A picture containing food, drawing

Description automatically generatedWork from Home Security Checklist

Perimeter security is dead. With data being accessed from unknown locations on untrusted devices, new risks are at an all-time high. These checklists are meant to highlight the most important tasks to ensure your users, devices, apps, and data are protected. It focuses on hybrid Microsoft O365 and (Azure) Active Directory technologies. It is not meant to be a completely exhaustive list. The guidance is based on common Microsoft licensing, but notes premium features when applicable. Recommendations are gleaned from sources such as Microsoft, CIS, NIST, and Enabling’s own experiences.

# Identities

|  |  |  |
| --- | --- | --- |
| ID | Description | Status |
| 1.0 | Ensure multifactor authentication is enabled for all users in administrative roles  *Minimize the number global admin accounts (2-4 ideal)*  *Ensure an emergency account exists with a 128-character password* |  |
| 1.1 | Enable multifactor authentication is enabled for all users in all roles  *Use the Azure AD Application Proxy to secure on-prem servers with MFA* |  |
| 1.2 | Enable AAD Password Protection to AD to prohibit the use of common passwords. |  |
| 1.3 | Configure Self-Service Password Reset in Azure AD (Premium 1 required) |  |
| 1.4 | Block legacy authentication with Conditional Access policies |  |
| 1.5 | Configure password hash sync (even if using AD FS) |  |
| 1.6 | Enable Identity Protection and review (weekly) for anomalous logins |  |
| 1.7 | Block logins from countries where your org has no legitimate users (AAD P1) |  |

# Devices

|  |  |  |
| --- | --- | --- |
| ID | Description | Status |
| 2.0 | Ensure IT staff and Privileged Users are using dedicated, corporate workstations (or a jumpbox such as Azure Bastion with Just-in-Time access) to perform admin changes in the environment (not personal devices). |  |
| 2.1 | Disable local Admin rights, or restrict potentially unwanted app installation using Defender Application Guard |  |
| 2.2 | Control macros by using Defender Exploit Guard Attack Surface Area Reduction, Controlled Folder Access, and Network Protection rules |  |
| 2.3 | Either disable USB altogether via Intune or protect against malware by scanning removable drives (using Microsoft Defender or similar) |  |
| 2.4 | Use Windows Firewall, Hello for Business, Screen Saver timeouts, and SmartScreen |  |
| 2.5 | Keep machines patched! Ensure proper configuration of Automatic Windows Updates using Intune, Config Manager, or Windows Update Service  *Optimize updates when using Configuration Manager and Cloud Management Gateway* |  |
| 2.6 | Manage mobile devices using Intune MDM or Mobile Device Management (EMS E3 required) |  |
| 2.7 | Use device health and management status (from Defender ATP and Intune) as inputs into Conditional Access and MFA rules |  |
| 2.8 | Use Conditional Access, Cloud App Security, and Intune to control unmanaged device access |  |
| 2.9 | Use Intune application control policies for device-level information protection |  |

# Applications

|  |  |  |
| --- | --- | --- |
| ID | Description | Status |
| 3.0 | Ensure Exchange’s Common Attachment Types Filter is enabled |  |
| 3.1 | Ensure Exchange Online Spam Policies are set to notify an admin when a sender in your tenant has been blocked for sending spam emails |  |
| 3.2 | Config and audit transport rules to prohibit forwarding email to external domains |  |
| 3.3 | Ensure Advanced Threat Protection Safe Links & Attachments are enabled (O365 E5) |  |
| 3.4 | Ensure basic authentication for Exchange Online is disabled |  |
| 3.5 | Configure anti-phishing policies to block impersonation attempts |  |
| 3.6 | Enable SPF, DKIM, and DMARC for all Exchange Online accepted custom domains |  |
| 3.7 | Config Exchange Online Protection to notify admin when internal users are blocked for sending malware |  |
| 3.8 | Audit Teams with external guests and force guests to authenticate with MFA |  |
| 3.9 | Prevent OneDrive syncing to non-domain joined or unmanaged devices |  |

# Data

|  |  |  |
| --- | --- | --- |
| ID | Description | Status |
| 4.1 | Use Office 365 Sensitivity Labels and Data Loss Prevention rules to prevent inappropriate sharing, sending, saving in Exchange, Teams, OneDrive, SharePoint |  |
| 4.2 | Prohibit leakage of work data into personal accounts/apps by using Intune App Protection Policies (EMS E3 required) |  |
| 4.3 | Use Microsoft Cloud App Security (CASB) to secure SaaS applications and ensure security/confidentiality of corporate files. (EMS E5 required) |  |
| 4.4 | Instead of allowing access to company content from personally owned PCs or laptops, use Windows Virtual Desktop to securely publish Win10 and LOB apps |  |
| 4.5 | Use Office 365 retention policies and archiving to preserve data in the event of lost/stolen devices or regulatory requirements |  |

# Networks & Infrastructure

|  |  |  |
| --- | --- | --- |
| ID | Description | Status |
| 5.1 | Use VPN tunnel for on-premises apps, but split the tunnel for Office 365/SaaS traffic |  |
| 5.2 | Use layer 7 firewalls with user-aware policies to inspect traffic after the user connects to VPN. |  |
| 5.3 | Monitor VPN during patch updates. If WSUS updates traverse the VPN/ISP circuit, use smaller group sizes or use Cloud Management Gateway to avoid saturation. |  |
| 5.4 | Block port 3389 (RDP) wherever and whenever possible |  |
| 5.5 | Ensure home network routers are patched and have non-default passwords and WPA2 or WPA3 encryption |  |

# Social Engineering Awareness

|  |  |  |
| --- | --- | --- |
| ID | Description | Status |
| 6.1 | Do not defer system software updates. |  |
| 6.2 | Verify the legitimacy of financial emails, by calling or texting the sender |  |
| 6.3 | Be wary of COVID-19 or other newsworthy emails, which are often phishing |  |
| 6.4 | Report malware or phishing by using Outlook’s report message button |  |
| 6.5 | Don’t allow family to use work machines, and don’t share passwords |  |
| 6.6 | Update acceptable use policies for remote work, and associated risks |  |
| 6.7 | Ensure MailTips are enabled for all users |  |
| 6.8 | Test your employees’ resistance to phishing by regularly simulating attacks |  |