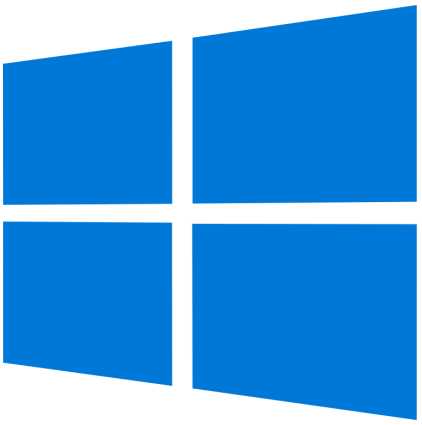
Bayssié Loïc
Bedat Joritz

Sécurité des systèmes d'exploitation
Guide de durcissement Microsoft Windows



Bayssié Loïc
Bedat Joritz

Table des matières

Stratégie compte utilisateur

Établir longueur minimale de mot de passe

Chemin : Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password length

Valeur par défaut : 7 caractères
Valeur recommandée : 14 caractères minimum

Activer la demande de complexité du mot de passe

Chemin : Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Password must meet complexity requirements

Conditions demandées :

- Ne pas utiliser plus de 2 lettres consécutives du nom d'utilisateur
- Au moins 6 caractères de longueur
- Au moins une majuscule
- Au moins une minuscule
- Au moins un caractère spécial (!,$,#,%...)
- Au moins un caractère supplémentaire ne rentrant pas dans les 4 catégories précédentes

Valeur par défaut : Disabled
Valeur recommandée : Enabled

Vérifier la valeur du stockage de mot de passe utilisant un chiffrement réversible

Chemin : Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Store passwords using reversible encryption

Valeur par défaut : Disabled
Valeur recommandée : Disabled

Attribution droits utilisateurs

Autoriser l'accès au réseau aux administrateurs et utilisateurs authentifiés uniquement

Chemin : Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access this computer from the network

Valeur par défaut : *Administrators, Backup Operators, Users, Everyone*
Valeur recommandée : *Administrators, Remote desktop users*

Empêcher les utilisateurs standards d'utiliser "agir en tant que partie du système"

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Act as part of the operating system*

Valeur par défaut : *No one*
Valeur recommandée : *No one*

Autoriser l'ouverture de session local aux Administrateurs uniquement

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on locally*

Valeur par défaut : *Administrators, Backup Users, Guests, Users*
Valeur recommandée : *Administrators, Users*

Refuser le droit "ouvrir une session en tant que service" aux utilisateurs invités et ce, localement ou via RDP

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on through Remote Desktop Services*

Valeur par défaut : *Administrators, Remote Users*

Valeur recommandée : *Administrators, Remote Users*

Paramètres de sécurité utilisateur

S’assurer que le statut de compte Administrateur est désactivé

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Administrator account status*

Valeur par défaut : Disabled
Valeur recommandée : Disabled

S’assurer que le blocage de comptes Microsoft soit paramétré sur ‘Utilisateurs ne pouvant pas ajouter ou se connecter avec un compte Microsoft

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Administrator account status*

Valeur par défaut : *N/o*
Valeur recommandée : *N/o*

S’assurer que le blocage de comptes Microsoft soit paramétré sur ‘Utilisateurs ne pouvant pas ajouter ou se connecter avec un compte Microsoft

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Administrator account status*

Valeur par défaut : *N/o*
Valeur recommandée : *N/o*

S’assurer que le statut de compte Invité est désactivé

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Guest account status*

Valeur par défaut : *Disabled*
Valeur recommandée : *Disabled*

Renommer le compte Administrateur

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename administrator account*

Valeur par défaut : *Administrator*
Valeur recommandée : *N/o*

Renommer le compte Invité

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename administrator account*

Valeur par défaut : *Guest*
Valeur recommandée : *N/o*

Paramètres de journaux d'événements (logs)

Taille max des journaux d'évènements

Chemin : *Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application\Specify the maximum log file size (KB)*

Valeur par défaut : *20,408KB*
Valeur recommandée : *32,768KB ou plus*

Méthode de conversation des journaux

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Log successful connections*

Valeur par défaut : *No*
Valeur recommandée : *Yes*

Contrôle d’accès au réseau

Vérifier la désactivation des demandes de SID par les utilisateurs anonymes

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Allow anonymous SID/Name translation*

