

Best Practice Checklist Series - Issue 9

Workstation Security, Standards, and Practices

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®

Workstation Security, Standards and Practices

Workstations are one of the most essential components of a network. With the continual rise of social engineering and other threats to security, properly securing and controlling front line devices is essential. (*For purposes of this issue, we use the term workstations to include laptops and user computers of various form factors*). Although no practical environment can be 100% secure, the handful of recommendations that follow can go a long way toward protecting your organization.

Unfortunately, security isn't always convenient or pleasant, and many measures are understandably met with resistance from users. For any organization to have strong security, it must have the will to do so. Moreover, for success, it is essential that its commitment to security be supported and expressed from the very top.

We hope that you find the following recommendations useful within your organization, and as always, should you have questions, feel free to contact your Sandbox Technologies Engineer, Account Manager, or Consulting CIO.

SANDBOX TECHNOLOGIES

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

Table of Contents

Workstation Security 4
Workstation Standards and Practices 9

SANDBOX TECHNOLOGIES

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

Workstation Security

Hardening Standards*

Have formal hardening standards been adopted and implemented for all workstations and any exceptions documented?

Hardening standards create a framework to mitigate vulnerabilities on workstations in an environment. Examples of workstation hardening settings include:

- User rights (restricting UAC bypassing, removing local administrative rights, etc.)
- Windows Firewall settings (disallowing all inbound communications, restricting certain outbound connections, etc.)
- Changing the way workstations communicate and operate (disallowing more than two previously cached credentials, forcing session re-authentication every twenty minutes, etc.)

The National Institute of Standards & Technology (NIST) publishes an extensive list of recommended hardening standards which are the generally accepted benchmark used by security professionals. Different use scenarios require different settings, so while they are recommended when possible, NIST standards aren't necessarily one size fits all, and some settings may need to be altered in order for a user to perform their required job functions.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

*Several of the individual recommendations that follow fall within the scope of NIST hardening standards and may be redundant if workstation hardening is implemented.

Local Administrative Rights Disallowed

Are local user administrative privileges restricted?

Granting local administrative rights to user workstations weakens security and is strongly discouraged. Often, full administrative rights to a local machine are required for viruses, trojans and rootkits to take full effect. While infection is sometimes still possible without local administrative rights, the restriction of privileges for normal domain users can reduce the likelihood of infection. It is also possible for domain users with administrative access to make unauthorized changes to their workstations (creating shares, installing unauthorized software) or, in some cases, to bypass security policies entirely. This in turn can affect system stability by nullifying security configurations and creating security flaws that can be used as attack vectors inside the network environment.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

SANDBOX TECHNOLOGIES

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

DNS Filtering

Are all workstations configured to browse Internet resources via a DNS provider that blocks sites deemed to be potentially malicious?

DNS (Domain Name Server) is the system by which domain names (e.g., www.google.com) are referenced to the IP address hosting the respective name. For example, www.google.com can also be reached by entering the IP address 172.217.14.68 into a browser and sometimes vise-versa. A DNS scanning solution matches traffic originating in a network environment and destined for public Internet resources against a database of known malicious addresses.

The solution also matches this traffic against a heuristic database of features and attributes in an attempt to identify new malicious destinations. When a malicious destination is detected, the scanning solution responds with a warning page, routing the traffic away from the threat, thus helping to mitigate the dangers posed by “drive by infections”, “phishing websites”, “Trojan Horses” and other types of malware. DNS filtering solutions add another layer of security for the environment and help to mitigate loss and downtime due to non-targeted, infections stemming from the use of Internet resources.

.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Antivirus/Anti-Spyware

Has a centrally managed and updated antivirus solution been deployed and properly configured?

Workstation antivirus is one of the fundamental safeguards a network has against cybersecurity threats. A properly configured antivirus solution can help mitigate outbreaks on a network. An effective antivirus suite offers protection against Internet-based threats, and infected resources that are introduced into an organization’s network. Antivirus solutions can also mitigate the use of rootkits and backdoors by malicious actors in the event of a compromise.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Drive Encryption

Has a centrally managed and updated antivirus solution been deployed and properly configured?

In the event of loss or theft, unencrypted computer data (files, cached emails, saved passwords, etc.) can be susceptible to unauthorized access. Password security on unencrypted devices can be circumvented easily by removing and attaching the device’s hard drive to another computer. With minimal effort, even deleted files can often be accessed, provided they have not been overwritten by other data.
Whole disk encryption is designed to prevent anyone except the password holder from accessing data, and it is recommended for all workstations and laptops that access company resources or contain company data.

SANDBOX TECHNOLOGIES

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

While workstation encryption can be enabled on an individual basis using the built-in encryption capability of current revisions of Windows, policy-based deployment is recommended for proper control and visibility. Optimally, a third-party solution with the ability to centrally manage keys and facilitate encryption using software other than the built-in BitLocker encryption is recommended.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

Screen Saver Locking

Are screen savers enabled and set to lock automatically after a reasonably brief period of inactivity?

Leaving an unattended workstation logged in creates exposure to unauthorized access if a malicious actor gains physical access to the machine. While users should be required to lock their workstations anytime they will be unattended, it is recommended that screen savers be configured to lock automatically after no longer than 15-30 minutes of inactivity, and ideally less.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

Removable Media Restrictions

When possible, is the use of removeable media restricted?

