Sunucu Kurulumu

- Altyapı ekibi tarafından performans, kapasite, güvenlik ve süreklilik ihtiyaçlarına bağlı olarak sunucunun fiziksel veya sanal olacağına karar verilir.
- Sunucu fiziksel ise lokasyonu belirlenir, sanal ise sanallaştırma yazılımı üzerinden sunucu gereksinimleri karşılanır.
- Kritik sunucular canlı ortama alınmadan önce zafiyet tarama araçlarıyla taranmalıdır tespit edilen açıklıklar giderilmelidir. Açıklık giderilmeden sunucunun canlı ortama alınmasına izin verilmemelidir.
- Sunucular fiziksel ve mantıksal olarak ayrıştırılmış ağlarda ve fiziksel güvenliği sağlanmış sistem odalarında kullanım amaçlarına uygun şekilde konumlandırılmalıdır İnternet erişim standartta kapalı tutulup, açık olması gerektiği durumlarda sunucular izole ağlarda konumlandırılmalıdır.
- Sunucunun bağlı olacağı ağ segmenti ve IP adresi belirlendikten sonra sunucunun veri hattı aktif edilir. İç veya Dış DMZ gibi ayrım var ise sadece dış taraf DMZ sunucularına internet çıkış hakkı verilmelidir.

Sunucu Güvenlik Standartları

- Sunucular domaine (etki alanı) alınmalıdır ve domain politikası uygulanmış olmalıdır. İlgili sunucunun kullanım amacına göre ayrı ayrı sıkılaştırma kuralları yazılmalı ve uygulanmalıdır.
- Domain' e alınmaması gereken sunucu var ise Security Baseline ile Local GPO yapılandırılmalıdır.(https://techcommunity.microsoft.com/t5/Microsoft-Security-Baselines/bg-p/Microsoft-Security-Baselines) .
- Kurumca işletim sistemi özelinde uluslararası standartlara uyumlu sıkılaştırma kuralları belirlenmelidir. CIS Baseline veya Microsoft Security Baseline' ları referans alınabilir. Örnek yapılandırmayı EK de bulabilirsiniz.

- Desteği bitmiş hiç bir sunucu veya uygulama yapı içerisinde konumlandırılmamalıdır. Desteği devam eden ve kritik açıklık içermeyen işletim sistemi kurulmalıdır.
- Sunucular üzerinde ortaya çıkabilecek açıklıklar düzenli olarak takip edilmelidir, yayınlanan kritik yamalar şirket politikasına göre en kısa zamanda uygulanmalıdır.
- Yama yönetimi için merkezi araçlar kullanılmalıdır.
- Üçüncü parti yazılımlar içinde merkezi yama yönetim araçları kullanılmalıdır.
- Kullanılmayan servis, fonksiyon ve portlar kaldırılmalı veya pasif hale getirilmelidir.
- Varsayılan olarak gelen kullanıcı hesapları kaldırılmalıdır. Üretici firma tarafından tanımlanmış kullanıcılar, parolalar, portlar ve parametreler kurulum sırasında değiştirilmelidir.
- Kullanıcı yetkilendirmeleri rol ve grup temelli yapılmalıdır.
- Görevler ayrılığı ilkesi keskin şekilde belirlenmelidir.
- Kullanıcılara görev tanımlarıyla uyumlu yetkiler verilmelidir.
- Kullanıcı hesapları kişiye özeldir. Paylaşımlı/ortak hesap kullanılmaz. Ortak kullanıma sebebiyet verecek "Administrator" ve "Root" benzeri kullanıcı isimleri değiştirilmelidir. Söz konusu kullanıcıların şifreleri değiştirilmeli(LAPS kullanılabilir) ve kontrolsüz ifşa olmasını engelleyecek şekilde güvenlik altında tutulmalıdır.
- Sunucu üzerinde çalışan servisler, uyarı ve hata mesajlarında sunucu ve işletim sistemi çeşidi ve versiyonunu paylaşmayacak şekilde yapılandırılmalıdır.
- Sunucu üzerinde çalışan servisler ihtiyaç duyulan minimum yetkiye sahip kullanıcı hesaplarıyla çalıştırılırmalıır. Servisler ihtiyaç duyulmadıkça yönetici yetkileriyle çalıştırılmamalıdır. İmkan var ise bu tarz işlemler PAM çözümleri ile yapılmalıdır. Örn: Cyberark
- Sunuculara erişim güvenli iletişim kanallarıyla gerçekleştirilmelidir. Yapıda Tiering modeli uygulanmalıdır. Sunucu erişimleri PAM araçları ile yapılmalıdır.
- Yetkili kullanıcılar için yeterli seviyede yetki(Just Enough Administrarion) verilmelidir.
- Kritik sunuculara erişim çift katmanlı erişim ile sağlanmalıdır.
- Erişilecek sunucu Active Directory ise erişimler sadece PAW makinaları üzerinden yapılmalıdır. (https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations)
- Sunucu erişim logları aktif olmalı ve sunucu kapasitesine göre düzenli olarak yedeklenmelidir. Loglar merkezi log sunucusunda gönderilmeli ve asgari olarak 6 ay online erişilebilecek şekilde minimum 1 veya 2 sene saklanmalıdır.(Yasal mevzuat göz önünde bulundurulmalıdır)
- SIEM uygulaması üzerinde alarm tanımlamaları yapılandırılmalı ve kurallar sürekli güncel durumlara göre gözden geçirilip düzenlenmelidir, şüpheli aktivitelere ilişkin üretilen alarmlar ilgili ekipler tarafından kontrol edilmelidir.
- Sunucuların performansı, kaynak kullanımı düzenli olarak NOC, Monitoring ekipleri tarafından takip edilmelidir.

