

WINDOWS 2000/XP İŞLETİM SİSTEMLERİ İÇİN GÜVENLİK STANDARTLARI (SECURITY BASELINE) BELGESİ v1.0

Bu belge, ODTÜ yerleşkesinde ağ omurgasına bağlı bilgisayarlarda Windows 2000 ve XP işletim sistemlerinin kurulumu ve güvenlik ayarları ile ilgili bilgileri ve önerileri içermektedir. Kurulum ve ayarların bu belgede önerilenlere göre yapılması, belgenin çoğaltılarak personele dağıtılması ve personelin konunun önemi hakkında bilgilendirilmesi, gerek personelin bilgisayarlarında barındırdığı özel ya da üniversiteye ait bilgilerin güvenliğinin sağlanması, gerekse yerleşke ağ omurgasının sağlıklı işletilebilmesi açısından önem taşımaktadır.

ODTÜ Bilgi İşlem Daire Başkanlığı
Bilişim Teknolojileri Güvenliği Ekibi

Hazırlayanlar: İbrahim Çalışır, Cengiz Acartürk
security@metu.edu.tr
<http://guvenlik.metu.edu.tr>, <http://antivirus.metu.edu.tr>

Ekim 2003

İçindekiler:

BIOS şifresi aktif hale getirilmelidir.....	3
Bilgisayar açılış işlemi kesinlikle sabit diskten yapılmalıdır	3
Disk yapılandırması NTFS olmalıdır.....	3
İşletim sistemi güncellemeleri yapılmalıdır	3
Parola kullanılmalıdır	4
Antivirüs yazılımı kurulmalı ve güncel tutulmalıdır	4
Diskteki bilgiler düzenli olarak yedeklenmelidir	4
Günlük dosyası poliçeleri (Audit policy) belirlenmelidir.....	5
Kullanıcı hesabı poliçeleri (Account policy) belirlenmelidir	6
Security Options altındaki poliçeler belirlenmelidir.....	7
Gereksiz servisler kapatılmalıdır.....	8
Kullanıcı hakları düzenlenmelidir	10
Kayıt dosyasında (Registry) gerekli ayarlar yapılmalıdır	13
Kaynaklar.....	14

BIOS şifresi aktif hale getirilmelidir

Bilgisayarın BIOS ayarları genellikle son kullanıcıların kullanmadığı ayarlardır. Bilgisayar açılırken DEL ya da F1 tuşuna basılarak erişilebilir. Erişimin parolalı hale getirilmesi bilgisayarın fiziksel güvenliği açısından önemlidir. Bu işlem BIOS menülerinden yapılabilir. BIOS sık kullanılmadığından şifresinin unutulması olasıdır, şifrenin güvenli bir yere not edilmesi faydalı olabilir.

Bilgisayar açılış işlemi kesinlikle sabit diskten yapılmalıdır

Açılış işleminin sadece sabit diskten yapılabiliyor olması kötü niyetli bir kişinin bilgisayarı diskette ya da CD ile açmasını ve içindeki verileri, parolaları ele geçirmesini engellemek amacıyla alınacak ilk önlemdir. Bu ayar bilgisayarın BIOS'u kullanılarak yapılır. BIOS menüsünde genellikle "Startup Options" ya da "Startup Devices" bölümünde sadece HDD seçilir.

Disk yapılandırması NTFS olmalıdır

Kullanıcıların erişim haklarının kısıtlanması gereken durumlarda FAT32 dosya sistemi yeterli olmamaktadır. Kullanıcıların %system, %windows gibi, sistem dosyalarının bulunduğu dizinlere erişim hakları NTFS dosya sistemi kullanan Windows 2000/XP işletim sistemlerinde kısıtlanabilmektedir. Bu nedenle işletim sistemi kurulumu sırasında dosya sisteminin NTFS olarak seçilmesine özen gösterilmelidir.

İşletim sistemi güncellemeleri yapılmalıdır

Virüslerin çoğu, işletim sistemi ve üzerinde kurulu yazılımların açıklarından faydalanarak bilgisayarları etkilemektedir. Bu açıklara karşı işletim sistemi üreticileri güncellemeler yayınlamaktadır. Bu güncellemelerin yayınlandıktan sonra en kısa zamanda yapılması önem taşımaktadır.

Microsoft Windows işletim sistemleri için firma belirli aralıklarla Service Pack dosyaları çıkarmaktadır. Bu dosyalar hacim olarak büyük olup, işletim sisteminin piyasaya sürüldüğü tarihten Service Pack dosyasının kullanıma sunulduğu tarihe kadar olan bütün güncellemeleri içerir. Önerimiz, işletim sistemi kurulumundan sonra öncelikle Service Pack dosyalarının kurulmasıdır. Bu dosyalara ODTU FTP arşivinden erişilebilmektedir. (<ftp://ftp.metu.edu.tr/popular/Microsoft>)

Bununla birlikte, Service Pack dosyaları işletim sistemindeki güvenlik açıklarının tamamını kapatmaz. Service Pack dosyasının yazıldığı tarihten sonraki güvenlik açıklarını kapatmak için Windowsupdate web sitesine (<http://www.windowsupdate.com>) bağlanarak bilgisayarı güvenlik açıklarına karşı kontrol ettirmek ve öncelikle kritik güncellemeleri indirerek kurmak gerekmektedir.

