TÜBİTAK
UEKAE

ULUSAL ELEKTRONİK VE KRİPTOLOJİ
ARAŞTIRMA ENSTİTÜSÜ

Doküman Kodu: BGT-1010

KÜÇÜK OFİS VEYA EV KULLANICISI WINDOWS 7 GÜVENLİĞİ KILAVUZU

SÜRÜM 1.2

14 MAYIS 2010

Hazırlayan: Erdem ALPARSLAN

P.K. 74, Gebze, 41470 Kocaeli, TÜRKİYE
Tel: (0262) 648 1000
Faks: (0262) 648 1100
http://www.bilgiguvenligi..gov.tr
teknikdok@bilgiguvenliği.gov.tr

2. MİCROSOFT WİNDOWS 7 GÜVENLİĞİ

2.1 Giriş

İşletim sistemleri; bilgisayar donanımının doğrudan denetimi ve uygulama programlarını çalıştırmaktan sorumlu olan sistem yazılımlarıdır.

İşletim sistemi bilgisayarın her türlü altyapı çalışmalarını düzenler, çeşitli aygıtların birbirleriyle anlaşmasını sağlar. Bu sayede çeşitli uygulama yazılımları, güven içinde çalışıp kullanıcıya hizmet edebilirler. Bu yüzden bir bilgisayarın donanım özellikleri kadar işletim sistemi de önemlidir. Çünkü sistemin genel performansı gibi işlevleri de kullanılan işletim sistemine göre değişir. Bu yüzden sistem ne kadar karmaşıksa, işletim sistemi de o oranda gelişmiş olmak zorundadır.

Sistemin güvenli olarak çalışabilmesi, işletim sisteminin güvenliğinin sağlanmasına bağlıdır. Bundan dolayı kullanıcılar tarafından işletim sistemlerinin güvenlik ayarları yapılarak sistem güvenli hale getirilmelidir.

Bu bölümde Microsoft'un yeni işletim sistemi olan Windows 7 Ultimate işletim sistemine ait güvenlik özellikleri ele alınacaktır. Windows 7 Ultimate işletim sistemi değişik şekillerde kullanılmaktadır. Burada küçük ofiste veya evde merkezi kullanımı olmayan yapı anlatılacaktır. Burada anlatılan ayarların büyük bir kısmı Windows 7 Home, Professional ve Enterprise Edition, Windows XP ve Windows Vista'ya uygulanabilir.

2.2 Windows 7

Windows 7 işletim sistem Microsoft'un Vista ürününden sonra çıkardığı en yeni nesil işletim sistemidir. Vista işletim sistemi ile birlikte Windows ailesine kazandırılmaya çalışılan yeni görsel arayüz mantığı Windows 7'de daha belirgin hale getirilmiştir. Bu belirginleşme ile beraber sistem kaynaklarını da ihtiyacı olacak minimum seviyede tüketerek bu görselliğin gerçeklenmesi sağlanmaktadır.

Aynı zamanda Windows 7, kendisinden önce sıklıkla kullanılmakta olan Windows XP Professional işletim sistemine nazaran güvenlik konusunda daha bütüncül bir yaklaşım benimser. Microsoft Vista işletim sisteminde "güvenlik merkezi" adı altında gerçekleştirilmeye çalışılan bu bütüncül güvenlik anlayışı, Windows 7 işletim sisteminde "işlem merkezi" isimli denetim masası kontrolü tarafından gerçekleştirilir. İşlem merkezi sadece güvenlikle ilgilenmez; bununla beraber performans ilkelerini de düzenleme imkanı sunar. Yani denilebilir ki Windows 7 güvenlik sorununu performans sorunu ile beraber düşünür, güvenlik kaynaklarının temel kaynaklarla uyum içerisinde çalışmasını sağlar.

Microsoft Vista işletim sistemi ile beraber hazır uygulama olarak gelen Microsoft Defender yazılımı Windows 7'de de aynı şekilde hazır olarak bulunmaktadır. Bununla beraber hem dıştan içe hem içten dışa trafiğin kontrol edilebildiği Windows Güvenlik Duvarı da bu işletim sisteminde gelişmiş olarak bulunur. Antivirüs uygulamaları ile uyum içerisinde çalışan Windows 7 işlem merkezi kullanıcı hesaplarının denetimi ve ebeveyn kontrolü gibi ek özellikleri de bünyesinde barındırır.

Dosya ve dizin güvenliği, şifrelenmesi Windows 7'nin de odaklandığı bir noktadır. Öyle ki Enterprise sürümünde hazır olarak gelen BitLocker yazılımı disk bölümü şifreleme imkanı sunmaktadır.

Tabii ki Windows Güncellemeleri Windows 7 işletim sisteminin de en üzerinde durduğu konulardan birisidir. Güncellemeler konusunda farklı politika seçimleri kullanıcıya bırakılmıştır.

2.3 Dosya Şifrelenmesi (EFS -Encrypting File System)

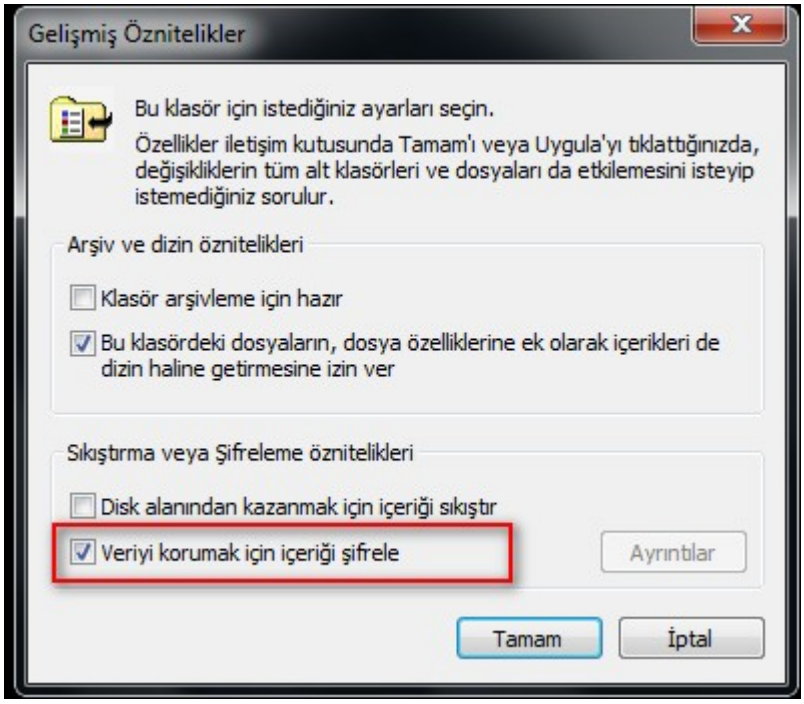
Bilgisayardaki önemli ve gizli kalması gereken verilere sadece erişim hakları ile koruma sağlamak yetersiz olabilir. Erişim hakkı düzenlemeleri sırasında yapılacak hata, yetkisiz kişilerin de dosyalara erişmesini neden olabilir. Bu durum önemli bir güvenlik açığıdır. Bu tür durumlara karşı, Windows XP ve Vista işletim sisteminde olduğu gibi Windows 7 Ultimate işletim sistemi de kullanıcılara dosya ve dizinleri şifreleme özelliği sağlamaktadır.

EFS sadece NTFS dosya sisteminin desteklediği bir özelliktir. Dosya şifrelendiği zaman, EFS verileri şifrelenmiş olarak disk üzerinde saklar. Şifrelenmiş dosyalara sadece dosyanın sahibi erişebilir.

Herhangi bir kişi şifrelenmiş dosyalara erişmeye kalkışırsa dosyaları göremeyecek, erişimin engellendiğini belirten bir mesajla karşılaşacaktır.

Şifrelenecek dizin ya da dosya üzerinde sağa tıklanır. Açılan menüden özellikler seçilir.

Özellikler penceresinden gelişmiş butonuna tıklanır. Gelişmiş penceresinden "veriyi korumak için şifrele (Encrypt contents to secure data) " seçeneği işaretlenir.



Şekil 1 Dosya Şifreleme

Windows 7 Ultimate işletim sistemi kullanıcıların dosyanın özelliklerine bakmadan şifrelenmiş olup olmadığını anlaması için, simgelerinin altındaki yazıların rengini değiştirir. Bu sayede gezgin penceresinden dosyanın özelliği belli olur.

Dosya ve klasörleri şifrelemek sadece NTFS dosya sistemine ait bir özellik olduğu için, şifrelenmiş bir dosyanın NTFS olmayan bir volume üzerine taşınması durumunda şifrelenme özelliği kalkacaktır. Bu durumda dosyaya erişmek isteyen bir kullanıcı tanınamayan karakterler halinde dosyayı görecektir.

Şifrelenmiş dosyaların ağ üzerinden transferi sırasında, şifreleme özellikleri ortadan kalkar. Ağ üzerindeki transfer sırasında güvenlik sağlanmak istenirse EFS kullanılamaz. Bunun yerine ağ üzerindeki güvenliği sağlamak için IPSec, Remote Desktop veya Terminal servisleri kullanılır. Bu uygulamalar dosyaları ağ üzerinden şifrelerini açmadan gönderirler.

2.4 Dosyaların Yedeklenmesi

İşletim sistemlerinde sistem çökmesi ve donanım hatalarından dolayı veriler kaybedilebilir. Bu sebeplerden dolayı dosyaların yedeklenmesi gerekir. Yedekleme işlemi; kaybolma tehlikesi olan verilerin başka ortamda kopyalarını bulundurma işlemidir.

Windows 7 ortamında önemli verilerin etkin bir şekilde korunması için öncelikle diskin uygun bir şekilde biçimlendirilmesi gerekmektedir. Bu biçimlendirmede işletim sistemi ve kullanıcıya ait önemli bilgiler disk üzerinde yaratılmış farklı mantıksal disklere (partition) konulmalıdır. Çünkü herhangi bir nedenden dolayı işletim sistemi kullanılmaz hale geldiğinde kullanıcıya ait önemli veriler zarar görmemelidir. Kullanıcı işletim sisteminin kurulu olduğu mantıksal diske (partition) format atarak yeniden kurabilmelidir. Örneğin 160 GB alana sahip olan bir disk 50 GB işletim sistemi diski (C:\ sürücüsü) 110 GB kişisel dosyaları ve programları saklamak için arşiv diski (D:\ sürücüsü) olarak iki parçaya ayrılabilir. Hatta bilgisayar üzerine Windows dışında bir işletim sistemi kurulacaksa arşiv diski 90 GB yapılıp 20 GB alan da ikinci işletim sistemi (Örneğin: linux) için ayrılabilir.

Hatta problemin kaynağının tespit edilebilmesi için işletim sistemine ait olay kayıtları da işletim sisteminin bulunduğu diskte bulunmamalıdır.

Windows 7 işletim sisteminin dosyalarını ve ayarlarını saklamak için bir yedekleme programı mevcuttur. Bu programı çalıştırmak için "*Başlat→Denetim Masası→Yedekleme ve Geri Yükleme"* seçenekleri ile yedekleme programı çalıştırılarak dosya ve ayarların yedeği alınabilir. Bu yedeklemeye ait ayrıntılar bu dokümanda verilmeyecektir.

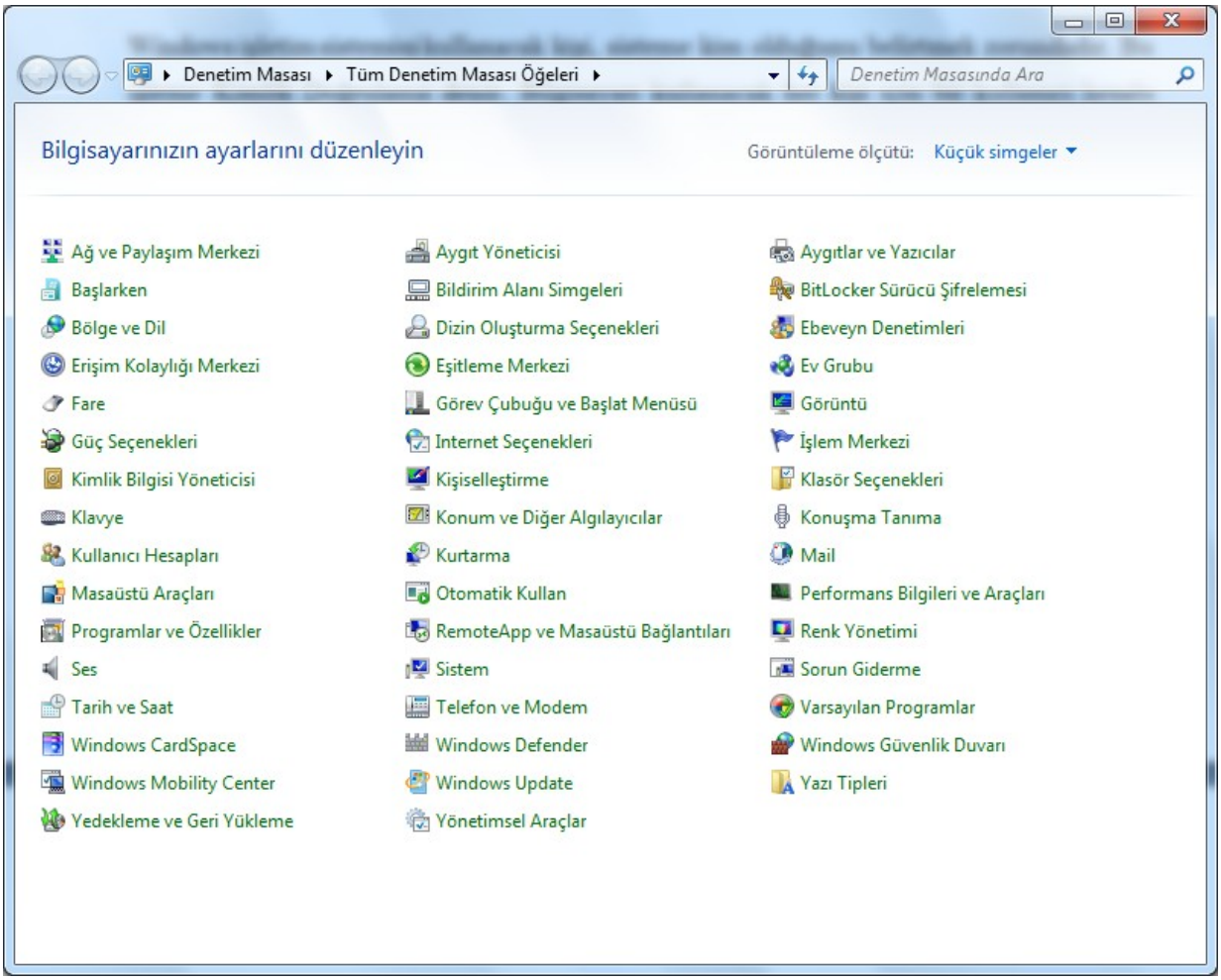
Sabit diskin bozulması veya uzaktan ele geçirilerek içerisindeki verilerin silinmesine karşın sabit diskte bulunan önemli dosyalar başka bir saklama ortamına (USB Disk, Tape Kartuşu, CD, DVD, vb.) yedeklenmelidir.