- Sunucular üzerinde yapılacak tüm değişiklikler talep yönetim uygulaması üzerinden kayıt altına alınmalıdır Gerekli onayların verilmesi sonrasında ilgili değişiklikler planlı bir şekilde gerçekleştirilmelidir. (Remedy, CA kullanılabilir)
- Sunucular üzerinden yapılan önemli değişiklikler sonrası sunucular zafiyet tarama araçlarıyla taranmalıdır(Nessus,Qualys vb) Açıklık tespit edildiyse açıklıklar kurum politikaları doğrultusunda en kısa sürede giderilmelidir.
- Şirket politikasına göre sunuculara merkezi yönetilen Endpoint çözümü konumlandırılmalıdır. İstisnalar ise Server / Uygulama bazlı yapılmalıdır ve ilgili istisnalar kayıt altına alınmalıdır.
- Sunucu envanteri sağlıklı şekilde tutulmalıdır.
- Yılda en az 1 defa Pentest yapılmalıdır.
- Pentest sonucu bulunan açıklıklar en kısa zamanda giderilmelidir.
- Yetkili personele yılda en az 1 kez olmak üzere farkındalık eğitimi verilmelidir.
- Prosedür düzenli olarak en az yılda 1 kez olmak kaydıyla gözden geçirilmeli ve güncel tehditlere göre güncellenmelidir.

GÜVENLİ SUNUCU KONFİGÜRASYONU PROSEDÜRÜ

1. EKLER

Grup Politika Ayarları	Hd.local
1.1 Account Policies	
1.1.1 Enforce Password History	5 Passwords remembered
1.1.2 Maximum Password Age	42 Days
1.1.3 Minimum Password Age	1 Days
1.1.4 Minimum Password Length	8 Characters
1.1.5 Password must meet complexity requirements	Enabled
1.1.6 Store passwords using reversible encryption	Disabled
1.1.7 Account lockout duration	30 minutes
1.1.8 Account lockout threshold	3 Attempts
1.1.9 Reset account lockout counter after	15 minutes
1.1.10 Enforce user logon restrictions	Enabled
1.1.11 Microsoft network server: Disconnect clients when logon hours expire	Enabled
1.1.12 Maximum tolerance for computer clock synchronization	5 – Domain Controllers only
1.1.13 Maximum lifetime for service ticket	600– Domain Controllers only
1.1.14 Maximum lifetime for user ticket renewal	7 days – Domain Controllers only
1.1.15 Maximum lifetime for user ticket	10 hours – Domain Controllers only
1.2 Audit Policy	
1.2.1 Audit Account Logon Events	Success and Failure
1.2.2 Audit Account Management	Success and Failure
1.2.3 Audit Directory Service Access	<Not Defined>, [Active setting: No Auditing]
1.2.4 Audit Logon Events	Success and Failure
1.2.5 Audit Object Access	Success and Failure
1.2.6 Audit Policy Change	Success and Failure
1.2.7 Audit Privilege Use	Success and Failure
1.2.8 Audit Process Tracking	Failure
1.2.9 Audit System Events	Success and Failure
1.2.10 Audit: Shut down system immediately if unable to log security audits	Disabled