Windows XP işletim sistemlerinde işletim sistemi güncellemelerinin otomatik olarak yapılması güncellemelerin sürekliliğinin sağlanması açısından önem taşımaktadır. Güncellemeler, My Computer → Properties → Automatic Updates altından otomatik hale getirilebilmektedir.

Parola kullanılmalıdır

İşletim sistemi tek bir kullanıcı tarafından kullanılsa bile bu kullanıcıya ait bir parola ile işletim sistemine erişilmesi bilgisayardaki verilerin korunması açısından önem taşımaktadır. Bunun yanında bilgisayarın fiziksel güvenliğinin sağlanabilmesi amacıyla ekran koruyucuların parola olarak kullanılması önerilmektedir.

Antivirüs yazılımı kurulmalı ve güncel tutulmalıdır

Virüslerin bilgisayarı etkilemesine karşı alınacak en etkili önlem antivirüs yazılımının kurulması ve güncellenmesidir. Tanımlarına sahip olduğu virüsleri fark edebildiği için antivirüs yazılımının güncellenmesini yapmak, yazılımı kurmak kadar önemlidir.

2003 yılı itibarı ile ODTÜ yerleşkesinde lisanslı olarak kullanılacak antivirüs yazılımı McAfee VirusScan'dir. Bunun dışında ücretli olarak sunulan antivirüs yazılımları için lisans satın alınmadığından lisanssız yazılımların kullanılmaması gerekmektedir. McAfee VirusScan yazılımı ODTÜ lisanslı yazılımları FTP sitesinden (<ftp://ftp.cc.metu.edu.tr>) indirilebilmekte, güncellemeleri ODTÜ FTP arşivinden (<ftp://ftp.metu.edu.tr/virus-updates/mcafee>) yapılabilmektedir. McAfee VirusScan yazılımı hakkındaki bilgilere ODTÜ Antivirüs web sitesinden (<http://antivirus.metu.edu.tr>) ulaşılabilir. McAfee Antivirüs yazılımı güncellemeleri, ODTÜ FTP arşivi dizini üzerinden otomatik olarak yapılabilir.

Diskteki bilgiler düzenli olarak yedeklenmelidir

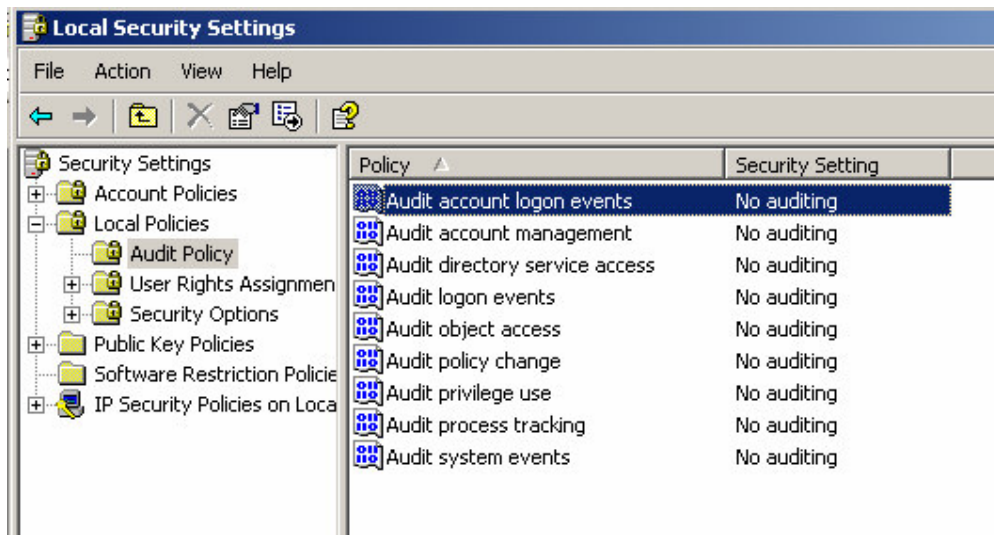
Diskteki dosyaların düzenli olarak yedeğinin alınması çok önemlidir. Bilgilerin diğer kullanıcılar tarafından ele geçirilmesi, değiştirilmesinden diskin yanmasına kadar çok sayıda risk bulunmaktadır. Yedekleme ortamı aynı disk üzerinde bulunmamalıdır. İkinci bir disk yedekleme amacıyla kullanılabilir gibi önerilen yöntem yedeklerin CD ya da ZipDrive gibi farklı ortamlara alınmasıdır. Önemli ve küçük boyutlu dosyalar merkezi sunucu sistemler üzerindeki kullanıcı

hesaplarında, personel kullanıcı hesapları için tanımlanan (2003 yılı itibarı ile) 25 MB'lik kota gözönünde bulundurularak saklanabilir. Merkezi sunucu sistemler üzerinde 24 saatte bir yedek alınmakta, 6 ay önceki yedeklere kadar ulaşılabilir.

Günlük dosyası poliçeleri (Audit policy) belirlenmelidir

Günlük dosyası poliçeleri, Microsoft Windows 2000/XP işletim sisteminin, izlenmesine izin verilen güvenlik olaylarını kayıt etmesini sağlar. Bu ayarlara Start Menu → Settings → Control Panel → Administrative Tools → Local Security Policy → Local Policies → Audit Policy altından ulaşılabilir. Kurulumdan sonra varsayılan değer “No auditing” olacaktır. Poliçeler çift tıklanarak “Success” ve “Failure” olarak değiştirilebilir.