Valeur par défaut : *Disabled*
Valeur recommandée : *Disabled*

Vérifier l’interdiction d'énumération des comptes SAM

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts*

Valeur par défaut : *Enabled*
Valeur recommandée : *Enabled*

Vérifier l’interdiction d'énumération anonymes des comptes SAM et les partages

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares*

Valeur par défaut : *Disabled*
Valeur recommandée : *Disabled*

Paramètres de sécurité : réseau

Autoriser “système local” à utiliser l’identité de l’ordinateur pour NTLM

chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow Local System to use computer identity for NTLM*

Valeur par défaut : *Disabled*
Valeur recommandée : *Enabled*

Désactiver recours session Local NULL

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow LocalSystem NULL session fallback*

Valeur par défaut : *Disabled*
Valeur recommandée : *Disabled*

Configurer les types de cryptages autorisés pour Kerberos

chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Configure encryption types allowed for Kerberos*

Valeur par défaut : ***RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1****, Future encryption types.*
Valeur recommandée : ***AES128_HMAC_SHA1, AES256_HMAC_SHA1****, Future encryption types*

Ne pas stocker de valeur de hachage de niveau LAN manager

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Do not store LAN Manager hash value on next password change*

Valeur par défaut : *Enabled*
Valeur recommandée : *Enabled*

Configurer le niveau d'authentification de LAN manager pour autoriser NTLMv2 et refuser LM & NTLM

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: LAN Manager authentication level*

Valeur par défaut : *Send NTLMv2 response only. (Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it; Domain Controllers accept LM, NTLM & NTLMv2 authentication.)*
Valeur recommandée : *NTLMv2 response only. Refuse LM & NTLM.*

Activer pare-feu Windows sur les trois profils

Domaine

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Firewall state*

Valeur par défaut : *On*
Valeur recommandée : *On*

Privé

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Firewall state*

Valeur par défaut : *On*
Valeur recommandée : *On*

Public

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Firewall state*

Valeur par défaut : *On*
Valeur recommandée : *On*

Configurer le pare-feu Windows pour bloquer tout trafic entrant sur les trois profils

Domaine

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Inbound connections*

Valeur par défaut : *Block*
Valeur recommandée : *Block*

Privé

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Inbound connections*

Valeur par défaut : *Block*
Valeur recommandée : *Block*

Public

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Inbound connections*

Valeur par défaut : *Block*
Valeur recommandée : *Block*

Paramètre de sécurité : connexion bureau à distance

Activer l'authentification au niveau du réseau (NLA : Network Level Authentication)

Chemin : *Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Require user authentication for remote connections by using Network Level Authentication*

Valeur par défaut : *Enabled* depuis Windows 8 (compris)
Valeur recommandée : Enabled

Configurer un certificat SSL sur le serveur et forcer l'utilisation de la couche de sécurité « SSL »

Chemin : *Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Require use of specific security layer for remote (RDP) connections*

Valeur par défaut : *Negotiate*
Valeur recommandée : *Enabled*

Toujours demander le mot de passe à la connexion

Chemin : *Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Always prompt for password upon connection*

Valeur par défaut : *Disabled*
Valeur recommandée : *Enabled*

Utiliser le niveau de chiffrement "Élevé" afin de protéger les données RDP à l'aide d'un chiffrement renforcé

Chemin : *Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Set client connection encryption level*

Valeur par défaut : *High Level*
Valeur recommandée : *High Level*

Activer Remote Credential Guard

Chemin : *Computer Configuration\Policies\Administrative Templates\System\Credentials Delegation\Remote host allows delegation of non-exportable credentials*

Valeur par défaut : *Disabled*
Valeur recommandée : *Enabled*

Paramètre de sécurité : Serveur membre domaine AD

Chiffrer ou signer numériquement les données des canaux sécurisés

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally encrypt or sign secure channel data (always)*

Valeur par défaut : *Enabled*
Valeur recommandée : *Enabled*

Chiffrer numériquement les données des canaux sécurisés

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally encrypt secure channel data (when possible)*

Valeur par défaut : *Enabled*
Valeur recommandée : *Enabled*

Signer numériquement les données des canaux sécurisés

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally sign secure channel data (when possible)*

Valeur par défaut : *Enabled*
Valeur recommandée : *Enabled*

Exiger des clés de session fortes

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Require strong (Windows 2000 or later) session key*

Valeur par défaut : *Enabled*
Valeur recommandée : *Enabled*

Stratégie Audit

Auditer la gestion des comptes utilisateur

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit User Account Management*

Valeur par défaut : *Success*
Valeur recommandée : *Success and Failure*

Auditer les ouvertures et fermetures de sessions

Logoff

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logoff*

Valeur par défaut : *Success*
Valeur recommandée : *Success*

Logon

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logon*

Valeur par défaut : *Success*
Valeur recommandée : *Success and Failure*

Auditer les changements de stratégie

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Audit Policy Change*

Valeur par défaut : Success
Valeur recommandée : Success

Auditer les changements de stratégie d'authentification

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Authentication Policy Change*