Grup Politika Ayarları	Hd.local
1.2.11 Audit: Force audit policy subcategory settings to override audit policy category settings	Enabled
1.3 Detailed Security Auditing	
1.3.1 Audit Policy: System: IPsec Driver	Success and Failure
1.3.2 Audit Policy: System: Security State Change	Success and Failure
1.3.3 Audit Policy: System: Security System Extension	Success and Failure
1.3.4 Audit Policy: System: System Integrity	Success and Failure
1.3.5 Audit Policy: Logon-Logoff: Logoff	Success
1.3.6 Audit Policy: Logon-Logoff: Logon	Success and Failure
1.3.7 Audit Policy: Logon-Logoff: Special Logon	Success
1.3.8 Audit Policy: Object Access: File System	Failure
1.3.9 Audit Policy: Object Access: Registry	Failure
1.3.10 Audit Policy: Privilege Use: Sensitive Privilege Use	Success and Failure
1.3.11 Audit Policy: Detailed Tracking: Process Creation	Success
1.3.12 Audit Policy: Policy Change: Audit Policy Change	Success and Failure
1.3.13 Audit Policy: Policy Change: Authentication Policy Change	Success
1.3.14 Audit Policy: Account Management: Computer Account Management	Success and Failure
1.3.15 Audit Policy: Account Management: Other Account Management Events	Success and Failure
1.3.16 Audit Policy: Account Management: Security Group Management	Success and Failure
1.3.17 Audit Policy: Account Management: User Account Management	Success and Failure
1.3.18 Audit Policy: DS Access: Directory Service Access	No Auditing
1.3.19 Audit Policy: DS Access: Directory Service Changes	No Auditing
1.3.20 Audit Policy: Account Logon: Credential Validation	Success and Failure
1.4 Event Log	
1.4.1 Application: Maximum Log Size (KB)	81920 Kilobytes
1.4.2 Application: Retain old events	Disabled
1.4.3 Security: Maximum Log Size (KB)	81920 Kilobytes
1.4.4 Security: Retain old events	Disabled
1.4.5 System: Maximum Log Size (KB)	81920 Kilobytes

Grup Politika Ayarları	Hd.local
1.4.6 System: Retain old events	Disabled
Retention Method for application log	when needed
Retention Method for security log	when needed
Retention Method for system log	when needed
1.5 Windows Firewall	
1.6 Windows Update	
1.6.1 Configure Automatic Updates	5 – Allow local admin to choose setting
1.6.2 Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box	Enabled
1.6.3 Reschedule Automatic Updates scheduled installations	Enabled
1.7 User Account Control	
1.7.1 User Account Control: Admin Approval Mode for the Built-in Administrator account	Disabled
1.7.2 User Account Control: Behaviour of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent
1.7.3 User Account Control: Behavior of the elevation prompt for standard users	Automatically deny elevation requests
1.7.4 User Account Control: Detect application installations and prompt for elevation	Enabled
1.7.5 User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled
1.7.6 User Account Control: Run all administrators in Admin Approval Mode	Disabled
1.7.7 User Account Control: Switch to the secure desktop when prompting for elevation	Enabled
1.7.8 User Account Control: Virtualize file and registry write failures to per-user locations	Enabled
1.7.9 User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled
1.8 User Rights	
1.8.1 Access this computer from the network	Administrators, Authenticated Users
1.8.2 Act as part of the operating system	<None>

Grup Politika Ayarları	Hd.local
1.8.3 Adjust memory quotas for a process	Network service Local service system GSR[x][yy]- npa_adjustmemoryquotaforaprocess-sp x -> environment yy -> tenantcode
1.8.4 Back up files and directories	Administrators, Backup Operators, Commvault
1.8.5 Bypass traverse checking	Administrators, Authenticated Users, Backup Operators, Local Service, Network Service
1.8.6 Change the system time	Administrators
1.8.7 Create a pagefile	Administrators
1.8.8 Create a token object	<None>
1.8.9 Create global objects	<Not Defined>, [Active setting: Administrators, Local System, Services]
1.8.10 Create permanent shared objects	<None>
1.8.11 Debug programs	<Not Defined>
1.8.12 Deny access to this computer from the network	Guests
1.8.13 Enable computer and user accounts to be trusted for delegation	<None>
1.8.14 Force shutdown from a remote system	Administrators
1.8.15 Impersonate a client after authentication	Administrators SERVICE
1.8.16 Increase scheduling priority	Administrators
1.8.17 Load and unload device drivers	Administrators
1.8.18 Lock pages in memory	None
1.8.19 Manage auditing and security log	Administrators
1.8.20 Modify firmware environment values	Administrators