Verilen tablodaki bilgiler yetersiz olduğu durumda arama motorlarında (Google öneriyoruz: <http://www.google.com.tr>) poliçe adı (örneğin “Audit account logon events”) aratıldığında genellikle ilk sırada çıkan Microsoft Technet bağlantısı tıklanarak detaylı bilgiye erişilebilir.



Audit Policy	Önerilen	Açıklama
Audit Account Logon Events	Success ve Failure	DC (Domain Controller) olarak kullanılan bilgisayarlarda domain'e bağlı kullanıcıların, masaüstü bilgisayarlarda yerel kullanıcıların diğer bilgisayarlardan sisteme giriş bilgilerini kaydeder.
Audit Account Management	Success ve Failure	Kullanıcı hesapları ile ilgili işlemleri kaydeder (yaratma, değiştirme, silme).
Audit Directory Service Access	No Auditing	AD (Active Directory) nesnelere erişimleri kaydeder.
Audit Logon Events	Success ve Failure	Kullanıcıların sisteme giriş çıkış bilgilerini kaydeder.
Audit Object Access	Failure	Kullanıcıların sistem üzerindeki nesnelere (dosyalar, dizinler vb.) erişim kayıtlarını tutar. Kayıt dosyası boyutunu hızlı artırdığından sadece başarısız girişimlerin (Failure) kaydının tutulması önerilmektedir.
Audit Policy Change	Success ve Failure	Poliçe değişiklikleri ilgili işlemleri kaydeder.
Audit Privilege Use	Failure	Kullanıcılar kendilerine verilen haklar dışında işlem yapmaya çalıştıklarında kayıt tutar.

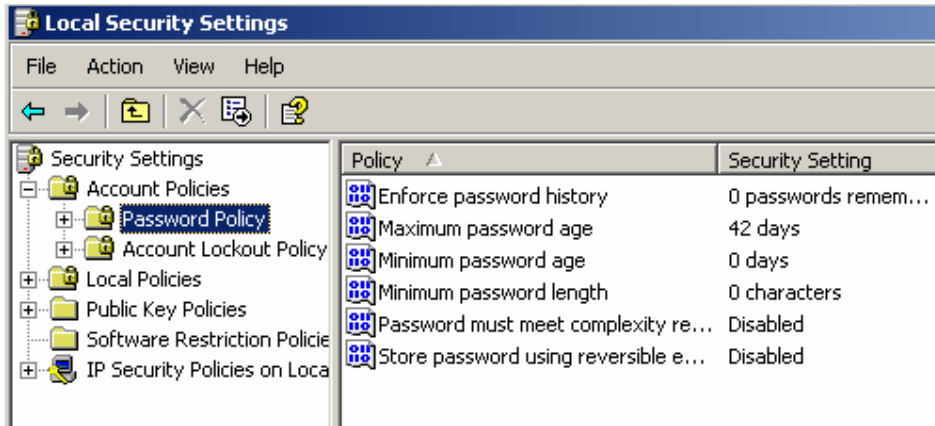
Audit Process Tracking	No Auditing	Her uygulama başlatıldığında ve durdurulduğunda kayıt tutar. Kayıt dosyasının boyutunu hızlı artırdığından sadece başarısız girişimlerin (Failure) kaydının tutulması önerilmektedir.
Audit System Events	Success ve Failure	Sistem ile ilgi işlemleri kaydeder (kapanma,açılma, vb).

Kullanıcı hesabı poliçeleri (Account policy) belirlenmelidir

İşletim sistemi üzerinde tanımlı kullanıcı hesapları ile ilgili poliçelere Start Menu → Settings → Control Panel → Administrative Tools → Local Security Policy → Account Policies altında ulaşılabilir. Kurulumdan sonra varsayılan değerlerin aşağıdaki tabloda tanımlandığı üzere değiştirilmesi önerilmektedir. Poliçeler çift tıklanarak değiştirilebilmektedir.

Kullanıcı hesabı poliçeleri “Password Policy” ve “Account Lockout Policy” olarak ikiye ayrılır. “Password Policy” kullanıcının parolayı seçiminin ve kullanımının sistem yöneticisinin belirlediği kriterlere uygun olmasını sağlar. “Account Lockout Policy” kullanıcı hesabının parolasının deneme yoluyla tahmin edilmeye çalışılması durumunda sistemin alacağı önlemleri içermektedir.

Günlük dosyası poliçelerinde olduğu gibi, verilen tablodaki bilgiler yetersiz olduğu durumda arama motorlarında (Google öneriyoruz: <http://www.google.com.tr>) poliçe adı (örneğin “Enforce password history”) aratıldığında genellikle ilk sırada çıkan Microsoft Technet bağlantısı tıklanarak detaylı bilgiye erişilebilir.