2.5 Kimlik Doğrulama ve Kullanıcı işlemleri (Authentication)

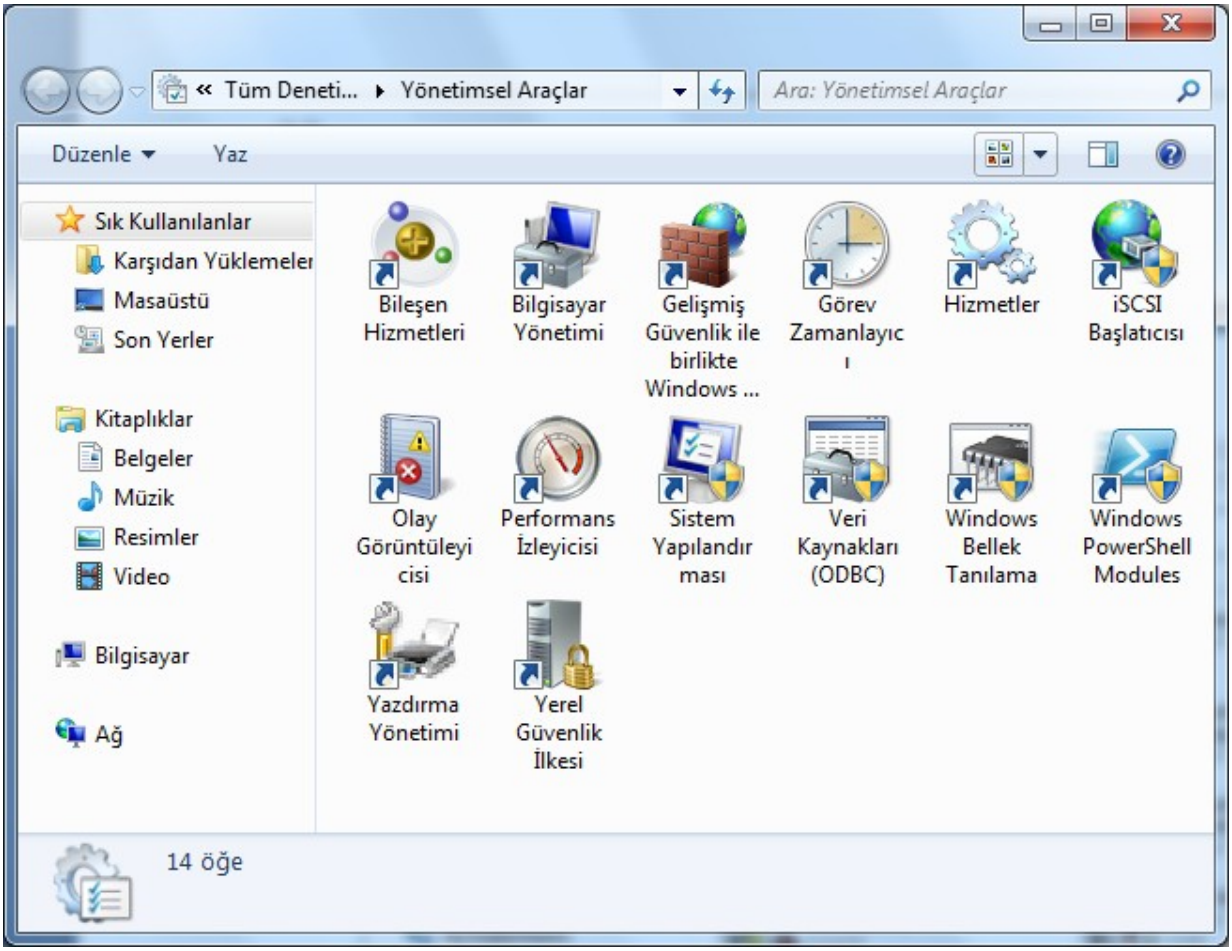
Windows işletim sistemini kullanacak kişi, sisteme kim olduğunu belirtmek zorundadır. Bu işleme Kimlik Doğrulama denir. Bilgisayarı kullanacak her kişi için bir kullanıcı hesabı oluşturulur. Bilgisayarı kullanacak kişi hesabın sahibi olduğunu ispatlamak için kullanıcı adı ve parolası girmek zorundadır. İşletim sistemi eğer bu bilgiler doğru ise sisteme girişe izin verir. İşletim sistemlerinde bu sürece oturum açma (logon) denir.

2.6 Parola İlkeleri Oluşturma

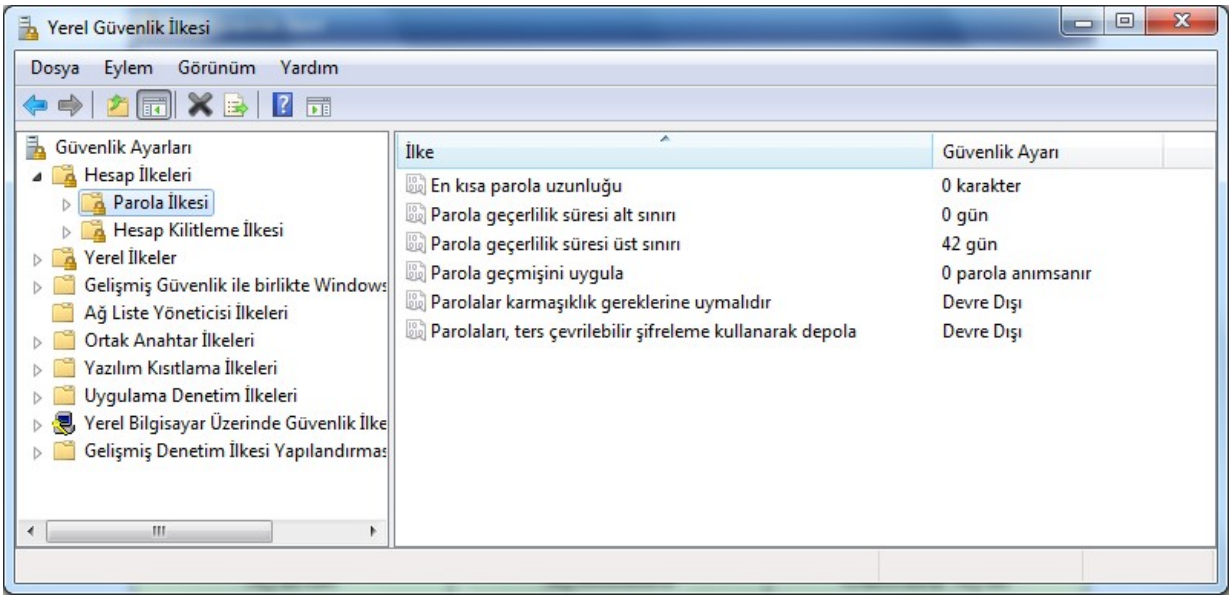
Kullanıcı parola ilkeleri oluşturmak için; *Denetim masası→Yönetimsel Araçlar→ Yerel Güvenlik İlkeleri*'ne girilir. *Hesap İlkeleri* altında *Parola İlkesi* seçilir.



Şekil 2 Denetim masası



Şekil 3 Yönetimsel araçlar



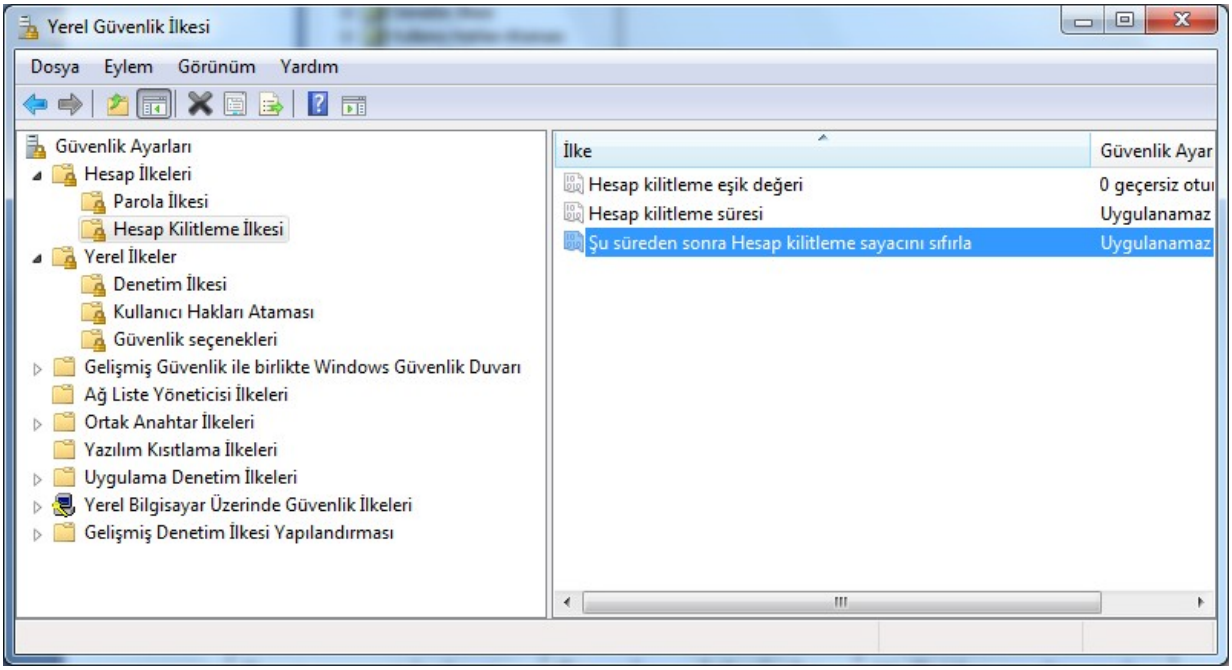
Şekil 4 Yerel güvenlik ilkeleri

Şifre politikasına ait tavsiye edilen değerler Tablo 1'de verilmiştir.

Ayarlar	Açıklaması	Önerilen Ayar
Parolaları, ters çevrilebilir şifreleme kullanarak depola	Bu güvenlik ayarı işletim sisteminin parolaları ters çevrilebilir şifreleme kullanarak depolayıp depolamayacağını belirler.	-----
Parola Geçerlilik Süresi Üst Sınırı (Maximum password age)	Kullanıcının verdiği şifreyi ne kadar süre kullanabileceği 0-999 arası bir değerdir. 0 olursa hep aynı şifreyi kullanabilir.	42'den fazla
Parola Geçerlilik Süresi Alt Sınırı (Minimum password age)	Kullanıcının şifresini değiştirebileceği minimum süre	-----
En Kısa Parola Uzunluğu (Minimum password length)	Kullanıcının şifresinin en az kaç karakter olacağı (0-14 arası	8 karakter
Parolalar Karmaşıklık Gereklerine Uymalıdır (Password must meet complexity requirement)	Kullanıcının şifre belirlerken uygulanması zorunlu değerler kullanmasını sağlar. Kullanıcı kendi adını şifre olarak giremez.	------

Tablo 1 Şifre politikası

Yerel güvenlik politikasına ait seçenekler Şekil 5'de gösterilmiştir.



Şekil 5 Yerel güvenlik politikası

Yerel güvenlik politikasında tavsiye edilen değerler Tablo 2'de verilmiştir.

Ayarlar	**Açıklaması**	**Önerilen**
Hesap kilitleme süresi (Account lockout duration)	Kullanıcının hesabının kilitli kalacağı süre	30 dk.'dan az olmamalı.
Hesap kilitleme eşik değeri (Account lockout threshold)	Kullanıcı kaç kez yanlış şifre girdiğinde hesabı kilitlensin	5'ten fazla olmamalı
Şu süreden sonra Hesap kilitleme sayacını sıfırla (Reset account lockout counter after)	Tanımlanan değer kadar sonra kullanıcının hesabı otomatik olarak açılsın	30 dk.'dan az olmamalı

Tablo 2 Kullanıcı hesabı politikası

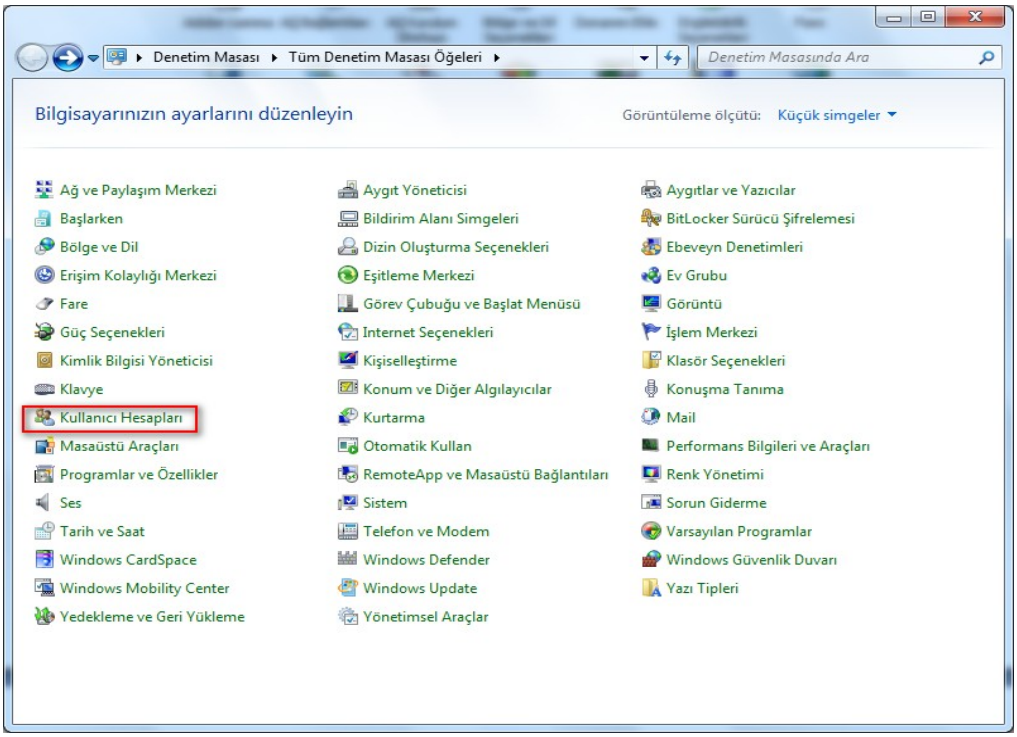
2.7 Kullanıcı Oluşturma ve Haklarını Belirleme

Kullanıcı hesabı, bilgisayar ortamında kullanıcıyı tanımlayan bir nesnedir. Kullanıcı hesabı ile bir kullanıcı bilgisayarda oturum açma ve kaynakları kullanma yetkisine sahip olur. Her kullanıcı sahibine erişim hakları ve izinleri verilir. Windows 7 işletim sistemine yeni bir kullanıcı tanımlandığında varsayılan değer olarak "users" grubuna katılır ve bu grubun makine üzerinde sadece kısıtlı erişime izni vardır. Bu hakka sahip kullanıcılar sisteme sınırlı haklarla erişim yapabilirler: program kuramaz, kaldıramaz, yeni kullanıcı ekleyemez, silemez, kendi hesabına ait şifreyi değiştirebilir, kendi hesabına resim ekleyebilirler.

