Lodestone

Best Practices Overview

Best Practices Overview

Lodestone recommends that organizations consider the best practices described below when making changes to their environments.

Employ a CASB

A cloud access security broker (CASB) can be placed between on-premises resources and cloud providers to monitor activities and enforce security controls. Properly configured CASBs can be useful in organizations where certain departments require the ability to procure and manage their own cloud resources. A number of security measures can be enforced within CASBs, including the implementation of web application firewalls (WAFs), data loss prevention (DLP), and access controls that can assist with the identification of suspicious activity within an environment. Lodestone recommends that companies consider employing CASBs.

Enable MFA

Multi-factor authentication (MFA) can help prevent the compromise of user accounts, an especially critical function for those with administrative privileges. MFA requires secondary authentication beyond an account name and password and can include verification methods such as phone calls, generated passcodes, smart cards, and biometric devices. Lodestone recommends that companies enable and enforce MFA for all user accounts.

Enforce Security Awareness Training

A widely supported principle in computer security is that a company's employees are its first line of defense. Educating personnel on how to identify suspicious activity, such as emails that may contain malicious links or attachments, can prevent compromise. Many security incidents begin with attackers tricking employees through social engineering tactics or luring them into opening suspicious attachments or links. Lodestone recommends that companies provide security awareness training to all employees upon hire and annually thereafter.

Establish an IRP

An effective incident response plan (IRP) should consist of roles and responsibilities for information technology (IT) staff, including detailed procedures for a number of different scenarios. A list of critical network and data recovery processes should be kept up to date within this document for use when data losses occur. Lodestone recommends that companies maintain IRPs and update them annually or as needed.

Enforce Strong Passwords

Complex and unique passwords on user and administrator accounts can reduce an environment's susceptibility to brute force attacks and other common tactics employed by threat actors. Lodestone recommends that companies require all user account passwords to be updated at least quarterly and contain one uppercase character, one lowercase character, one number, and one special character at a minimum.

Implement a DLP Solution

A DLP tool can be placed within an environment to detect potential data breaches or data exfiltration. An organization can configure a DLP solution to monitor for common characteristics of sensitive information handled by its personnel to help ensure that this data does not leave the environment either by accident or for nefarious purposes. These tools can be applied to data in a variety of forms, including data in use, data in transit, and data at rest. Lodestone recommends that companies obtain DLP solutions and tailor their configurations specifically for their businesses and the sensitive data they handle.

Maintain Backups

Retaining backup data and checking the integrity of the backups can help companies rebuild critical systems if unforeseen events cause them to be lost. Backing up and maintaining key information in safe locations both on-premises and off-site can enable companies to respond quickly to security incidents and other issues without fear of potential data loss. Lodestone recommends that companies configure daily backups of their critical systems.

Perform Proactive Monitoring

Monitoring networks for suspicious activity can empower companies to more quickly and effectively isolate and remove potentially unwanted programs or applications from environments. Lodestone recommends that companies consider the use of behavior-based endpoint detection and response (EDR) solutions to monitor their environments. Examples of EDR products include Endgame and Sentinel One.

Perform Security Reviews of Third-Party Vendors

Selected third-party IT vendors should be subject to thorough information security risk assessments and be required to provide proof of information security risk assessments and written policies and procedures that support security compliance. Lodestone recommends that companies require all IT vendors to provide proof of compliance with their own and the company's security requirements upon establishing contracts and annually thereafter.

Restrict User Permissions

Restricting user permissions to install and execute software applications can prevent the accidental or intentional introduction of malware into an environment. Lodestone recommends that companies employ the principle of least privilege, in which each user is assigned the minimum level of privilege necessary to perform their activities.

Retain and Review Logs

Adequate logging and auditing within an organization is critical to ensure the identification, prevention, and containment of suspicious or unwanted actions. Dynamic Host Configuration Protocol (DHCP), firewalls, intrusion detection systems (IDSs), antivirus (AV), virtual private networks (VPNs), Windows event logs, and other application and database logs should be appropriately maintained, reviewed, backed up, and made accessible to the appropriate staff members. Logging for some components, such as Microsoft 365 (M365), are disabled by default, but can provide critical information in preventing and responding to potential security incidents. Logging events can also be used to apply statistical analysis to user events and system activities to help identify anomalous behavior. Lodestone recommends that companies enable the collection of all event logs possible.