Valeur par défaut : Success
Valeur recommandée : Success

Auditer l'utilisation des privilèges

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Privilege Use\Audit Sensitive Privilege Use*

Valeur par défaut : *No auditing*
Valeur recommandée : *Success and Failure*

Paramètres de sécurité : OS

Désinstaller ou désactiver les services et fonctionnalités non utilisés

Bluetooth support device (bthserv)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Bluetooth Support Service*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

Computer Browser

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Computer Browser*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

Downloaded Maps Manager (MapsBroker)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Downloaded Maps Manager*

Valeur par défaut : *Automatic*
Valeur recommandée : *Disabled*

Geolocation service (lfsvc)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Geolocation Service*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

IISAdmin Service (IISADMIN)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\IIS Admin Service*

Valeur par default : *Not installed (automatic when installed)*
Valeur recommandée : *Disabled*

Infrared Monitor service (irmon)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Infrared monitor service*

Valeur par défaut : *Manual or Not installed*
Valeur recommandée : *Disabled*

Internet Connection Sharing (SharedAccess)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Internet Connection Sharing (ICS)*

Valeur par défaut : *Manual or Disabled*
Valeur recommandée : *Disabled*

Link-Layer Topology Discovery Mapper (lltdsvc)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Link-Layer Topology Discovery Mapper*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

LxssManager

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\LxssManager*

Valeur par default : *Not installed (manual when installed)*
Valeur recommandée : *Disabled*

Microsoft FTP Service (FTPSVC)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Microsoft FTP Service*

Valeur par default : *Not installed (automatic when installed)*
Valeur recommandée : *Disabled*

Microsoft iSCSI Initiator Service (MSiSCSI)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Microsoft iSCSI Initiator Service*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

OpenSSH SSH Server (sshd)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\OpenSSH SSH Server*

Valeur par default : *Not installed (manual when installed)*
Valeur recommandée : *Disabled*

Peer Name Resolution Protocol (PNRPsvc)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Peer Name Resolution Protocol*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

Peer Networking Grouping (p2psvc)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Peer Networking Grouping*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

Peer Networking Identity Manager (p2pimsvc)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Peer Networking Identity Manager*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

PNRP Machine Name Publication Service (PNRPAutoReg)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\PNRP Machine Name Publication Service*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

Problem Reports and Solutions Control Panel Support (wercplsupport)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Problem Reports and Solutions Control Panel Support*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

Remote Access Auto Connection Manager (RasAuto)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Remote Access Auto Connection Manager*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

Remote Desktop Configuration (SessionEnv)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Remote Desktop Configuration*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

Remote Desktop Services (TermService)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Remote Desktop Services*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

Remote Desktop Services UserMode Port Redirector (UmRdpService)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Remote Desktop Services UserMode Port Redirector*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

Remote Procedure Call (RPC) Locator (RpcLocator)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Remote Procedure Call (RPC) Locator*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

Remote Registry (RemoteRegistry)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Remote Registry*

Valeur par défaut : *Manual or Disabled*
Valeur recommandée : *Disabled*

Routing and Remote Access (RemoteAccess)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Routing and Remote Access*

Valeur par défaut : *Disabled*
Valeur recommandée : *Disabled*

Server (LanmanServer)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Server*

Valeur par défaut : *Automatic*
Valeur recommandée : *Disabled*

Simple TCP/IP Services (simptcp)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Simple TCP/IP Services*

Valeur par défaut : *Not installed*
Valeur recommandée : *Disabled*

SNMP Service

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\SNMP Service*

Valeur par défaut : *Automatic*
Valeur recommandée : *Disabled*

Special Administration Console Helper (sacsvr)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Special Administration Console Helper*

Valeur par défaut : *Disabled*
Valeur recommandée : *Not installed*

SSDP Discovery (SSDPSRV)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\SSDP Discovery*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

UPnP Device Host (upnphost)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\UPnP Device Host*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

Web Management Service (WMSvc)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Web Management Service*

Valeur par défaut : *Not installed (manual when installed)*
Valeur recommandée : *Disabled*

Windows Error Reporting Service (WerSvc)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Windows Error Reporting Service*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

Windows Event Collector (Wecsvc)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Windows Event Collector*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

Windows Media Player Network Sharing Service (WMPNetworkSvc)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Windows Media Player Network Sharing Service*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