Windows 7 işletim sistemi üzerinde "power users" grubuna katılmış bir kullanıcı sistem üzerinde basit değişiklikler yapabilir (örn; görüntü ayarları ya da güç ayarları). Kullanıcı "administrators" grubuna katıldığında ise yeni kullanıcı tanımlayabilir ya da silebilir, sistemde bulunan bütün dosyalara erişebilir, donanım ya da yazılımda değişiklikler yapabilir, sistem üzerinde geniş kapsamlı değişiklikler yapabilir.

Windows 7 işletim sisteminde iki şekilde kullanıcı tanımlanır:

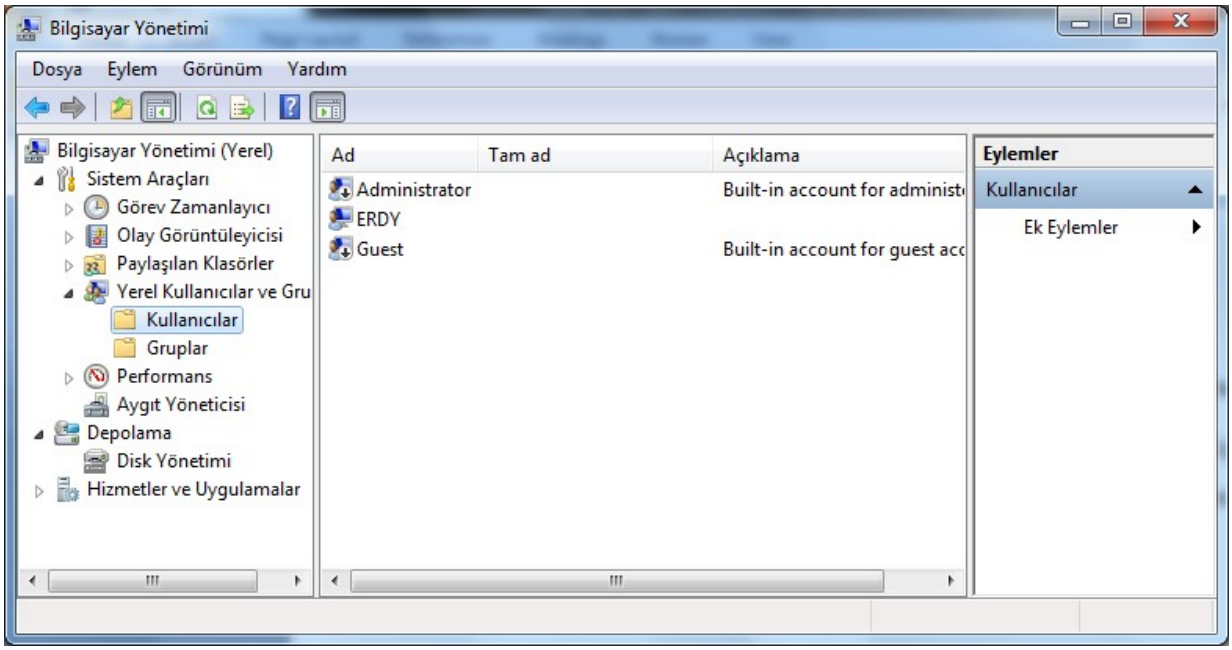
İlki klasik yöntem: *Denetim Masası → Kullanıcı Hesapları →Başka Bir Hesabı Yönetin →Yeni Hesap Oluştur.*



Şekil 6 Denetim masası

Sistemde yerel kullanıcı tanımlamak için ikinci yol; Bilgisayarım ikonu üstünde farenin sağ tuşu tıklanır *Yönet* seçeneği seçilir.

Gelen ekranda yerel kullanıcılar ve gruplar klasörleri görülmektedir. Bu durum Şekil 7'de görülmektedir.

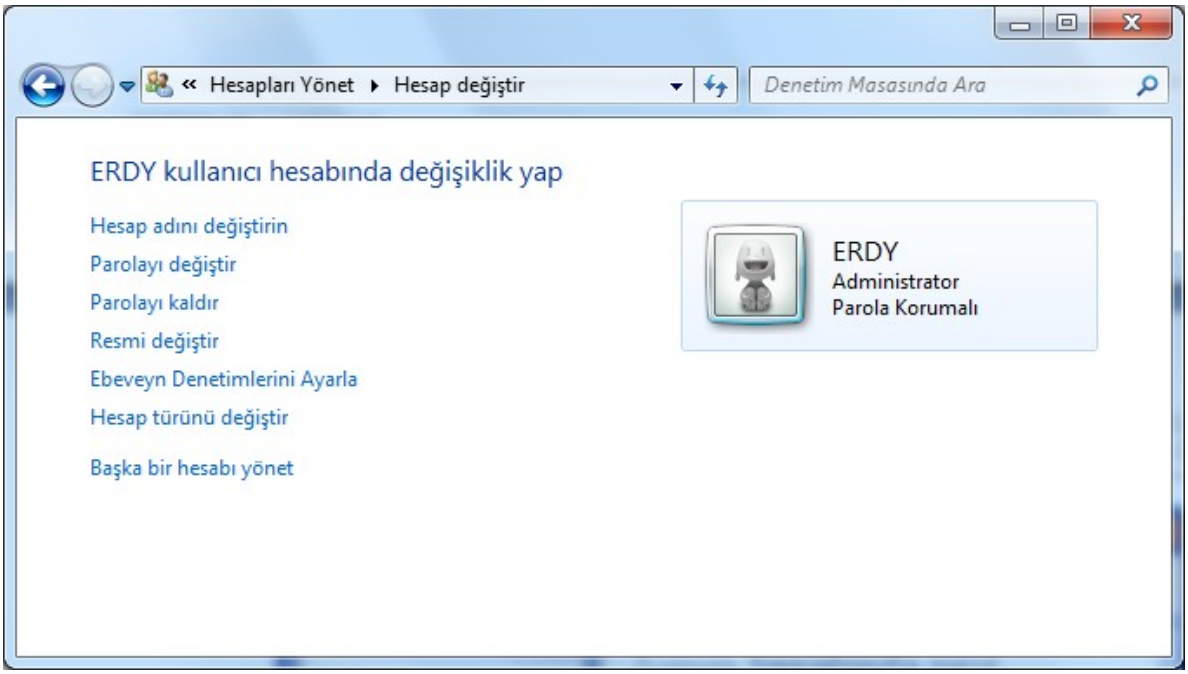


Şekil 7 Bilgisayar yönetimi

Sistemde bulunan kullanıcılar görülmektedir. Bu kullanıcılar varsayılan olarak gelmektedir.

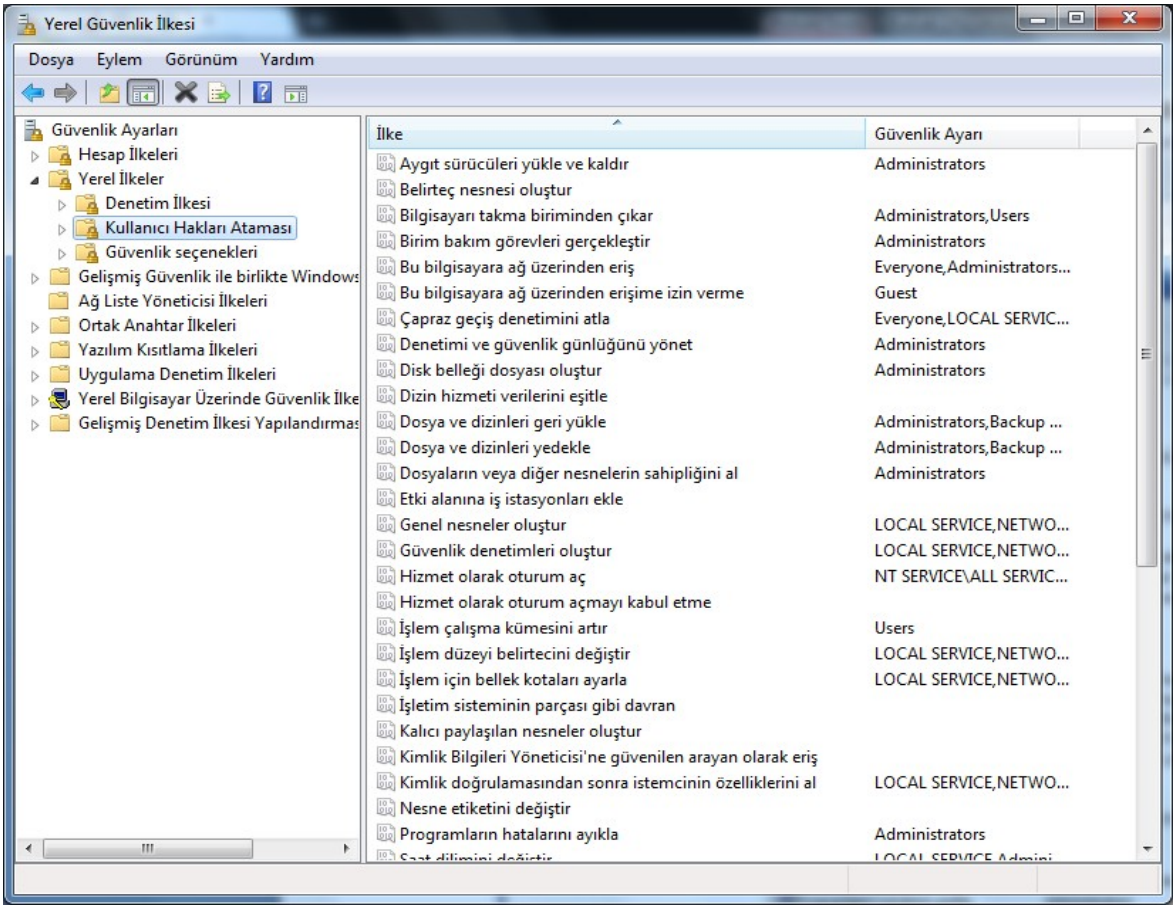
Yeni bir kullanıcı yaratılmak istendiğinde Şekil 7'de sağ pencere içinde bir yerde farenin sağ tuşuna tıklanarak yeni kullanıcı oluştur seçeneği seçilir. Gelen pencerede kullanıcı ismi parolası girilerek oluştur seçeneği ile kullanıcı oluşturulur.

Oluşturulan kullanıcıya ait ayarlama *Başlat→Denetim Masası→Kullanıcı Hesapları*'ndan kullanıcı seçilerek yapılabilir. Kullanıcı hesabı ile değiştirilebilecek ayarlar Şekil 8'da görülmektedir.



Şekil 8 Tanımlanan kullanıcı

Kullanıcı hakları yerel güvenlik ayarlarından verilmektedir.

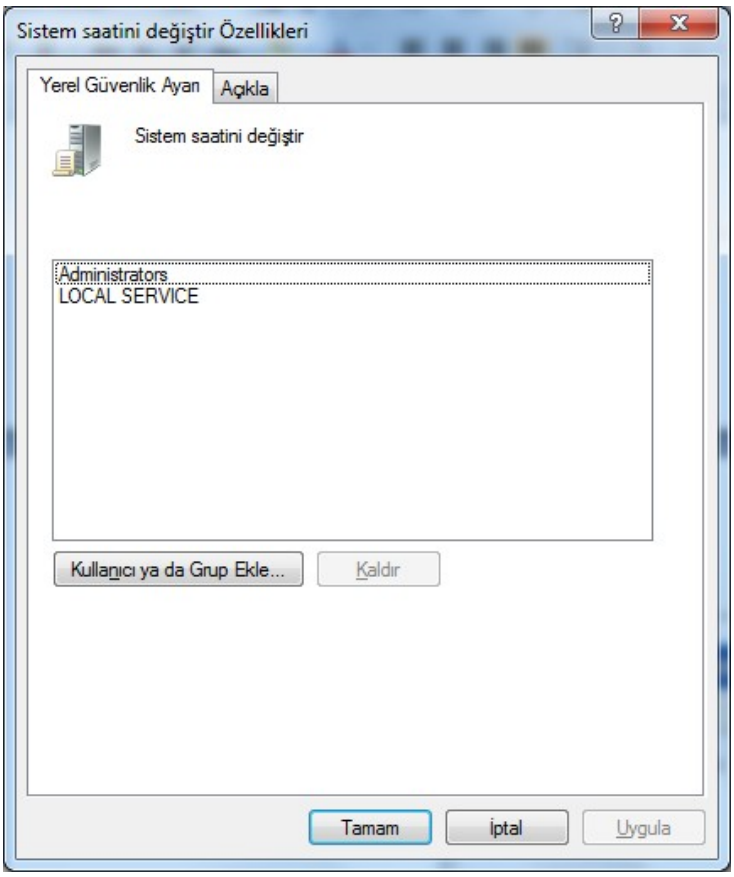


Şekil 9 Kullanıcı hakları

Bu ayarları yaparken kullanıcıya verilecek engelleme (deny) hakkı en baskın ayar olmakta ve kullanıcının diğer bütün izinlerini engellemektedir.