Password Policy	Önerilen	Açıklama
Enforce Password History	24 Remembered	Kullanıcın seçtiği parolaların daha önce seçtiği kaç paroladan farklı olacağını belirten sayıdır.
Minimum Password Age	1 Day	Kullanıcı hesabının açılmasının ardından kullanıcının yeni parolayı değiştirmesi için tanınan süredir.
Maximum Password Age	90 Days	Kullanıcının parolasını değiştirmeden kullanabileceği süredir.
Minimum Password Length	8 Characters	Kullanıcının seçebileceği en kısa parola karakter sayısıdır.
Password Complexity	Required	Kullanıcının seçebileceği parolanın özel karakterler, sayılar, büyük harfler ve küçük

		harflerden oluşan dört gruptan en az üçünü içinde bulundurması zorunluluğunu tanımlar.
Store Password using reversible encryption	Disabled	Kullanıcının parolasının düz metin olarak, şifrelenmeden tutulmasını sağlar. "Disabled" seçeneği bunu engeller.
Account Lockout Policy	Önerilen	Açıklama
Account Lockout Duration	60 minutes	Kullanıcının parolası deneme yoluyla bulunmaya çalışıldığında hesabın ne kadar kapalı kalacağını belirler.
Account Lockout Treshold	5 Bad Login Attempts	Kullanıcının parolası deneme yoluyla bulunmaya çalışıldığında hesabın kaçınıcı denemeden sonra kapatılacağını belirler.
Reset Account Lockout After	60 minutes	Kullanıcının parolası deneme yoluyla bulunmaya çalışıldığında hesaba ne kadar zaman içinde belirtilen sayıda yanlış parola denemesi yapılabileceğini belirleyen süredir.

Security Options altındaki poliçeler belirlenmelidir

Security Options altındaki ayarlar Windows 2000 ve XP işletim sistemlerinde farklılık gösterebilir (örneğin Windows 2000'de "Allow Server Operators to Shedule Task" adındaki poliçe Windows XP'de "Domain Controller: Allow Server Operators to Shedule Task" adıyla tanımlanmaktadır), bazı poliçeler sadece Windows 2000, bazıları sadece Windows XP'de bulunabilir. Bu ayarlara Start Menu → Settings → Control Panel → Administrative Tools → Local Security Policy → Local Policies → Security Options altından ulaşılabilir. Aşağıdaki tabloda poliçelerin hepsi açıklanmamış, sadece kurulumdan sonra değiştirilmesi önerilen poliçelere yer verilmiştir.

Aşağıdaki tabloda poliçeler için ayrıntılı açıklama yapılmamıştır, sunucu ve masaüstü bilgisayarlar için önerilen değerler verilmiştir. Yukarıda bahsedilen poliçelerde olduğu gibi, arama motorlarında (Google öneriyoruz: <http://www.google.com.tr>) poliçe adı (örneğin "Allow Server Operators to Shedule Task") aratıldığında genellikle ilk sırada çıkan Microsoft Technet bağlantısı tıklanarak detaylı bilgiye erişilebilir.

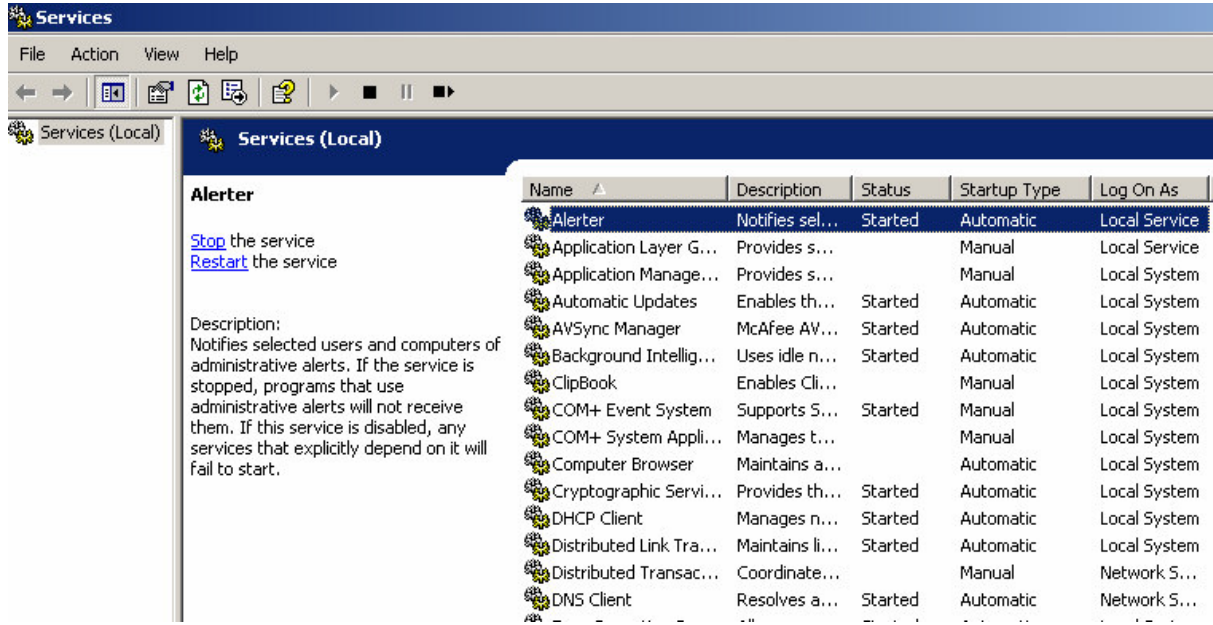
Security Options	Sunucu	Masaüstü
Allow Server Operators to Shedule Task	Administrator	Not defined
Allow System to be Shut Down Without Having to Log On	Disable	Disable
Amount of Idle Time Required Before Disconnecting Session	Not defined	15 dakika
Disable CTRL-ALT-DEL Requirement for Logon	Disable	Disable
Do Not Display Last User Name in Logon Screen	Enabled	Enabled
Lan Manager Authentication Level	Send LM & NTLM – Use NTLMv2 session security if negotiated	Send LM & NTLM – Use NTLMv2 session security if negotiated
Message Txt for Users Attempting to Log On		
Message Title for Users Attempting to Log On		Örnek: Dikkat! Bu izlenen bir bilgisayardır
Number of Previus Logons on Cache	Not defined	0
Prevent System Maintenance of Computer Account Password	Not defined	Not defined