Allowing access to USB ports carries with it a number of risks. The ability for users to connect non-company owned USB devices (thumb drives, external USB hard drives, etc.) creates exposure, because it is not uncommon for such devices to contain data that is infected with malware, rootkits, ransomware, etc.

USB access is also a common method that dishonest employees use to remove data from corporate networks without authorization. Microsoft Windows GPOs (Group Policy Objects) can be configured to disable USB ports while permitting authorized devices to function on PC workstations. To ensure minimal disruption, this feature requires testing and a thorough review of employee workflows prior to implementation.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

SANDBOX TECHNOLOGIES

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

Password Complexity

Does workstation access require the use of a complex password?

Workstations should always be password protected. Password complexity refers to the mandatory use of different types of characters to form passwords: letters, digits, and special characters. Greater password complexity and increased length can help to prevent unauthorized access, because the time and resources required to exploit passwords increases exponentially as complexity and length increase.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

Multifactor Authentication

Is access to the workstation secured by multifactor authentication?

Multifactor authentication (MFA) requires a device such as a token or a mobile device application, in addition to a password, to authenticate to various workstations and resources in an environment. This greatly increases security by not only requiring the knowledge of a working password (1st factor), but also the possession of a device (2nd factor) to gain access to resources. It is strongly recommended that MFA be implemented for all workstations.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

Patch Management

Has a solution been deployed to automate the deployment of operating system and software patches?

Software vendors regularly release updates intended to fix security vulnerabilities and system instabilities. Keeping operating systems and software up to date helps to mitigate exploitation of security flaws. Downtime due to known software bugs is also reduced, along with the attendant support costs.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

Software Firewall

If the company's security practices include the use of software firewalls for mobile devices and/or remote users, has the company's chosen firewall solution been deployed and/or configured?

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

SANDBOX TECHNOLOGIES

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

Third-Party Storage Solutions

Has the installation of third-party storage solutions been restricted to only solutions authorized and controlled by the organization?

Dropbox, iCloud, Hightail and other file sharing services create both security hazards (from the lack of control over what is being uploaded and download), as well as potential legal exposure due to the sharing of sensitive data over platforms with

File sharing services also enable users to potentially remove files from an otherwise secure location, thus bypassing many security measures.

Workstations that auto-sync or auto-upload can cause a situation where damaged data (such as corrupted data or files encrypted by ransomware) is inadvertently synchronized with other machines, overwriting, and destroying viable data as a result. Auto synchronizing can also permit ransomware or other malware to infect other computers that share folder access with the infected workstation.

Status ☐ ☐ ☐

NOTES: _____

_____

_____

Password Complexity

Does workstation access require the use of a complex password?

Workstations should always be password protected. Password complexity refers to the mandatory use of different types of characters to form passwords: letters, digits, and special characters. Greater password complexity and increased length can help to prevent unauthorized access, because the time and resources required to exploit passwords increases exponentially as complexity and length increase.

Status ☐ ☐ ☐

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

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

Workstation Standards and Practices

Supported Operating Systems Only

Are all workstations utilizing unsupported/end of life operating systems retired from service?

Unsupported operating systems can lead to system instability, compatibility issues with new software and hardware, and security holes when unpatched bugs or exploits are used by malicious actors, viruses, or trojans. Operating systems nearing end of life should be retired prior to the discontinuation of support by the operating system manufacturer.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Surge Protection

Are all workstations connected to surge protectors?

Power surges and "brown-outs" can damage workstation hardware and result in data loss. Optimally, workstations should be protected surge protection device featuring small battery units that will briefly sustain power continuity in the event of a brief power interruption, providing users an opportunity to save any work in progress and shut down gracefully. At a minimum, workstations, displays and associated equipment should be connected to power strips featuring surge protection, and never plugged directly into a wall receptacle.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Remote Access

Has remote access been restricted to only company authorized solutions?

VPN and other remote access rights should be granted only to trusted employees with a demonstrated business need and limited to only the required systems. Prior to implementation, remote access should be approved by both department heads, and IT management. Prior to implementation, any third-party remote access applications should be thoroughly vetted, documented, and formally approved. (For more information about remote worker solutions, see Issue #1, "Remote Worker Productivity and Productivity".

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

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

RMM Deployment

If the organization utilizes a Remote Monitoring and Management (RMM) solution, has the solution been deployed and properly configured on all relevant nodes?

The deployment of a secure and effective RMM solution plays a pivotal role in ensuring that systems are well managed and maintained. Improper configuration can lead to missed alerts, failed patch deployment and other exposure.

Status ☐ ☐ ☐

NOTES: _____

_____

_____

Authorized Software Only

Are users prohibited from installing (or directing IT to install) software not formally vetted and authorized for use on company systems?

Unauthorized software installations can create system instability due to incompatibilities and/or security flaws arising from unpatched bugs.

Such software can also cause performance degradation on local workstations, effectively reducing lifecycles and necessitating premature replacement. A reduction in useful lifecycle for as little as six months can cost an organization thousands of dollars, given that workstations are typically replaced en masse, or by groups.

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.