Kullanıcı haklarını kaldırmak ya da ekleme yapmak için; istenilen ayar üzerinde sağa tıklanır.

Örneğin; Sistem zamanını değiştirme yetkisi, administrators ve power users'a aittir. Bu durum Şekil 10'de görülmektedir. Kaldır denilerek kullanıcı hakkı kaldırılabilir ya da kullanıcı ekle diyerek bu hak başka kullanıcılara verilebilir.



Şekil 10 Kullanıcı hakları

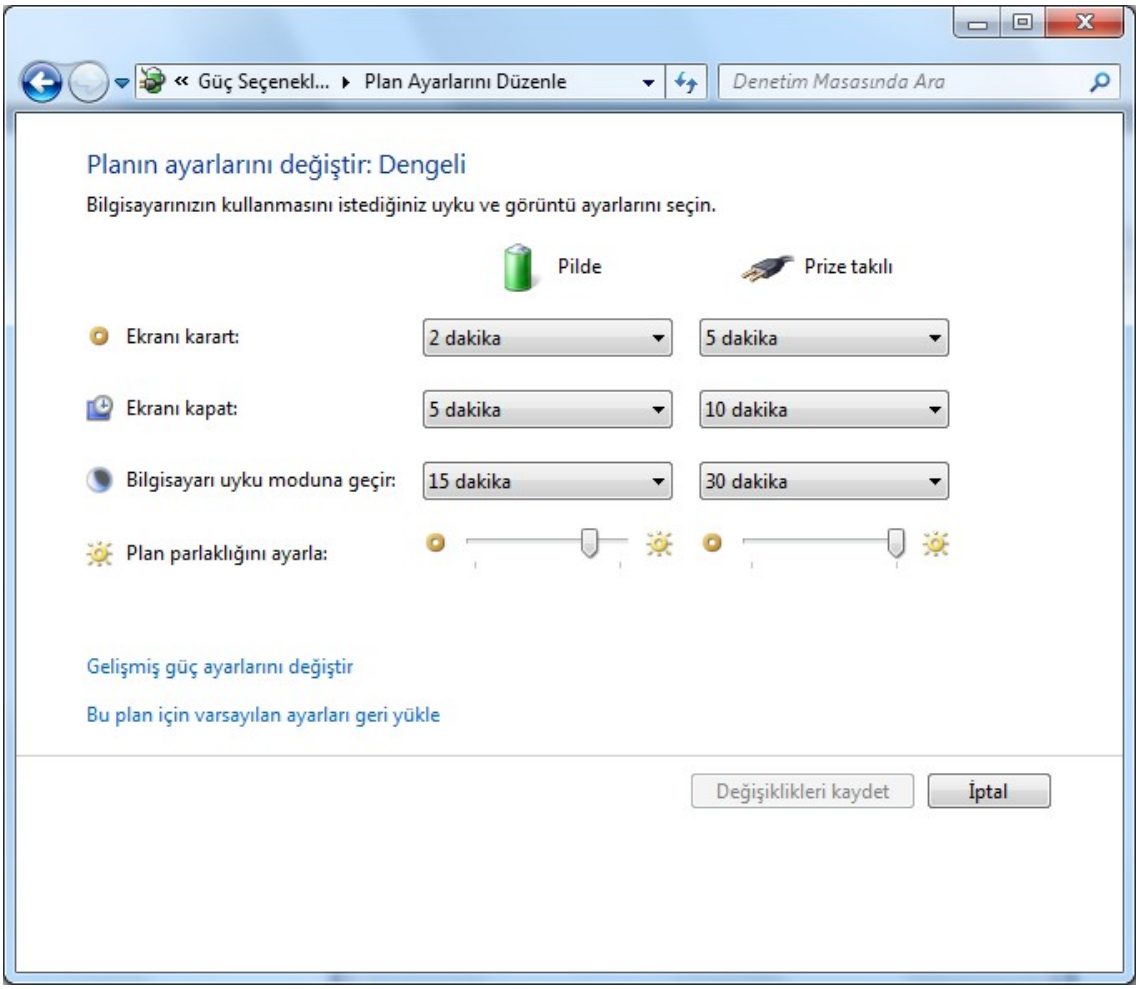
2.8 Ekran Kilitlenmesi

Bu ayarlama, bilgisayarın kullanılmadığı zamanlarda güvenliği ve daha az enerji harcamasını sağlamak amacıyla yapılır. Güç yönetimi ayarlarında monitörü kapat, sabit diskleri kapat ve sistem bekleme konumu özellikleri için belirli bir süre belirlenebilir. Belirlenen bu süre sonunda o aygıt bir anlamda uyku konumuna geçip minimum düzeyde enerji harcamaya başlar.

Güç yönetimi ayarlarını yapmak için;

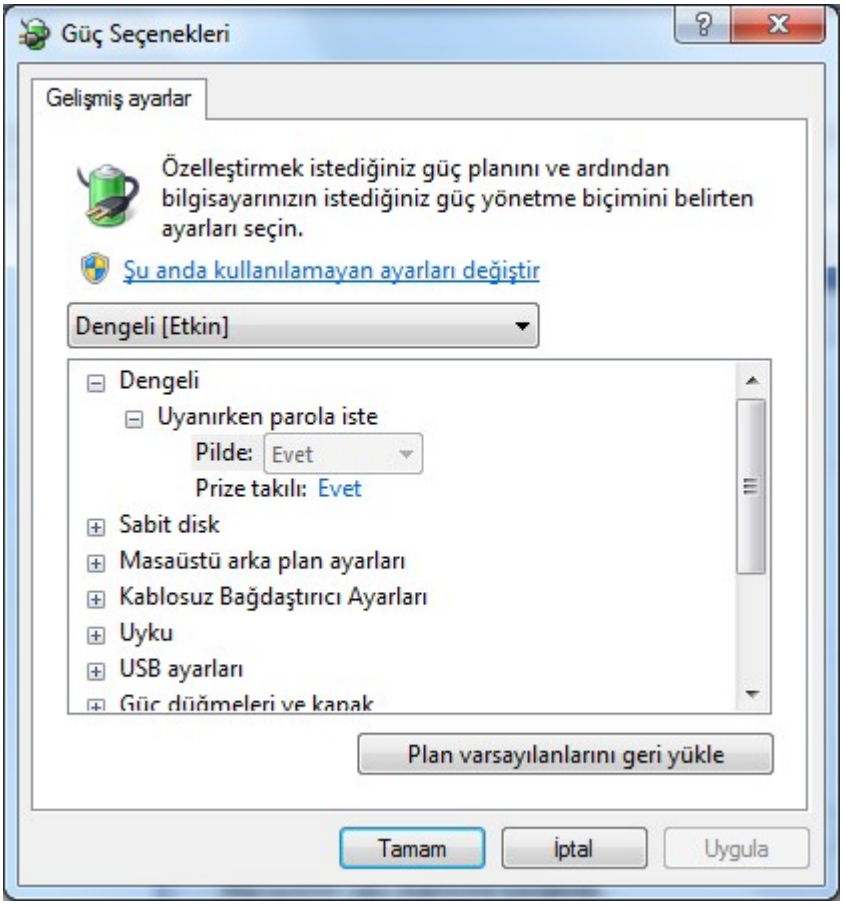
Denetim masası→Performans bilgileri ve araçları→ Güç ayarlarını düzenle ekranı

Gelen ekranda monitör, hardisk ve sistem bekleme durumu ile ilgili ayarlar yapılmıştır.



Şekil 11 Güç yönetim özellikleri

Gelişmiş sekmesine tıklanır ve bilgisayar bekleme ya da uyku modundan çıkmadan önce bilgisayarın Windows parolasını istemesi için ayar yapılabilir.



Şekil 12 Gelişmiş sekmesi

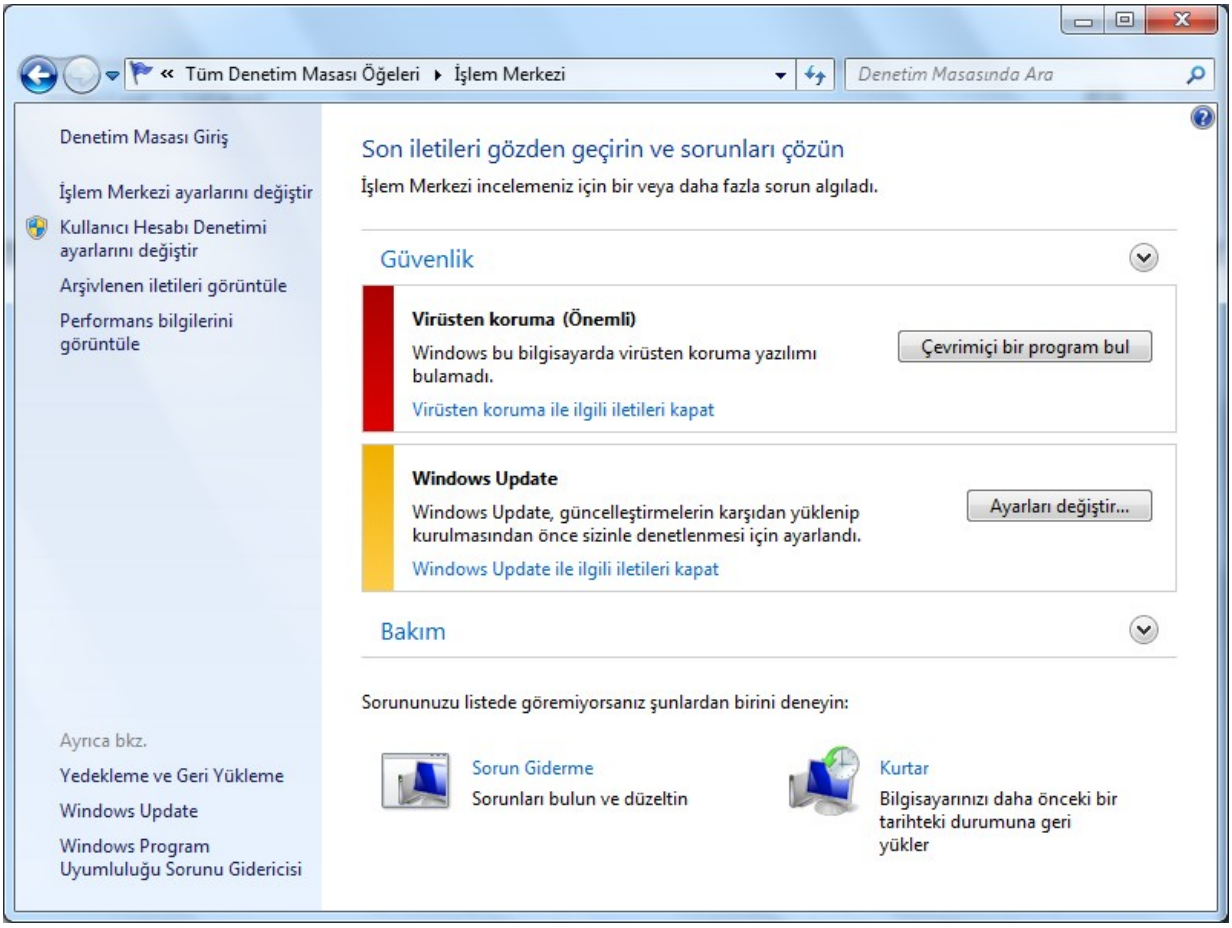
Belli bir süre sonra bilgisayar kullanılmazsa aşağıda görülen ekran gelir ve sistemde tekrar oturum açmak gerekir.

Şekil 13 Ekran kilitlenmesi

2.9 Microsoft 7 Güvenlik Merkezi

2003 yılında Windows XP servis paketi 2 çıkarılırken güvenli artırmak için güvenlik duvarı, antivürüs koruması ve güncellemeyi içeren Windows Güvenlik Merkezi eklendi. Bu üç güvenlik servisinden birinin durdurulması ya da güncelliği kaybetmesi durumu doğrudan kullanıcıyı uyaracak şekilde ayarlandı.

Windows 7 işletim sisteminde ise işlem merkezi adı altında işletim sisteminin hem güvenlik hem de performans takibinin ve değişikliklerinin yapıldığı bir arayüz ortaya konmuştur. İşlem merkezine *Denetim Masası -> Güvenlik-> Güvenlik Merkezi* seçeneğinden ulaşılabilir.



Şekil 14 İşlem Merkezi

2.9.1 Güncelleme Yapılması (Update)

Günümüzde bilgisayar sistemleri üzerinde ciddi boyutlarda hasara neden olan virüs, ajan yazılım ve solucan türü zararlı programlara karşı önlem almak zorunludur. Bunun yanı sıra işletim sistemlerinde zaman içinde tespit edilen açıkları kapatmak ve hatalı yazılmış kodları düzeltmek amacıyla Microsoft firması belirli aralıklarla yama ve hizmet paketleri yayınlamaktadır. Bilgisayar sistemlerini dışarıdan gelebilecek olası saldırılara (virüs ya da hackerlar) karşı koruma altına almak için Microsoft tarafından yayınlanan yama ve hizmet paketlerinin sürekli takip edilmesi gerekir. Microsoft geliştirdiği güncelleme yazılımlarını kullanımda kolaylık sağlaması için belli kategorilere ayırır.

Güvenlik Yaması (Security Patch): Belli bir ürünün güvenlik açığını kapatır. Mutlaka uygulanmalıdır.

Kritik Güncelleme (Critial Update): Kritik bir hatayı giderir. Mutlaka kurulmalıdır.

Güncelleme (Update) Belirli bir problemi giderir.