Review Integrated Applications

Applications can be integrated into the M365 environment to support a number of functionalities. Consistent vetting of these applications can assist with the identification of unapproved or unvetted third-party software. Lodestone recommends that companies block and disable unmanaged applications to help prevent users from inadvertently granting malicious software access to company information.

Secure BYOD Devices

Bring-your-own-device (BYOD) policies can present a unique challenge to security, as the devices themselves are not owned by the company. Lodestone recommends that companies take measures to ensure that BYOD devices are only given access to necessary resources and are otherwise segregated from their infrastructure.

Segment Networks

Proper network segmentation can improve an organization’s security posture by restricting access to specific resources within the environment and makes potential unauthorized access more difficult. Maintaining a flat and open network can create a major security risk: if unauthorized access occurs, a threat actor can easily access additional computer systems on the network. A segmented network would limit the threat actor to the same subnet as the initially infected system. Efficient network segmentation also limits internal resources that can be easily accessed, which can also strengthen security against internal threats. Lodestone recommends that companies maintain well-defined network configurations that include secure, internal network zones and external, untrusted network zones.

Update and Patch Regularly

Attackers often scan Internet-exposed devices for outdated programs and operating systems with known vulnerabilities that can be exploited. Lodestone recommends that companies update software applications as quickly as possible when new versions are released and maintain the latest operating system patches on hosts within their networks.

Block Attachments by File Type

Lodestone recommends that companies harden their Outlook instances against malware attachments by blocking attachments with certain file types.

Configure this feature using the M365 Defender portal with the following steps:

- Navigate to the portal and navigate to **Email & collaboration** > **Policies & rules** > **Threat policies** > **Anti-malware** in the **Policies** section.

- On the **Anti-malware** page, double-click on **Default (Default)**.
- Select **Edit protection settings** at the bottom of the new window that appears.
- On the next page, under **Protection settings**, select the checkbox next to **Enable the common attachments filter**.
- (Optional) Add or delete file types from the list of file types using **Customize file types**.
- Select **Save**.

Disable Legacy Authentication Protocols

Legacy authentication protocols can be defined as authentication requests via older mail protocols such as Internet Message Access Protocol (IMAP), Simple Mail Transfer Protocol (SMTP), and Post Office Protocol version 3 (POP3). Though some services accept this type of authentication for ease of access, these types of logins are not compatible with MFA and can weaken an organization's security posture. In addition, successful logins via legacy authentication protocols allow the corresponding user's mailbox to be synced (i.e., fully downloaded to an external location). This can be exploited by threat actors to quickly exfiltrate the contents of a mailbox. Lodestone recommends that companies disable legacy authentication protocols wherever possible.

Disable Macro Scripts

Active Microsoft Office macro scripts are not necessary for every environment, and some malicious macro scripts are employed by attackers to compromise systems. Administrators can disable macros within Microsoft Office applications to help prevent such malicious payloads from executing within the environment. Lodestone recommends that companies consider whether macro scripts are necessary for their operations and, if not, disable them.

Implement a PAW

Privileged access workstations (PAWs) can help ensure that the execution of administrative tasks is as secure as possible. PAWs are dedicated computers to be used for sensitive configuration tasks, such as M365 settings that require the use of a global administrator account. PAWs should never be used for web browsing or email to reduce their exposure to potential malicious content. Lodestone recommends that companies set up at least one PAW for use by their IT teams when performing configurations using administrator accounts.

Implement gMSAs

Group Managed Service Accounts (gMSAs) are a feature in Microsoft Windows Server 2012 and later that enable additional security controls related to service accounts. In addition to native improvements on password security, gMSAs can be hardened to reduce a threat actor's means to escalate privileges and move laterally in the event that an account is compromised. Lodestone recommends that companies pursue the conversion of their service accounts to gMSAs if this feature is not already in use.