Prevent User to Change Password Before Expiration	Not defined	Not defined
Recovery Console: Allow Floppy Copy and Access to All Drivers and All Folders	Disable	Disable
Rename Administrative Account	“Administrator” dışında herhangi bir değer	“Administrator” dışında herhangi bir değer
Rename Guest Account	“Guest” dışında herhangi bir değer	“Guest” dışında herhangi bir değer
Restrict CD-ROM Access to Locolly Logged-on Users Only	Enable	Enable
Restrict Floppy Access to Locally Logged-on Users Only	Enable	Enable
Secure Channel: Digitally Encrypted or Sign Secure Channel Data (Always)(When Possible)	Enable	Enable
Secure Channel: Require Strong (windows 2000 ve sonrasında) Session Key	Enable	Enable
Send Unencrypted Password to Connect to Third-Party SMB Servers	Ağda Samba sunucusu yoksa Disable	Ağda Samba sunucusu yoksa Disable
Shut Down System Immediately If Unable to Log Security Audits	Enable	Enable
SmartCard Removal Behavior	SmartCard yoksa No Action	SmartCard yoksa No Action
Strengthen Default Permissions of Global System Object	Enable	Enable
Unsigned Driver Installation Behavior: (Warn, but allow install)	Warn, but allow install	Warn, but allow install
Unsigned Non-Driver Installation Behavior: (Warn, but allow install)	Warn, but allow install	Warn, but allow install

Gereksiz servisler kapatılmalıdır

Bu kısımda genellikle masaüstü bilgisayarlarda kullanılmaması önerilen servisler anlatılmaktadır. Bu ayarlara Start Menu → Settings → Control Panel → Administrative Tools → Services altından erişilebilmektedir. Servislerin fonksiyonları ile ilgili bilgiler “Description” başlığı altından görülebilir.

Çalışan servislerin kapatılması özellikle ağ üzerindeki erişimleri engelleyebileceğinden kapatılan servislerin not edilmesinde fayda vardır. Sorun yaşandığında servisler tekrar çalıştırılarak sorunun kaynağı bulunabilir.



Alerter: Seçilen bilgisayarı ve kullanıcılara işletim sisteminin yönetimi ile ilgili mesajları gönderen servistir. Messenger servisi ile birlikte çalışmaktadır. Messenger servisinin güvenlik açıkları nedeniyle kapatılması önerilmektedir.

Clipbook: “Clipboard” üzerindeki (bilginin geçici olarak yüklendiği bellek alanı) bilgilerin ağ üzerinden paylaşılmasını sağlayan servistir. Kesinlikle kapatılması önerilmektedir.

Computer Browsing Service: Ağ komşuları altından ağdaki bilgisayarların ve paylaştıkları bilgilerin görüntülenmesini sağlayan servistir. Kapatıldığı zaman kullanıcının ilgili paylaşımın kaynağını bilmesi ve Windows Explorer penceresinden yazarak ulaşması gerekmektedir (örnek: \\144.122.xxx.xxx\paylas). Windows işletim sistemi üzerinden dosya paylaşımı, güvenlik açıklarına neden olduğu ve bilgisayar bu paylaşımlar üzerinden gelen virüslerden kolayca etkilendiği için kapatılması önerilmektedir. Dosya paylaşımının UNIX tabanlı merkezi sunucu sistemleri (Beluga, Orca, Rorqual, Narwhal) üzerinde tanımlı kullanıcı hesapları kullanılarak, SSH/SFTP ile yapılması önerilmektedir.

Fax Service: Faks almayı sağlayan servistir. Kullanılmıyorsa kapatılması önerilmektedir.

FTP Publishing Service: Microsoft IIS (Internet Information Service) web sunucusu paketi içinde bulunan bir servistir. Varsayılan olarak yüklenmez. Masaüstü bilgisayarların, dosya paylaşımını IIS’in kullandığı bir FTP sunucusundan yapması kesinlikle önerilmemektedir.

IIS Admin Service: Microsoft IIS web servisi sunucusuna uzaktan erişim sağlar. Masaüstü bilgisayarlarda bulunmaması gereken bir servistir. Web sunucusu olarak, çok sayıda güvenlik açığı içeren ve virüslerin öncelikli hedefi olan Microsoft IIS yerine Linux üzerinde çalışan Apache web sunucusunun kullanılması önerilmektedir.

Internet Connection Sharing: İnternet’e bağlı bilgisayarın ağ geçidi (gateway) olarak çalışmasını sağlayan servistir. Yerleşkimizde gerçek IP kullanımı önerilmektedir. Bu servis sınırlı sayıda IP sahibi olan İnternet Cafe vb. mekanlarda kullanılmaktadır.

Messenger: Alerter servisi ile birlikte çalışan, mesajları ağ üzerinde belirlenen diğer bilgisayarlara gönderen servistir. Güvenlik açıkları nedeniyle kapatılması önerilmektedir.

NetMeeting Remote Desktop Sharing: Sistem yöneticileri tarafından kullanıcı bilgisayarlarına doğrudan erişim sağlamak amacıyla kullanılan servistir. Kullanılmıyorsa kapatılması önerilmektedir.