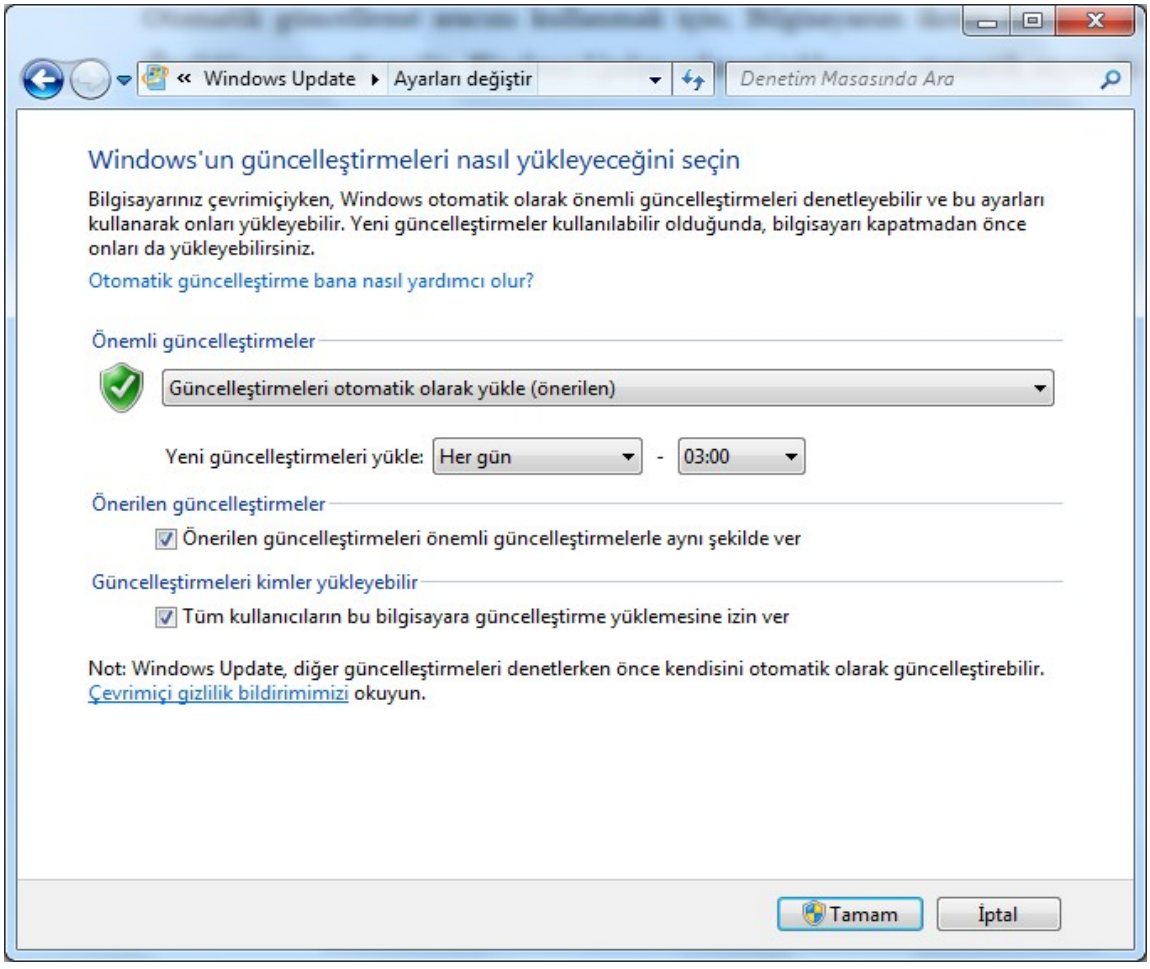
Servis paketi (Service Pack): Belirli bir ürünün tüm güncellemelerini yapar.

İşletim sisteminin güvenli olabilmesi için kullanıcı bu güncelleme yazılımlarını mutlaka yüklemelidir.

Güncelleştirmeler, http://www.update.microsoft.com/ sitesinden indirilebilir. Site, sistemin ihtiyacı olan güncellemeleri bulup listeleyebilir. Her güncellemenin açıklamasını yapar ve istenilenleri kurabilir. Güncellemelerin yapılabilmesi için Windows seri numaranızın gerçek olması gerekmektedir.

Güncellemeleri elle yapmak kullanıcıya bir yük getirir. Windows, güncellemelerin otomatik olarak yapılmalarını sağlar. Otomatik güncelleme aracı gerekli güncellemeleri otomatik olarak indirip kurulmalarını sağlar.

Otomatik güncelleme aracını kullanmak için; Bilgisayarım ikonu üzerinde sağa tıklanır *Özellikler* seçeneği seçilir. *Windows Update* bağlantısı tıklanır ve *Ayarları Değiştir* bağlantısına basılır. Gelen ekranda otomatik seçeneği işaretlenir.

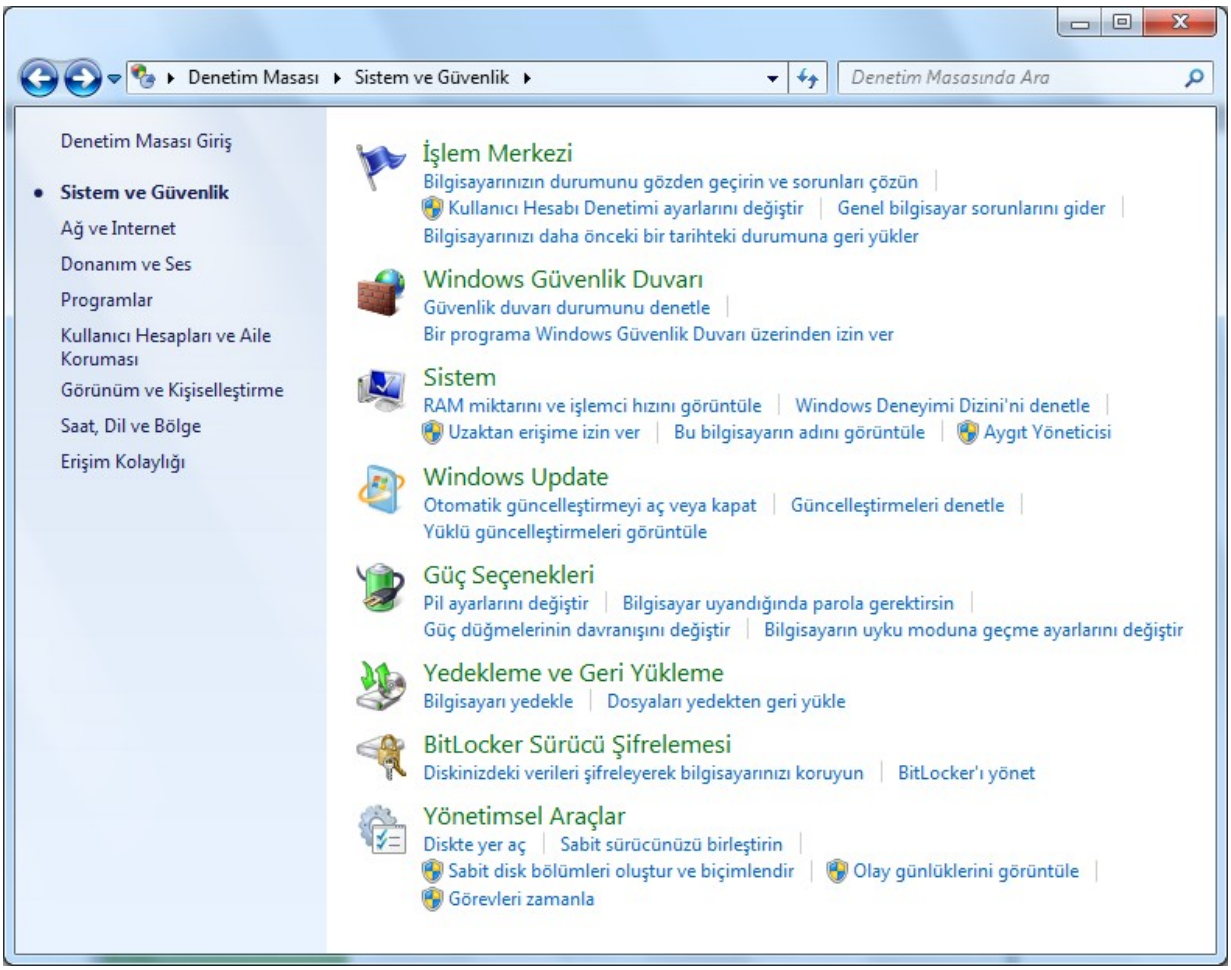


Şekil 15 Otomatik güncelleme

2.9.2 Güvenlik Duvarı

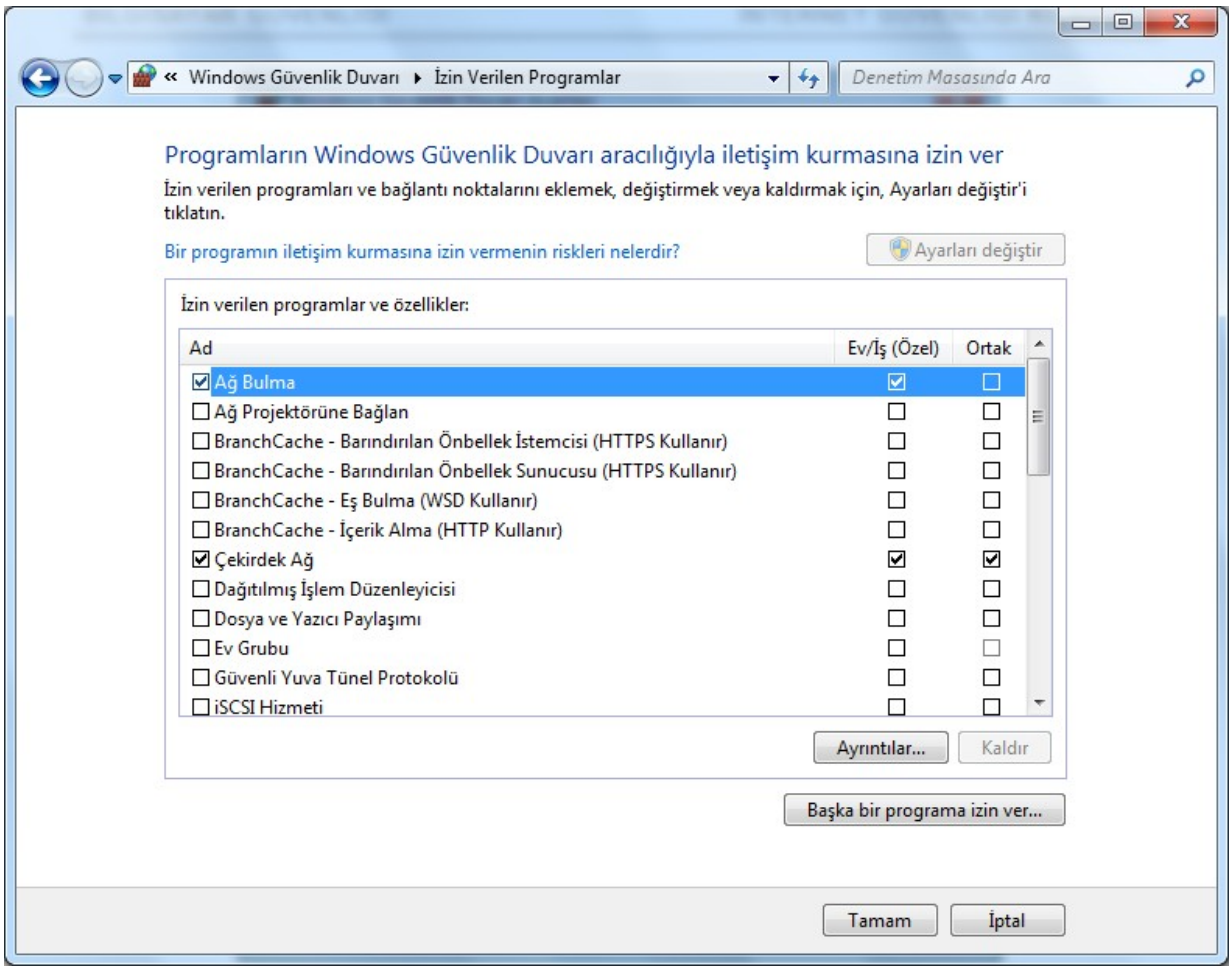
Güvenlik duvarı etkinleştirildiğinde bilgisayarı zararlı yazılımlara karşı korur. İç ağdan dış ağa gidecek ya da dış ağdan iç ağa girecek trafiğinin kontrolünü sağlar. Yani sadece kullanıcının isteği iletişime izin verir.

Güvenlik duvarı ayarlarını yapmak için; *Denetim Masası→Sistem ve Güvenlik* seçeneğine tıklanarak işlem merkezi, güvenlik duvarı, güncelleme, virüs koruma, casusu/zaralı yazılımlara karşı koruma, internet güvenlik ayarları ve kullanıcı hesabı denetim ayarlarına ulaşılabilir.