Windows Mobile Hotspot Service (icssvc)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Windows Mobile Hotspot Service*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

Windows Push Notifications System Service (WpnService)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Windows Push Notifications System Service*

Valeur par défaut : *Automatic*
Valeur recommandée : *Disabled*

Windows PushToInstall Service (PushToInstall)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Windows PushToInstall Service (PushToInstall)*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

Windows Remote Management (WS-Management) (WinRM)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Windows Remote Management (WS-Management)*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

World Wide Web Publishing Service (W3SVC)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\World Wide Web Publishing Service*

Valeur par défaut : *Automatic*
Valeur recommandée : *Disabled*

Xbox Accessory Management Service (XboxGipSvc)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Xbox Accessory Management Service*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

Xbox Live Auth Manager (XblAuthManager)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Xbox Live Auth Manager*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

Xbox Live Game Save (XblGameSave)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Xbox Live Game Save*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

Xbox Live Networking Service (XboxNetApiSvc)

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Xbox Live Networking Service*

Valeur par défaut : *Manual*
Valeur recommandée : *Disabled*

Fermer tous les ports non utilisés

S'assurer que tous les ports et protocoles non utilisés soient fermés afin de bloquer un éventuel trafic indésirable en laissant fonctionner ceux qui sont essentiels aux besoins de l'entreprise sur chaque système.

Système de fichier « NTFS »

S'assurer que les espaces de stockage soient configurés en système NTFS pour s'assurer des performances, de la fiabilité et une gestion de l'espace disque nécessaire au stockage des données d'entreprise.

Configurer la date & heure système, synchroniser ensuite l'horloge avec un serveur NTP

Chemin : *Computer Configuration\Policies\Administrative Templates\System\Windows Time Service\Time Providers\Enable Windows NTP Client*

Valeur par défaut : *Disabled*
Valeur recommandée : *Enabled*

Activer le chiffrement de lecteur BitLocker

Il est important d'activer et de configurer le chiffrement de certaines partitions avec un outil tel que BitLocker dans le but de protéger les données sensibles et de configurer la récupération de ces dernières en gardant la clé en sûr.

Restreindre au maximum les droits aux utilisateurs du réseau

Restreindre au maximum les droits utilisateurs du réseau permettra de limiter l'impact dans le cadre d'une attaque ou d'une action involontaire de la part d'un utilisateur lambda qui pourrait avoir de terribles conséquences.

Installer et configurer un anti-virus et un anti-spyware

Un anti-virus et un anti-spyware sont également de mise dans le but de prévenir contre d'éventuelles menaces, il est également recommandé de configurer la mise à jour automatique de ces derniers.

Sécurité physique

Ne pas autoriser l'arrêt du système sans avoir ouvert de session Windows

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Shut down the system*

Valeur par défaut : *Administrators, Users.*
Valeur recommandée : *Administrators, Backup Operators, Users.*

S'assurer que 'Boot-Start Driver Initialization Policy' est activé pour vérifier l'ordre de boot des pilotes et périphériques

Chemin : *Computer Configuration\Policies\Administrative Templates\System\Early Launch Antimalware\Boot-Start Driver Initialization Policy*

Valeur par défaut : *Disabled*
Valeur recommandée : *Enabled: Good, unknown and bad but critical*

Configurer un écran de veille après un certain temps d'inactivité

Chemin : *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine inactivity limit*

Valeur par défaut : *0 seconds*
Valeur recommandée : *900 or fewer seconds, but not 0*

Utiliser MBSA

MBSA est un outil d'analyse de vulnérabilités sur les anciens systèmes Windows pouvant encore être en fonctionnement aujourd'hui, il est recommandé de l'utiliser pour scanner les éventuelles vulnérabilités des anciens systèmes utilisés.

Bibliographie

Sources :
CIS Windows Benchmark :
https://www.newnettechnologies.com/downloads/cis/Windows/Windows10/CIS_Microsoft_Windows_10_Enterprise_Release_20H2_Benchmark_v1.10.0.pdf?utm_campaign=CIS%20Controls%20Campaign&utm_medium=email&_hsmi=84139151&_hsenc=p2ANqtz-_qtLikHRMEF22Ikk_t7tuv5OrWS3A46kNvKHl3PlswZ7Ahtz2a0Svfy3uZl0pR-ScXBQO4KoZTpAYhonkkoiRFK3mwhg&utm_content=84139151&utm_source=hs_automation&fbclid=IwAR3InGf6mX2AtWxmMv6Cp94SujIB3eln_pAP1HtSY76wNxcxO8sCOBL3IXg