Routing and Remote Access: Bir ağdaki bilgisayarın başka bir ağdaki bilgisayara erişmesine yardımcı olan ya da uzaktan erişim sunucusu olarak kullanılacak bilgisayarda çalışan servistir. Masaüstü bilgisayarlarda kullancılardan ihtiyacı yoktur, kapatılması önerilmektedir.

Simple Mail Transfer Protocol (SMTP): Masaüstü bilgisayarların e-posta sunucusu olarak kullanılmasını sağlayan servistir. IIS paketi ile gelen bu özellik, güvenlik açıkları nedeniyle kapatılmalı hatta tamamen kaldırılmalıdır. E-posta servisi için merkezi sunucu sistemlerimiz kullanılabilir (Sunucu sistemler üzerinde Pine, Mutt ya da <http://webmail.metu.edu.tr>), kullanıcılarımızın kendi e-posta sunucularını kurmalarını önerilmektedir.

Simple Network Management Protocol (SNMP) Service: Ağ üzerindeki cihazların uzaktan erişim ile yönetilmesini sağlayan protokoldür. Son zamanlarda çıkan güvenlik açıkları nedeniyle kullanılmıyorsa kapatılması önerilmektedir.

Simple Network Management Protocol (SNMP) Trap: SNMP servisinin iletişim kuracağı cihazda çalışması gereken servistir. Kullanılmıyorsa kapatılması önerilmektedir.

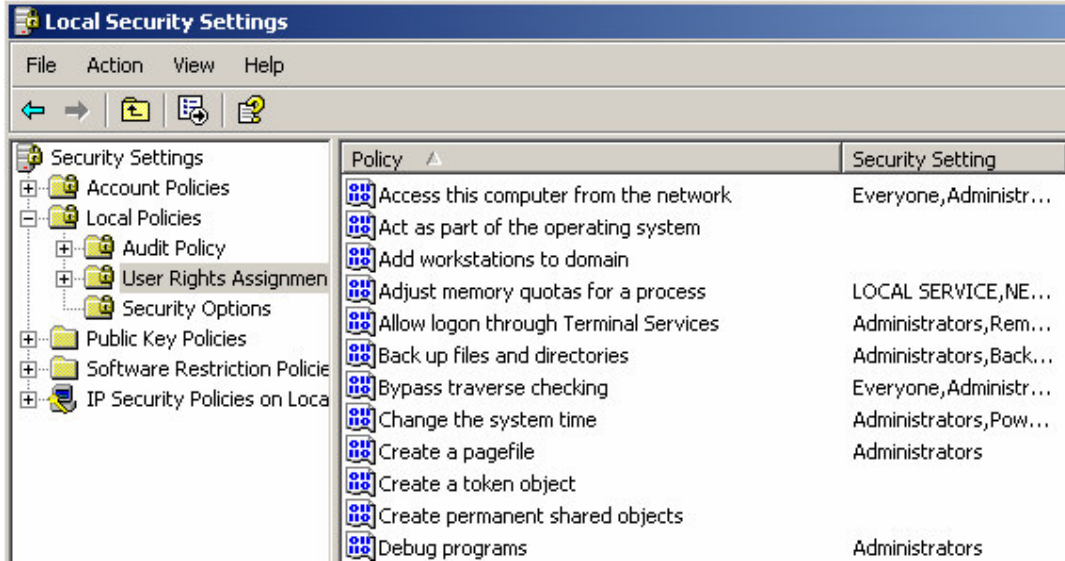
Telnet: Genelde masaüstü bilgisayarlarda varsayılan olarak çalışır durumda olmayan bu servis ağ cihazlarının komut satırından uzaktan yönetilmesini sağlamaktadır. Kullanıcı adı ve parola ikilisini ve diğer bilgileri ağ üzerinde şifrelemeden iletmesi nedeniyle kesinlikle kullanılmaması önerilmektedir.

World Wide Web Publishing Service: En çok saldırıya uğrayan ve en çok güvenlik açığı olan Microsoft servisidir. Varsayılan olarak çalışır durumda olmayan servisin masaüstü bilgisayarlardan tamamen kaldırılması önerilmektedir. Sunucu nitelikli bilgisayarlarda ise Linux üzerinde çalışan Apache gibi daha gelişmiş web sunucuları önerilmektedir.

Kullanıcı hakları düzenlenmelidir

İşletim sistemi üzerinde tanımlı kullanıcı hesaplarının ve gruplarının bilgisayara erişim yetkilerini tanımlayan bu poliçelere Start Menu → Settings → Control Panel → Administrative Tools → Local Security Policy → Local Policies → User Rights Assignment altından ulaşılabilmektedir. Kurulumdan sonra varsayılan değerlerin aşağıdaki tabloda tanımlandığı üzere değiştirilmesi önerilmektedir. Poliçeler çift tıklanarak değiştirilebilmektedir. Bilgisayarın ağdaki rolüne göre farklı değerlerde haklar önerilmektedir.

Aşağıdaki tabloda poliçeler için ayrıntılı açıklama yapılmamıştır, sunucu ve masaüstü bilgisayarlar için önerilen değerler verilmiştir. Yukarıda bahsedilen poliçelerde olduğu gibi, arama motorlarında (Google öneriyoruz: <http://www.google.com.tr>) poliçe adı (örneğin “Access this computer from the network”) arandığında genellikle ilk sırada çıkan Microsoft Technet bağlantısı tıklanarak detaylı bilgiye erişilebilir.