Şekil 16 Windows güvenlik merkezi

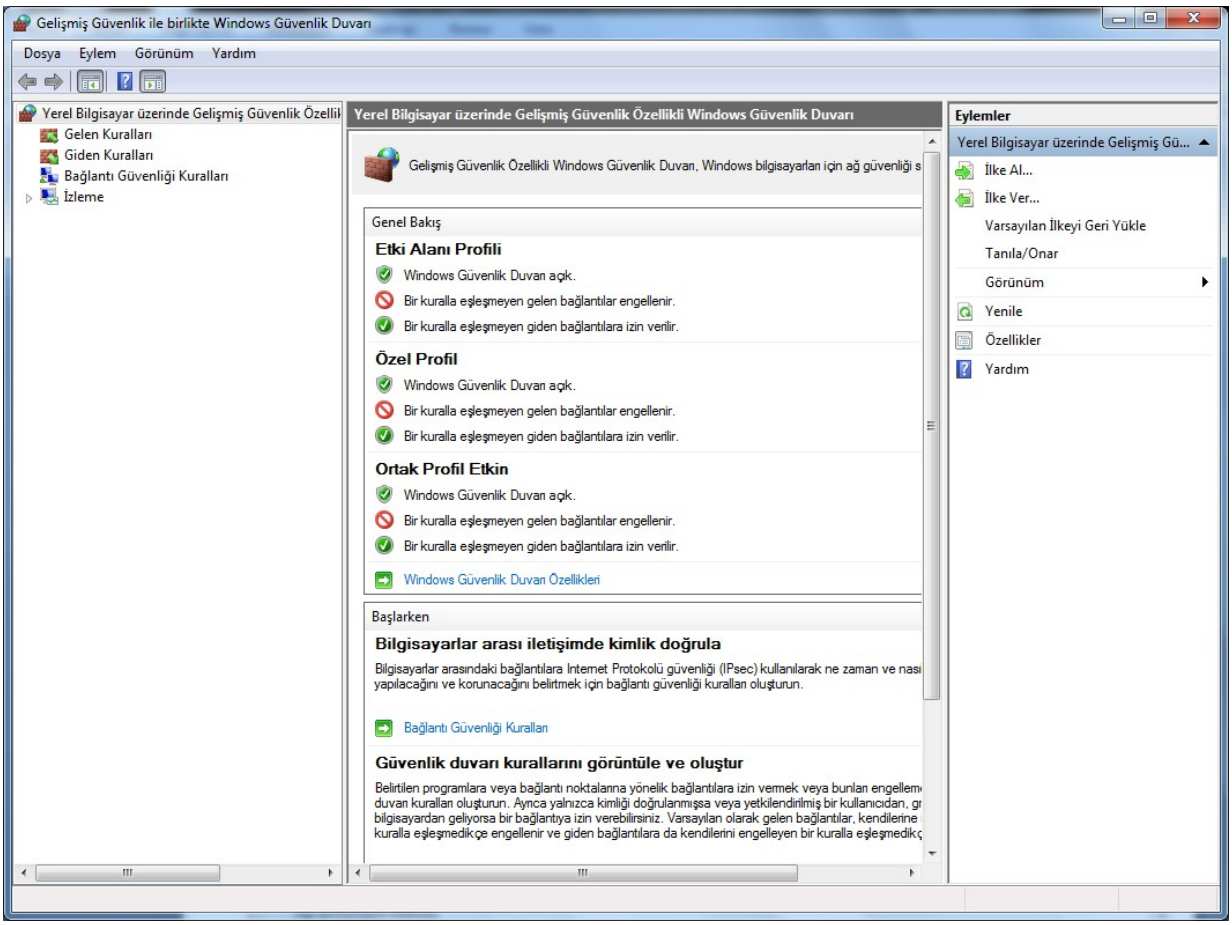
Normal koşullarda güvenlik duvarı içerden dışarıya her türlü erişime izin verir fakat dışarıdan içeriye hiç bir erişime izin vermez. *Bir programın ya da özelliğin güvenlik duvarını aşmasına izin ver* seçeneği istisnai olarak dışarıdan içeriye erişim izni verebilmek için konulmuştur. Çünkü bazı dosya paylaşım programları (Kaza, emule vb.) ve haberleşme programları (msn) dışarıdan erişim isteyebilirler. Bu erişimler buradan verilebilir. Kullanıcılar bilgisayara dışarıdan erişimi mümkün hale getiren bu ayarı yaparken dikkatli olmalıdır. Gerekmiyorsa hiçbir program için dışarıdan erişim verilmemelidir. Şekil 17'te güvenlik duvarı üzerinde dışarıdan erişime izin verilen servisler görülmektedir.



Şekil 17 Güvenlik duvarı ayarları

Gelişmiş seçeneğinde içeriden dışarıya veya dışarıdan içeriye bağlantılar kontrol edilebilir. Gelişmiş güvenlik duvarı ayarlarına ulaşabilmek için *Başlat→Denetim Masası→ Windows Güvenlik Duvarı -->Gelişmiş Ayarlar* seçilerek gelişmiş güvenlik duvarı ayarlarına erişilir. Gelişmiş güvenlik duvarı ayarlarında hem dışarıdan içeriye giden hem de içeriden dışarıya çıkan trafik kontrol edilebilir. İstenilen haberleşme ihtiyacına göre kurallar girilerek içeriye giriş yanında dışarıya çıkış da kontrol altına alınır.

Güvenlik duvarında *gelişmiş* seçeneği hangi ağın korunacağının belirlenmesini sağlar. Çünkü bir bilgisayarda dış dünyaya bağlantı sağlayan birçok arayüz (Ethernet, kablosuz 802.11 vb.) olabilir. Şekil 18'da güvenlik duvarı *gelişmiş* ayarları görülmektedir. *Varsyılanı yükle* seçeneği yaptığınız ayarların tamamını ortadan kaldırır.



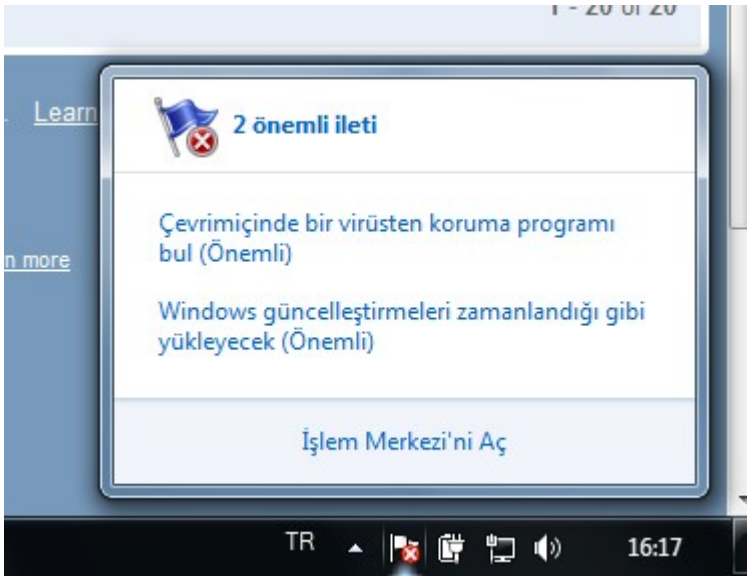
Şekil 18 Gelişmiş güvenlik duvarı ayarları

2.9.3 Zararlı Yazılımlara Karşı Korunma (Antivirüs)

Virüsler, solucanlar, casus yazılımlar ve diğer olası istenmeyen yazılımlar gibi zararlı yazılımlar, kişisel bilgilerin çalınması, kişisel bilgisayar performansının düşmesi ve istenmeyen reklamların (açılır reklamlar gibi) görüntülenmesi gibi çeşitli sorunlara neden olabilir. Zararlı yazılımların, yalnızca can sıkıcı içerikten zaman ve maddi kaynak kaybına neden olan önemli sorunlara kadar farklı etkileri olabilir.

Antivirüs programları, zararlı yazılımlara karşı koruma sağlamakta kullanılan en etkili kontrol mekanizmasıdır. Antivirüs programları, işletim sistemlerini, uygulamaları ve kullanıcının dosyalarını korur. Bu nedenle her bilgisayar kullanıcısı mutlaka bir antivirüs yazılımı kullanmalı ve antivürüs programını düzenli olarak güncellemelidir.

Bilgisayarda bir antivirüs programı olmaması durumunda Windows 7 işletim sistemi Şekil 19'deki gibi bir uyarı verir.



Şekil 19 Antivirüs uyarısı

2.9.4 Casus ve Diğer Zararlı Yazılım Koruma

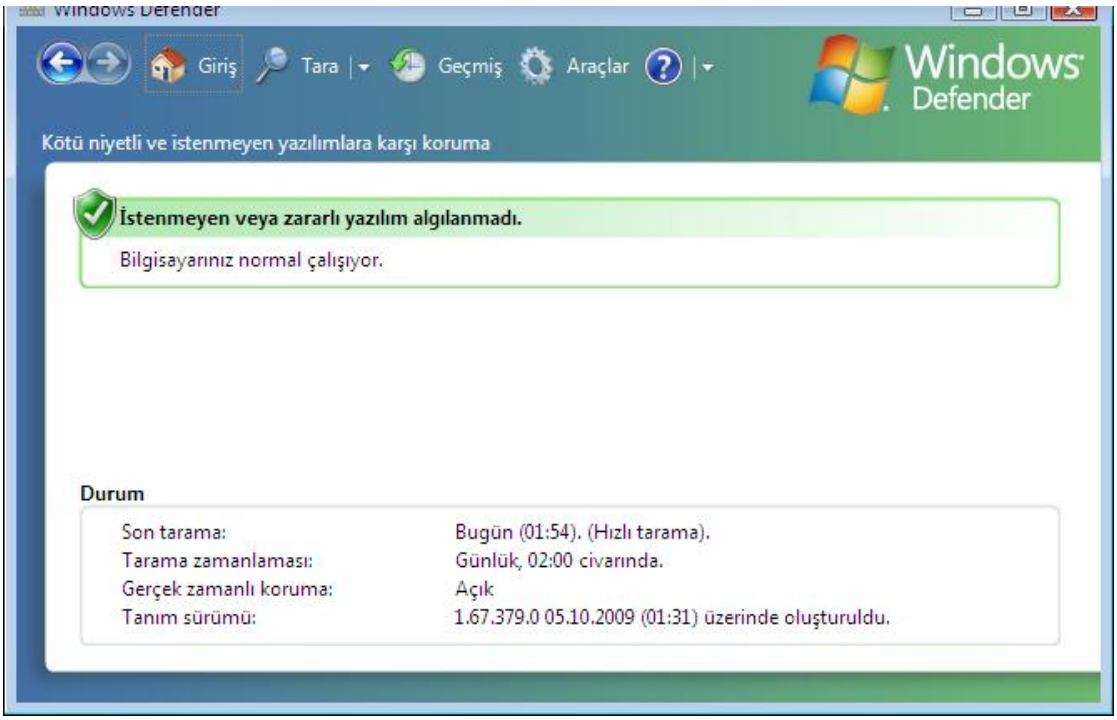
Microsoft Vista ile gelen ve Windows 7'de de bulunan yeni Defender aracı casus programları ve zararlı yazılımları tespit edebilir. Defender'in etkinleştirilmesini ve güncelliği güvenlik merkezinden kontrol edilebilir.

Bilgisayara casus program yükleyerek ya da zararlı yazılımlar çalıştırılarak bilgisayarda bulunan parola, kullanıcı bilgileri, kullanıcı özel dosyaları gibi bilgilerin çalınması ya da bilgisayarlarının kaynaklarının kötüye kullanılması atakları gerçekleştirilmektedir. Bu tür atakların önüne geçilmesi için Windows XP'ye seçenekli olarak yüklenen Defender programı Windows 7 ile birlikte gelmektedir. Defender programı bilgisayarda otomatik olarak güncellenip bilgisayarda sürekli olarak çalışarak zararlı yazılımları engellemektedir. Otomatik çalışma yanında Defender programı istenildiğinde de çalıştırılarak zararlı yazılımların tespiti yapılabilmektedir.

Başlat->Programlar->Microsoft Defender linki kullanılarak Defender programı çalıştırılabilir. Microsoft Defender çalıştırıldığında Şekil 20'deki arayüz görülür.

Tara: Kullanıcı istediği zaman zararlı yazılım arama işlemini başlatır.

Gelişmiş: Bilgisayara erişim izini verilen ve karantinaya alınan öğeleri gösterir.



Şekil 20 Windows Defeder programı arayüzü

Araçlar: Microsoft Defender'e ait araç ve ayarları gösterir. Şekil 21'de araç ve ayarlar gözükmektedir.

Seçanekler: Microsoft Defender'in periyodik otomatik taramayı ne zaman başlatacağı buradan ayarlanır.

Microsoft SpyNet: İstenilmesi durumunda bilgisayarınızdaki şüpheli aktiviteleri Micosoft'a bildiri. Size ait kişisel bilgileri de iletme riski vardı. Kullanıcının diğer zararlı yazılımlar hakkında bilgi almasını sağlar.

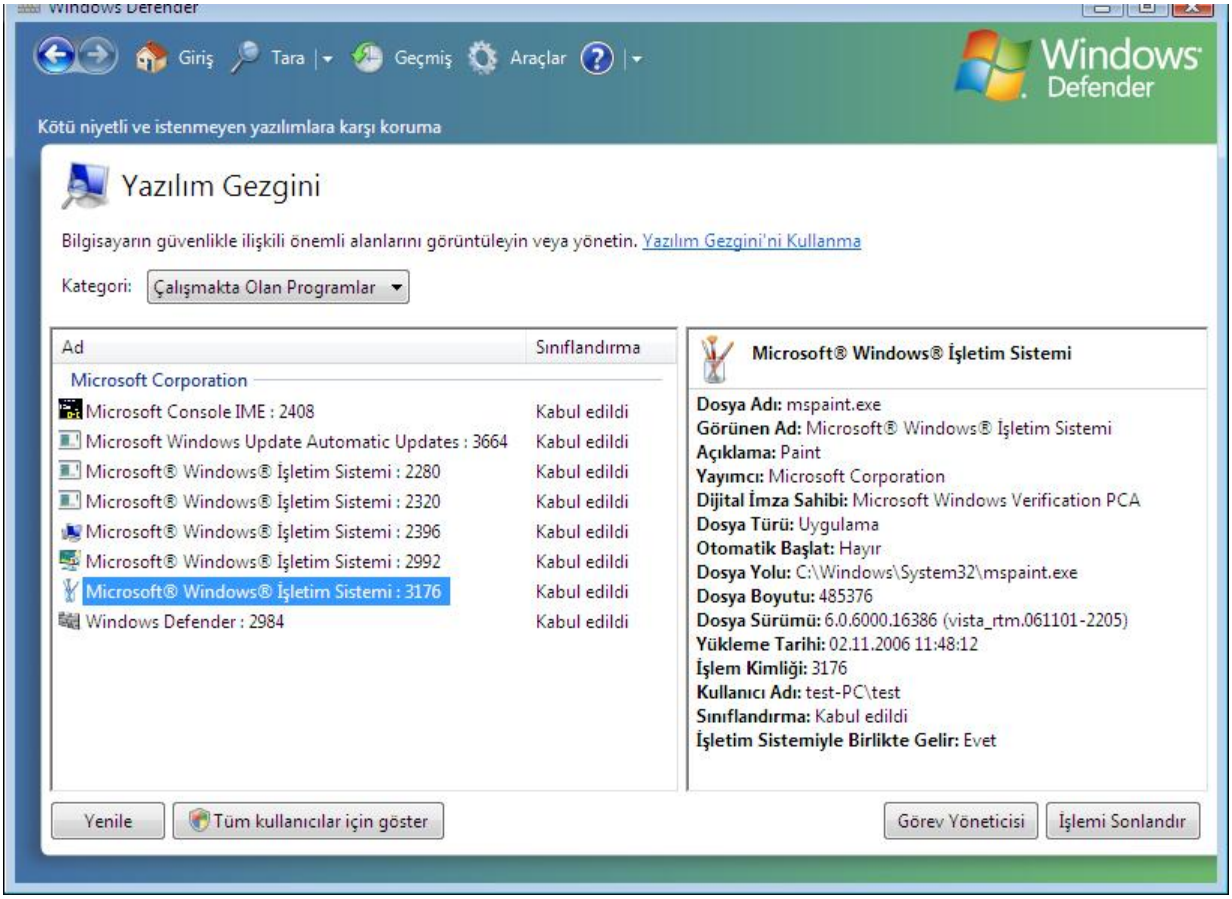
Karantinaya Alınan Öğeler: Karantinaya alınan öğeleri gösterir. Bu programları çalışması için geri yükleye bilirsiniz ya da tamamen bilgisayarınızdan kaldırabilirsiniz. Karantinaya alınmış program çalışmaz.

