate malfeasance. Non-secure connections to third-party services are also sometimes flagged and can indicate that an employee may be using an unauthorized communication platform.

SIEM solutions range in price and functionality. It is recommended at a minimum that organizations seeking to create a strong security posture implement, at a minimum, an automated SIEM solution to review data for anomalies, escalate potential threat indicators for human analysis, and report on suspicious network events.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Audit Utilities

Have suitable auditing utilities been deployed within the environment to provide a means of tracking administrative actions?

While many technologies feature built-in logging and/or auditing functions, more often than not, the data collected is minimal, and often disappears upon re-boot of the device. Third party products serve to bridge these shortcomings and increase visibility by aggregating and parsing logs and data from disparate systems into useable, actionable data. There are numerous reasons why the use of audit utilities is highly recommended:

-Should administrative personnel abuse their authority to obtain confidential information or deny making honest mistakes that unintentionally resulted in widespread problems, Audit utilities are an effective means of eliminating doubt by establishing who did what.

-Audit utilities often identify anomalies that lead to the identification of misconfigurations, the remediation of which can optimize performance and enhance security.

-In the event of a data breach, audit utilities can provide indispensable information to help identify attack vectors and responsible parties. Should a forensic examination be required to determine the source and scope of damage, an effective audit trail can mean the difference between spending countless financial

SANDBOX TECHNOLOGIES

© 2017-2021, All Rights Reserved. Sandbox Technologies, Inc.

resources assuming the worst and notifying an entire database of customers and mitigating damage to an organization's credibility by notifying only a small few whose records were accessed.

-In an environment where personnel work remotely, audit utilities can provide a detailed window into user activity that is often helpful to management when key performance indicators are unavailable or difficult to define.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Web Use Monitoring

Is a solution for monitoring and/or limiting the use of Web-based resources in accordance with company practices in place?

Web use monitoring is a strategy employed to proactively police employee conduct, protect proprietary data, and encourage employee 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.

If an organization is experiencing a significant decline in productivity believed to stem from personal Web activity during business hours, popular utilities can restrict access to designated content, and track user activity down to the keystroke. Such utilities can also enforce daily Internet use time limits for non-business activities (online shopping, etc.). Limits can be imposed selectively by groups, and access can be permitted or restricted entirely if desired.

Personnel whose business functions require access to Web destinations that might ordinarily be considered inappropriate can be exempted from filtering, however it is recommended that any such personnel also be provided with software that facilitates Web browsing via virtual sessions to reduce the likelihood of malware infections. In such cases, special considerations are often recommended to limit liability for personnel whose job functions require Web searches that are likely to yield results containing pornography, hate advocacy, or other objectionable content that could lead to employee litigation. Such considerations may include obtaining legal acknowledgements, modified employee position descriptions, adding privacy screens to displays, and/or positioning employee displays in such a manner as to prevent others from observing activity. In any such cases, the company should seek the guidance of its legal representation to determine suitability and the appropriate measures.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

© 2017-2021, All Rights Reserved. Sandbox Technologies, Inc.

Physical Access Control / Visitor Logging

Are suitable systems in place to restrict physical access to authorized personnel only, log visitor ingress and egress, and provide for the safety and security of employees, visitors, and other persons?

Electronic sign-in systems, cameras and visitor identification badges enhance an organization's physical security, and act as an added deterrent to individuals seeking easy targets for equipment theft and other crimes. Such measures are particularly beneficial in high-traffic environments, and in areas where sensitive data is housed, or high-value inventory items are stored. The use of visitor badges raises employee awareness, and aids in identifying individuals that may be on the premises without authorization.

Although physical access protections are an essential component of many businesses, their benefits to smaller organizations can vary. It is recommended that every organization's management consider the likelihood of unauthorized persons gaining access to the office suite if the reception desk or entry is unattended and decide whether the likelihood of theft or threats to personal safety justify the implementation of physical security measures.

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

© 2017-2021, All Rights Reserved. Sandbox Technologies, Inc.