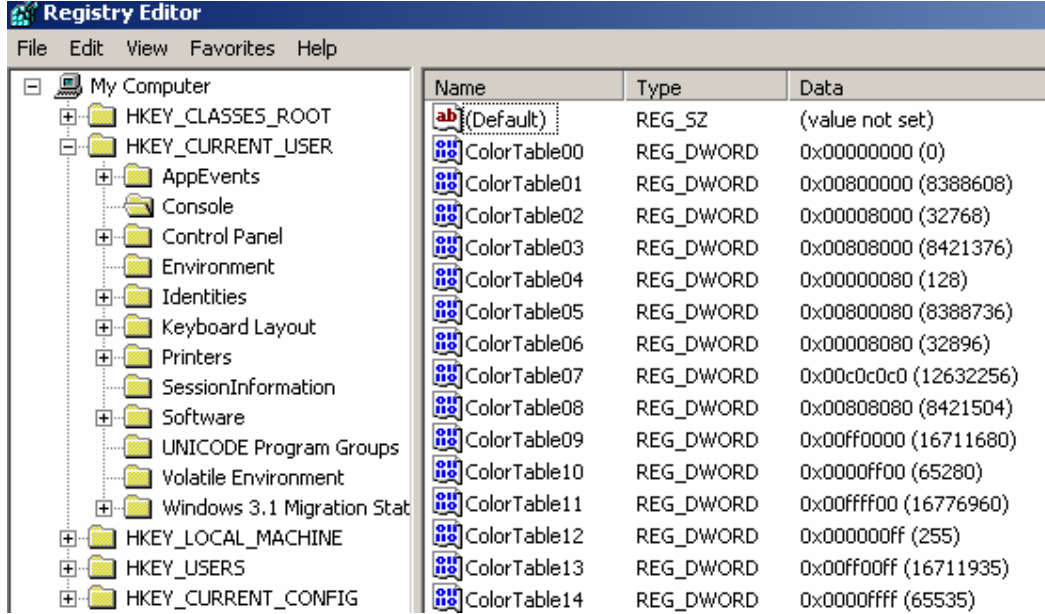


Kullanıcı Hakkı	Hakların kullanıcılara kontrolsüz biçimde verilmesi sonucunda karşılaşılabilecek olası problemler	Bilgisayar Domain Controller ise önerilen ayarlar	Bilgisayar tek makina (Standalone desktop) ya da Domain üyesi ise önerilen ayarlar	Profesyonel kullanıcı için önerilen ayarlar
Access this computer from the network	Administrator hesabının parolasının ele geçirilmesi durumunda bilgisayara ağdan erişerek hakim olunabilir.	Domain Users (Administrator kullanıcılarını çıkarın)	Domain Users	--
Act as part of the operating system	İşletim sistemi gibi hareket etmek her türlü hakka sahip olmak demektir.	--	--	--
Add workstation to the domain	Bu haklara sahip kullanıcılar ağa başka bir DC daha kurup SAM veritabanına ulaşabilirler.	Administrator	--	--
Backup files and directories	Hakkı olmayan kullanıcılar tarafından alınmış yedekler "Restore Files and Directories Right" ile birlikte kullanıldığında izinsiz erişimlere yol açabilir.	Backup Operators	Backup Operators	Backup Operators
Bypass traverse checking	Kullanıcı hakları ile çelişecek klasör erişimlerine yol açabilir.	Administrators, Server Operators, Backup Operators	Administrators, ("Users" IIS için gereklidir).	Administrators
Change the system time	Günlük dosyaları verilerinde karışıklıklara yol açabilir.	Administrator	Administrator	Administrator
Create a pagefile	Bazı durumlarda parolaları içerebilir, ele geçirilmesi riskli olabilir.	Domain Administrators	Administrator	Administrator
Create a token object	Gerekli değilse bu hakkın kullanıcılara verilmemesi önerilmektedir.	--	--	--
Create permanent	Gerekli değilse bu hakkın	--	--	--

shared object	kullanıcılara verilmemesi önerilmektedir.			
Debug programs	Kullanıcıların diğer programaları da kontrol etmelerine ve zararlı kod çalıştırmalarına neden olabilir	--	--	--
Deny access to this computer form the network	Yönetici grubundan birisi bilgisayara ağ üzerinden ulaşırsa parolası ele geçirilebilir	Administrator	--	--
Enable computer and user accounts to be trusted for delegation	Encrypting File System ile birlikte dosya paylaşım sunucularında kullanılır. Geremediği sürece kullanılmaması önerilmektedir.	--	--	--
Increase quotas	Sistem kaynaklarının dengesiz dağıtılmasına neden olabilir	Administrator	Administrator	Administrator
Increase scheduling priority	Kullanıcıların bir işin önceliğini artırması bilgisayarda diğer servislerin durmasına neden olabilir.	Administrator	Administrator	Administrator
Load and unload device drivers	Kullanıcıların sürücü dosyası olarak truva atı yüklemelerine olanak verebilir.	Administrator	Administrator	Administrator
Local pages in memory	Kullanıcı bu özelliği kullanarak servis durdurma saldırısı (Denial of Service Attack) yapabilir.	Administrator	Administrator	Administrator
Log on as a service	Bağlantı kullanıcıya sistem hakları ile bağlanmaya izin verir. Bu hakları isteyen anti-virüs programları vardır ancak izlenmesi önemlidir.	Gerekli programlar	--	--
Log on locally	Yerel bilgisayardan çalıştırıldığında kullanıcı haklarını artıran programlar sayesinde kullanıcılar haklarını değiştirebilirler.	Administrator, Server operators, Backup operators	Administrator, Server operators, Backup operators	Administrator, İzin verilmiş kullanıcılar
Replace a process level token	Kullanıcıya, çalıştırdığı programların önceliğini artırarak güvenlik kurallarını ihlal etme olanağı verebilir.			
Restore files and directories	Yedekleme hakkına da aynı anda sahip olan bir kullanıcı güvenlik açıkları olan yedekleri indirerek sistemde açık kapı yaratabilir.	Backup operators, ya da bu iş için tanımlanmış bir kullanıcı	Backup operators, ya da bu iş için tanımlanmış bir kullanıcı	Backup operators, ya da bu iş için tanımlanmış bir kullanıcı
Shut down the system	Bilinçsiz bir kullanıcı sistem önemli bir iş yaparken bilgisayarı kapatabilir.	Administrator, Server Operators	Administrator	İzin verilmiş kullanıcılar
Take ownership of files or other objects	Kullanıcılar kendilerine ait olmayan dosyaların haklarını elde edebilirler.	Administrator	Administrator	Administrator