İzin verilen Öğeler: İzin verilen öğeleri gösterir. Defender bu programların izlemesini yapmaz.

Yazılım Gezgini: Bilgisayarda çalışan servisleri ve o servislere ait bilgileri gösterir. Çoğu zaman bilgisayardaki çalışan program ve servislerin hangi üretici tarafından üretildiği, hangi exe dosyasını kullandığı, hangi dizinde yer aldığı gibi önemli bilgileri bilemeyiz. Bu araç çalışan her bir program ve servise ait bu ayrıntılı bilgileri gösterir. Bunu sonucunda çalışan program veya servis zararlı veya gereksiz ise kullanıcı bu program veya servisi silebilir.

Şekil 21 Araç ve ayarlar

Şekil 22'de bilgisayarda çalışan servis ve programlara ait bilgiler görülmektedir. Sol çerçevede bulunan servislerden hangisi seçilirse ona ait bilgiler sağ çerçevede görülür. Bu bilgiler yorumlanarak programın zararlı veya gereksiz olup olmadığına karar verilebilir. Örneğin sol tarafta seçilen programın mspaint.exe olduğu, Microsoft Corporation tarafından üretildiği c:\windows\system32\ dizininde bulunduğu, uygulama türü bir program olduğu bilgileri görülmektedir. Burada özellikle programın imzalı olup olmadığı büyük önem taşımaktadır. İmzalı bir programsa Microsoft tarafından test edildiği zararlı içerik içermediği anlamına gelir.



Şekil 22 Bilgisayarda çalışan servis ve programlara ait bilgiler

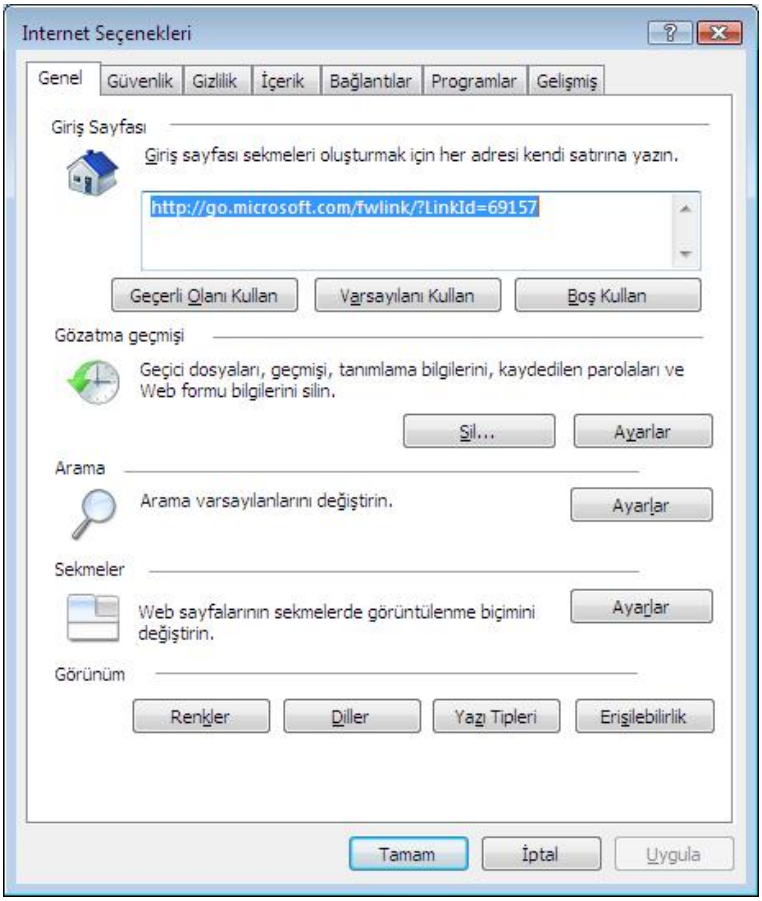
2.9.5 İnternet Güvenlik Ayarları

Windows 7 ile gelen işlem merkezi Internet Explorer 7 web tarayıcısının güvenli olarak yapılandırılmasını sağlar. Eğer Internet Explorer web tarayıcısının güvenlik ayarları değiştirilirse güvenlik merkezi sürekli kullanıcıyı uyarır.

Web tarayıcı güvenliği ayarlanırken dengeli bir koruma ayarı yapılmalıdır. Fazla kısıtlama konulursa, internetin aktif bir şekilde kullanılamaması, az kısıtlama yapılırsa internetten indirilen zararlı yazılım ve içeriklerin kullanıcı bilgisayarına ve verilerine büyük oranda zarar vermesi söz konusu olacaktır.

Internet Explorer'ın sunduğu *varsayılan güvenlik seviyeleri* özel bir durum için gerekmiyorsa düşürülmemelidir. Bir güvenlik ayarı değiştiriliyorsa da nedeni ve oluşturacağı güvenlik riskleri bilinmelidir.

Internet tarayıcı güvenlik ayarlarını yapabilmek için; internet explorer araçlar menüsünden, internet seçeneklerine tıklanır. Açılan ekrandan güvenlik sekmesi açılır. Güvenlik sekmesinde *Güvenilen Siteler* ve *Yasaklanan Siteler* seçenekleri kullanılarak güvenilen ve yasaklanan siteler ayrıca eklenebilir. Yasaklana Siteler zararlı olduğunu bildiğiniz halde güvenlik yazılımları tarafından tespit edilmeyen sitelere karşı koruma sağlar. İzin verilen sisteler ise güvenli olduğunu bildiğimiz halde güvenlik yazılımları tarafından zararlı olarak tespit edilen sitelerin İlgili siteyi buraya ekleyerek koruma sağlayabilirisiniz.



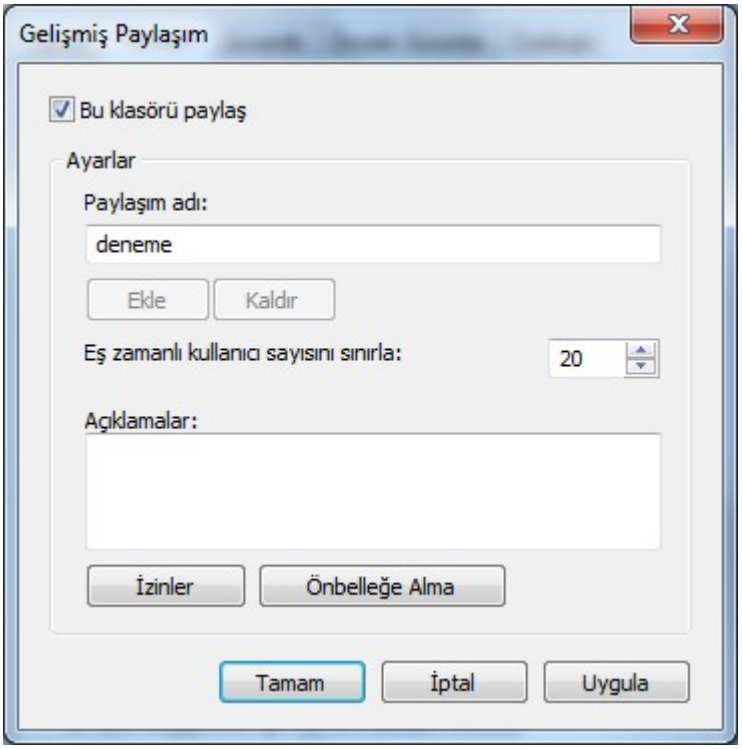
Şekil 23 Varsayılan ayar

Ayrıca, pop up pencerelerinin çıkmaması için pop up koruma açık olmalıdır. Bu işlemi yapmak için *Araçlar-> Açılır pencere engelleyicisi-> Açılır pencere* seçeneğini aç durumunda olmalıdır.

İnternet tarayıcınızı düzenli olarak güncellemeli ve gereksiz yere güvenliği varsayılan ayarlardan daha aşağı düşürmemelisiniz.

2.10 Dosya Paylaşımı ve Erişim İzinleri Yapılandırması

Dosya paylaşımında paylaşılacak dosya üzerinde sağa tıklanır *özellikler* → *Paylaşım* → *Gelişmiş paylaşım* seçeneğine girilir. Buradan "Bu klasörü paylaş" seçeneği işaretlenir ve klasör paylaşıma açılır.



Şekil 24 Paylaşım

Klasör paylaştırma penceresinden izinler düğmesine tıklanır ve buradan paylaşım izinleri ayarlanır. Paylaşım izinleri, paylaştırılmış klasöre hangi kullanıcıların erişilebileceğini belirler. Her bir kullanıcının üzerine tıklanarak hangi haklara sahip olduğu hem görülebilir hem de ayarlanabilir.

Verilen İzinler Şunlardır: Tam Denetim, Değiştir, Okuma ve Yürütme, Klasör İçeriğini Listele, Oku, Yaz, Özel İzinler.

NTFS dosya izinleri

Oku (Read): Okuma izni verir.

Yaz (Write): Yazma izni verir.

Okuma ve Yürütme (Read and Execute): Okuma ve çalıştırabilme izni verir.

Değiştir (Modify): Okuma, yazma ve çalıştırabilme iznini kapsar.

Tam Denetim (Full Control): Tüm izinleri kapsar.

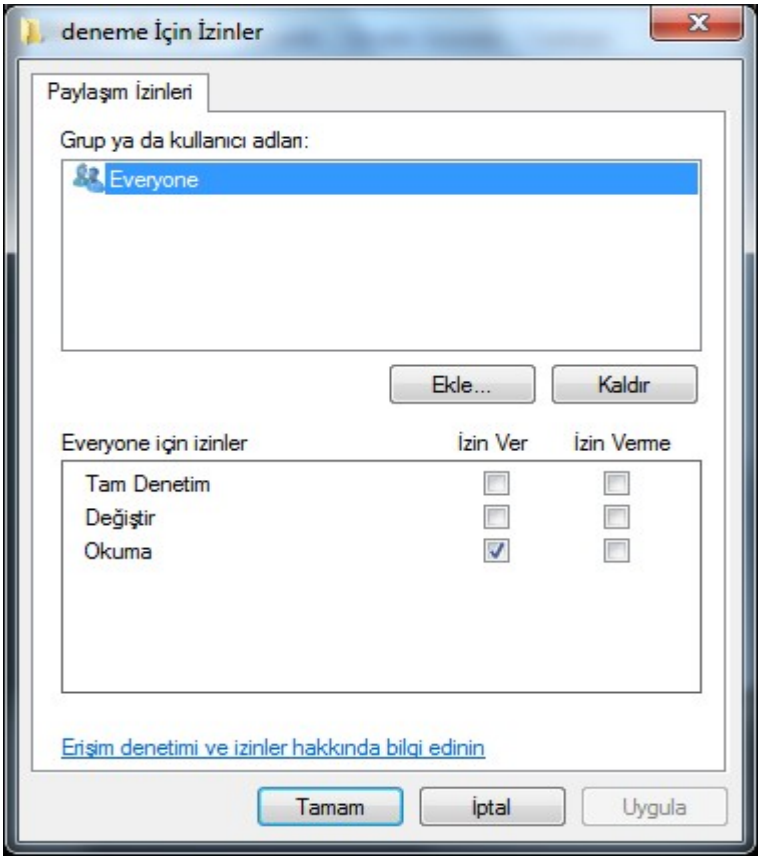
Klasör izinlerinde ise diğer izinlerden farklı olarak;

List folder contents: Klasörün altındaki diğer klasör ve dosyaları listeler.

Paylaşım verildikten sonra istenilen kullanıcıya dizin veya dosya üzerinde kendi işlerini halledebileceği minimum haklar verilmelidir. Örneğin kullanıcının bir dizinden sadece dosyayı alması gerekiyorsa sadece okuma hakkı verilmelidir.

Bu haklar FAT32'ye göre daha güvenli olan NTFS dosya sisteminde verilebilir.

Şekil 25'da dizin için verilebilecek haklar görülmektedir.



Şekil 26 Erişim İzinler

Bir kullanıcının bir dosya ya da dizine erişimi engellenmişse Şekil 27'deki mesaj alınır.

Şekil 27 Erişim engellendi mesajı

2.11 Olayların Günlük Kayıtlarının Alınması (Event Log)

Olaylar (events) Microsoft Windows 7 işletim sistemi için çok önemli olan kullanıcı aktiviteleri veya uygulama aktivitelerinin kaydedilmesidir. Sistem ve uygulama olaylarının görüntülenmesi kaynak kullanımını, sistem ve uygulama hatalarını takip etmek için kullanılır. Microsoft Windows 7 tarafından otomatik olarak ayarlanan sistem olayları sistem kayıtlarında (system log) tutulur. Uygulama geliştiricisi tarafından belirlenen uygulama olayları (application events) uygulama kayıtlarında (application log) saklanır. Olaylar bu kayıtlara geçtikten sonra bunlar analiz edilebilir ve bunlara göre sistem problemleri ortaya çıkarılabilir.