Grup Politika Ayarları	Hd.local
1.8.21 Perform volume maintenance tasks	Administrators
1.8.22 Profile single process	Administrators
1.8.23 Profile system performance	Administrators
1.8.24 Remove computer from docking station	None
1.8.25 Replace a process level token	NETWORK SERVICE, LOCAL SERVICE
1.8.26 Shut down the system	Administrators
1.8.27 Add workstations to domain	Administrators, Help Desk
1.8.28 Allow log on locally	Administrators
1.8.29 Allow log on through Remote desktop Services	Administrators, Remote desktop Users
1.8.30 Change the time zone	LOCAL SERVICE, Administrators
1.8.31 Create symbolic links	Administrators
1.8.32 Deny log on locally	gsr[x][yy]-npa_denylogonlocally-sp x -> environment yy -> tenantcode
Deny log on as a batch job	Guests
1.8.33 Deny log on through Terminal Services	gsr[x][yy]-npa_denyrdp x -> environment yy -> tenantcode
1.8.34 Generate security audits	LOCAL SERVICE, NETWORK SERVICE
1.8.35 Increase a process working set	LOCAL SERVICE, Administrators
1.8.36 Log on as a batch job	<Not Defined>
1.8.37 Restore files and directories	Administrators
1.8.38 Take ownership of files or other objects	Administrators
1.8.39 Access credential Manager as a trusted caller	None
1.8.40 Synchronize directory service data	None
1.9 Security Options	
1.9.1 Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require NTLMv2 Session Security, 128-bit Encryption
1.9.2 Network access: Remotely accessible registry paths and sub-paths	CIS Based

Grup Politika Ayarları	Hd.local
1.9.3 Accounts: Rename administrator account	midgard
1.9.4 Accounts: Rename guest account	Disabled
1.9.5 Accounts: Guest account status	Disabled
1.9.6 Network access: Allow anonymous SID/Name translation	Disabled
1.9.7 Accounts: Limit local account use of blank passwords to console logon only	Enabled
1.9.8 Devices: Allowed to format and eject removable media	Administrators
1.9.9 Devices: Prevent users from installing printer drivers	Enabled
1.9.10 Devices: Restrict CD-ROM access to locally logged-on user only	Enabled
1.9.11 Devices: Restrict floppy access to locally logged-on user only	Enabled
1.9.12 Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
1.9.13 Domain member: Digitally encrypt secure channel data (when possible)	Enabled
1.9.14 Domain member: Digitally sign secure channel data (when possible)	Enabled
1.9.15 Domain member: Disable machine account password changes	Disabled
1.9.16 Domain member: Maximum machine account password age	30 days
1.9.17 Domain member: Require strong (Windows 2000 or later) session key	Enabled
1.9.18 Domain controller: Allow server operators to schedule tasks	Not Defined
1.9.19 Domain controller: LDAP server signing requirements	Not Defined
1.9.20 Domain controller: Refuse machine account password changes	Not Defined
1.9.21 Interactive logon: Do not display last user name	Enabled
1.9.22 Interactive logon: Do not require CTRL+ALT+DEL	Disabled
1.9.23 Interactive logon: Number of previous logons to cache (in case domain controller is not available)	0 Logons
1.9.24 Interactive logon: Prompt user to change password before expiration	14 days
1.9.25 Interactive logon: Require Domain Controller authentication to unlock workstation	Enabled
1.9.26 Interactive logon: Smart card removal behaviour	Lock Workstation