Kayıt dosyasında (Registry) gerekli ayarlar yapılmalıdır

Windows kayıt dosyası (registry), işletim sistemi ve işletim sistemi üzerinde çalışan yazılımlar için belirlenen ayarları içerir. Kayıt dosyasındaki bilgilere Start Menü → Run → Regedit kullanılarak ulaşılabilmektedir. Kayıt dosyasının bilinçsiz bir biçimde değiştirilmesi sistemin çalışmamasına neden olabilir, bu nedenle aşağıdaki işlemler yapılırken dikkatli olunması önerilmektedir. Ayarlar değiştirilmeden önce mevcut kayıt dosyasının File menüsü altında bulunan “Export” komutu ile yedeklenmesi önerilmektedir. Sorun çıktığı durumda aynı menüde bulunan “Import” kullanılarak yedeklenmiş kayıt dosyası aktif hale getirilebilmektedir.



Kayıt dosyasında yapılan değişikliklerin geçerli olabilmesi için işletim sisteminin yeniden başlatılması gerekmektedir.

Aşağıda verilen listede, kurulumu yapılan işletim sisteminde değiştirilmesi ya da yaratılması önerilen değerler verilmektedir. Verilen değerler için ayrıntılı açıklama yapılmamıştır. Yukarıda bahsedilen poliçelerde olduğu gibi, arama motorlarında (Google öneriyoruz: <http://www.google.com.tr>) değer adı (örneğin “HKLM\Software\Microsoft\DrWatson\CreateCrashDump” ya da “CreateCrashDump”) aratıldığında detaylı bilgiye erişilebilmektedir.

1. HKLM\Software\Microsoft\DrWatson\CreateCrashDump (REG_DWORD) 0
2. HKLM\Software\Microsoft\Windows NT\CurrentVersion\AEDebug\Auto (REG_DWORD) 0
3. HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun (REG_DWORD) 255
4. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon (REG_DWORD) 0
5. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\DontDisplayLastUserName (REG_SZ) 1
6. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCDisable (REG_DWORD) 4
7. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCDScan (REG_DWORD) 1
8. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCSHOWProgress (REG_DWORD) 0
9. HKLM\System\CurrentControlSet\Control\CrashControl\AutoReboot (REG_DWORD) 0
10. HKLM\System\CurrentControlSet\Services\CDrom\AutoRun (REG_DWORD) 0
11. HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareWks (REG_DWORD) 0
12. HKLM\System\CurrentControlSet\Services\MrxSmb\Parameters\RefuseReset (REG_DWORD) 1
13. HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting (REG_DWORD) 2
14. HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect (REG_DWORD) 0
15. HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect (REG_DWORD) 0
16. HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery (REG_DWORD) 1

17. HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime (REG_DWORD) 300000
18. HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery (REG_DWORD) 0
19. HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect (REG_DWORD) 2
20. HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen (REG_DWORD) 100
21. HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpenRetired (REG_DWORD) 80
22. HKLM\System\CurrentControlSet\Services\Netbt\Parameters\NoNameReleaseOnDemand (REG_DWORD) 1
23. HKLM\System\CurrentControlSet\Services\IPSEC\NoDefaultExpemt (REG_DWORD) 1

Kaynaklar

1. Microsoft Inc. (<http://www.microsoft.com>)

Threats and Countermeasures Guide.pdf (<http://go.microsoft.com/fwlink/?LinkId=15159>)

Windows Server 2003 Security Guide (<http://go.microsoft.com/fwlink/?LinkId=14845>)

Microsoft Windows 2000 TCP/IP Implementation Details
(<http://www.microsoft.com/windows2000/docs/tcpip2000.doc>)

2. Center for Internet Security (<http://www.cisecurity.org/>)

CIS Security Benchmarks and Scoring Tools for Operating Systems:

Windows 2000 Professional -- Level 2 (http://www.cisecurity.org/bench_win2000.html)

Windows 2000 Server -- Level 2 (http://www.cisecurity.org/bench_win2000.html)

3. The SANS Institute (<http://www.sans.org>)

The Twenty Most Critical Internet Security Vulnerabilities (<http://isc.sans.org/top20.html>)

The SANS Security Policy Project (<http://www.sans.org/resources/policies/>)