Grup Politika Ayarları	Hd.local
1.9.27 Interactive logon: Message text for users attempting to log on	This system is for the use of authorized users only. Users may also be monitored. Users of this system expressly consent to such monitoring and are advised that if such monitoring reveals possible criminal activity, security staff may provide the evidence of such monitoring to law enforcement officials.
1.9.28 Interactive logon: Message title for users attempting to log on	Security Warning
1.9.29 Interactive logon: Require smart card	Not Defined
1.9.30 Microsoft network client: Digitally sign communications (always)	Enabled
1.9.31 Microsoft network client: Digitally sign communications (if server agrees)	Enabled
1.9.32 Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
1.9.33 Microsoft network server: Amount of idle time required before suspending session	10 minutes
1.9.34 Microsoft network server: Digitally sign communications (always)	Disabled (For Member Servers) Enabled (For DC)
1.9.35 Microsoft network server: Digitally sign communications (if client agrees)	Enabled (DC Only)
1.9.36 Microsoft network server: Disconnect clients when logon hours expire	Enabled
1.9.37 Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
1.9.38 Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled
1.9.39 Network access: Do not allow storage of credentials or .NET Passports for network authentication	Enabled
1.9.40 Network access: Let Everyone permissions apply to anonymous users	Disabled
1.9.41 Network access: Named Pipes that can be accessed anonymously	None

Grup Politika Ayarları	Hd.local
1.9.42 Network access: Remotely accessible registry paths	System\CurrentControlSet\Control\Product Options System\CurrentControlSet\Control\Server Applications Software\Microsoft\WindowsNT\CurrentVersion
1.9.43 Network access: Restrict anonymous access to Named Pipes and Shares	Enabled
1.9.44 Network access: Shares that can be accessed anonymously	None
1.9.45 Network access: Sharing and security model for local accounts	Classic
1.9.46 Network security: Do not store LAN Manager hash value on next password change	Enabled
1.9.47 Network security: LAN Manager authentication level	Send NTLMv2, refuse LM
1.9.48 Network security: LDAP client signing requirements	Negotiate signing
1.9.49 Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require NTLMv2 Session Security, 128-bit Encryption
1.9.50 Recovery console: Allow automatic administrative logon	Disabled
1.9.51 Recovery console: Allow floppy copy and access to all drives and all folders	Disabled
1.9.52 Shutdown: Clear virtual memory pagefile	Disabled
1.9.53 Shutdown: Allow system to be shut down without having to log on	Disabled
1.9.54 System objects: Require case insensitivity for non-Windows subsystems	Enabled
1.9.55 System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled
1.9.56 System cryptography: Force strong key protection for user keys stored on the computer	User must enter a password each time they use a key
1.9.57 System settings: Optional subsystems	None
1.9.58 System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Disabled
1.10 Terminal Services	
1.10.1 Always prompt client for password upon connection	Enabled

Grup Politika Ayarları	Hd.local
1.10.2 Set client connection encryption level	Enabled: Client Compatible
1.10.3 Do not allow drive redirection	Enabled
1.10.4 Do not allow passwords to be saved	Enabled
1.11 Internet Communication	
1.11.1 Turn off downloading of print drivers over HTTP	Enabled
1.11.2 Turn off the "Publish to Web" task for files and folders	Enabled
1.11.3 Turn off Internet download for Web publishing and online ordering wizards	Enabled
1.11.4 Turn off printing over HTTP	Enabled
1.11.5 Turn off Search Companion content file updates	Enabled
1.11.6 Turn off the Windows Messenger Customer Experience Improvement Program	Enabled
1.11.7 Turn off Windows Update device driver searching	Enabled
1.12 Additional Security Settings	
1.12.1 Do not process the legacy run list	Enabled
1.12.2 Do not process the run once list	Enabled
1.12.3 Registry policy processing	Enabled
1.12.4 Offer Remote Assistance	Disabled
1.12.5 Solicited Remote Assistance	Disabled
1.12.6 Restrictions for Unauthenticated RPC clients	Enabled: Authenticated
1.12.7 RPC Endpoint Mapper Client Authentication	Enabled
1.12.8 Turn off Autoplay	Enabled: All drives
1.12.9 Enumerate administrator accounts on elevation	Disabled
1.12.10 Require trusted path for credential entry	Enabled
1.12.11 Disable remote Desktop Sharing	Enabled

Not : İlgili kurallar şirket yapısına göre düzenlenmelidir. Referans olarak CIS Baseline veya Microsoft Baseline ları alınabilir.

Saygılarımla

Hasan DİMDİK

Cloud and Datacenter MVP