Microsoft Windows 7 üç değişik tipte kayıt tutar:

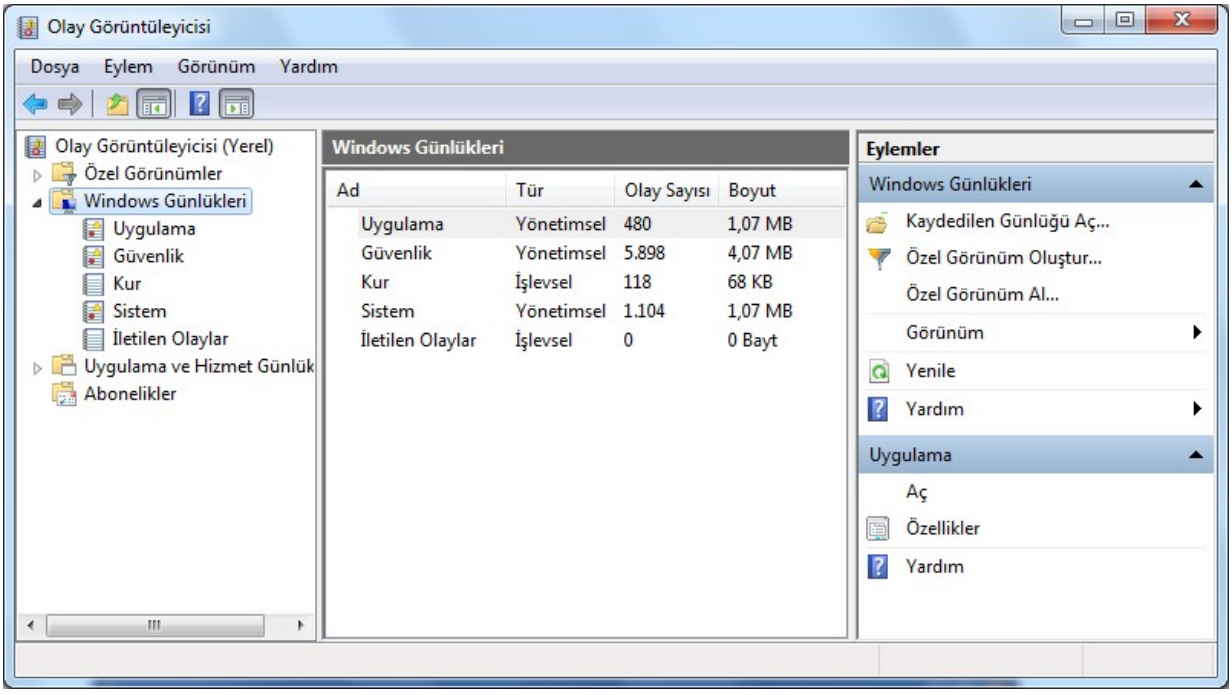
Uygulama kayıtları (application log) : Bu kayıt türü uygulamalar çalışırken meydana gelen olayların kayıtlarını içerir. Örneğin; bir veritabanı programına ait dosya hataları bu kayıtlar arasında yer alır. Program geliştirici hangi olayların kayıtlarının tutulacağına karar verir. Dr.Watson uygulamaları da bu kayıt tipinde görülebilir. Dr.Watson hata ayıklayıcı bir programdır. Herhangi bir uygulamada bir program hatası oluşursa Dr.Watson bununla ilgili Drwtsn32.log isimli bir kayıt tutar.

Güvenlik kayıtları (security log) : Bu kayıt türü bilgisayarda güvenlik ile ilgili kayıtları tutar. Bu türdeki kayıtlara örnek olarak başarılı veya başarısız oturum açma denemeleri, herhangi bir dosya oluşturma, açma veya silme gibi kaynak kullanımı ile ilgili olaylar verilebilir. Bilgisayarın yöneticisi hangi olayların kayıtlarının tutulacağına karar verir. Mesela yönetici oturum açma denemelerine izleme (audit) yapılandırılsa tüm oturum açma denemeleri bu kayıtların içinde görülecektir.

Sistem kayıtları (system log) : Bu kayıt türü Microsoft Windows 7 İşletim Sistemi'nin sistem bileşenleri içindeki olayları içerir. Örnek olarak bir sürücünün veya başka bir sistem bileşeninin açılış sırasında yüklenmemesi sistem kayıtlarında bir olay olarak görülür.

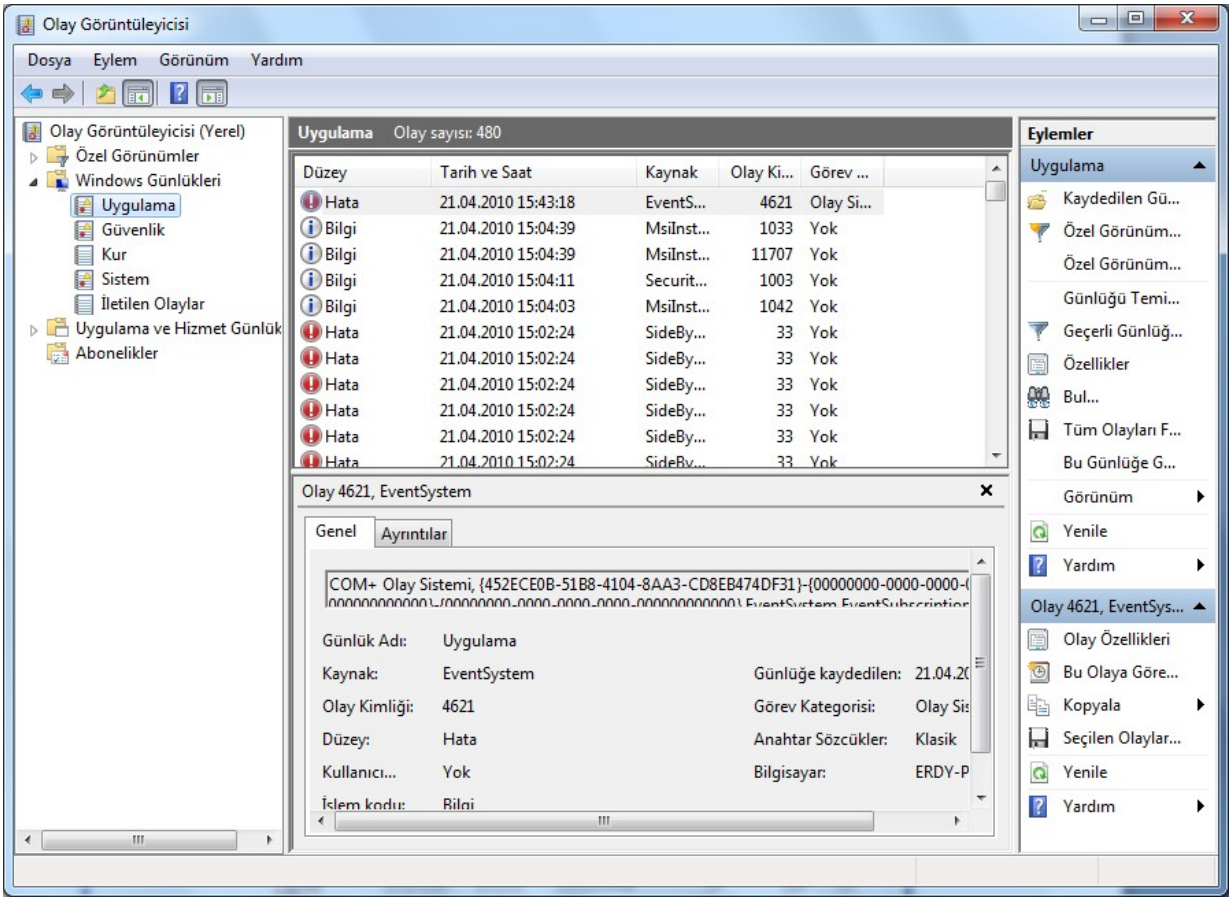
Olay görüntüleme aracında olayları incelemek için;

Denetim Masası →Yönetimsel Araçlar →Olay Görüntüleyicisi tıklanır.



Şekil 28 Olay kayıtları

Her olayın bir kimlik numarası vardır. Olayın numarasına http://www.eventid.net/ adresinden bakılarak olay ile ilgili bilgi alınabilir.



Şekil 29 Uygulama olayları

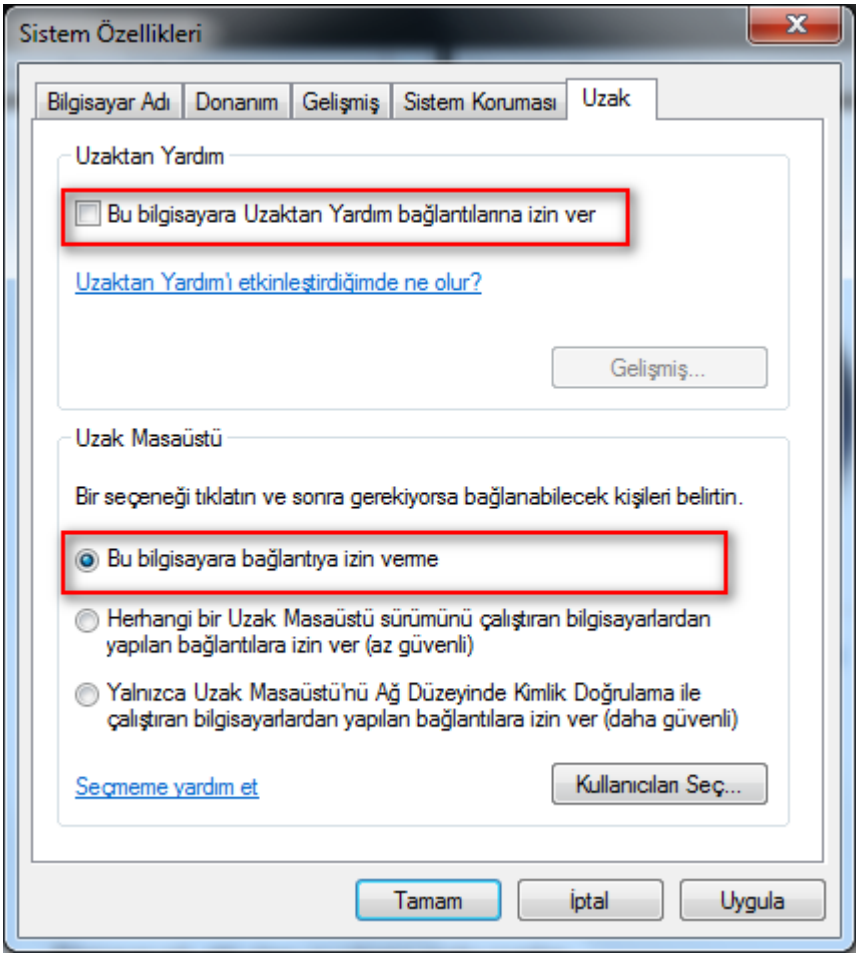
2.12 Uzaktan Erişim

Uzaktan yardım, ağ bağlantısının olduğu herhangi bir yerden (LAN, WAN, İnternet) yardım almak ve masaüstünün bağlantı kurulan kişiye transfer edilmesi ile sorunlara uzaktan çözüm bulunmasını sağlar.

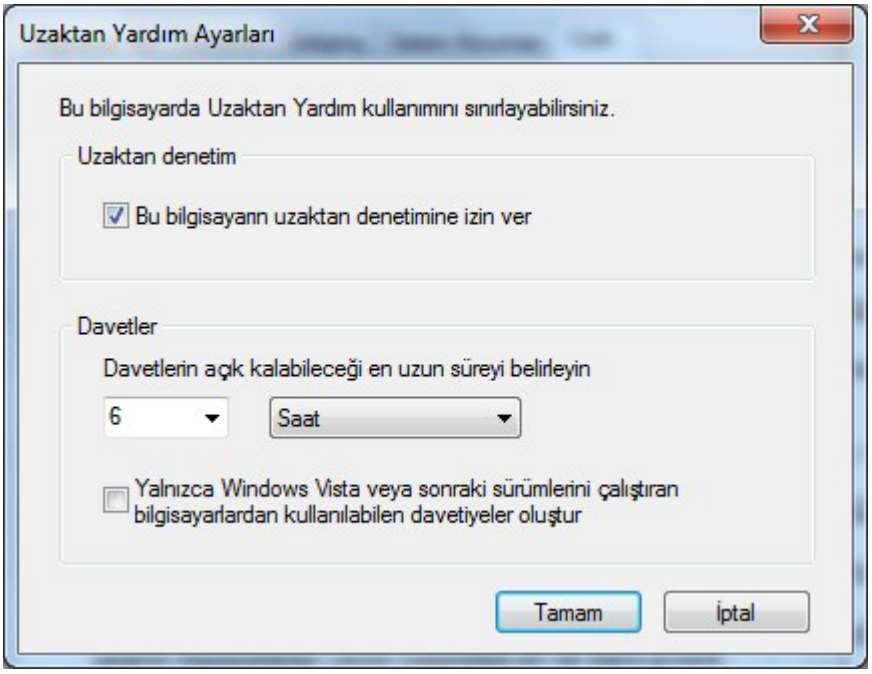
Bilgisayarda oluşan bir hatanın nedeni bilinmiyorsa ve o an için bu sorun ile ilgilenecek kimse yoksa uzaktan yardım yöntemi ile ağ ya da internet bağlantısı üzerinden yardım edecek biri bilgisayara bağlanabilir. Kontrol bilgisayar sahibinde olmak şartıyla klavye ve mouse hareketlerinin uzaktan kontrol edilmesi sağlanabilir.

Uzak masaüstü özelliği sayesinde ağ üzerindeki başka bir bilgisayardan kullanıcı kendi masaüstüne erişebilir. Buna ek olarak masaüstüne ulaşıldığında tüm uygulamalar çalıştırılabilir, kullanıcı kendi bilgisayarında oturuyormuş gibi dosya ve klasörlere erişebilir. Bilgisayara uzaktan erişirken bilgisayarı kimsenin yerel olarak kullanmaması gerekmektedir.

Uzaktan yardıma izin vermek için; bilgisayarım ikonu üzerine gelinerek sağ tuşa tıklanır ve özellikler seçilir. Sistem özelliklerinden *uzak bağlantı ayarları* linki tıklanır. Uzaktan yardım için; "*bu bilgisayara kullanıcıların uzaktan bağlanmasına izin ver*" (Allow remote assistance invitations to be sent from this computer) seçeneği aktif hale getirilir.



Şekil 30 Uzak sekmesi



Şekil 31 Uzaktan yardım ayarları

Uzak masaüstü bağlantısı için; Kullanıcıların "*herhangi bir uzak masaüstü sürümünü çalıştıran bilgisayardan yapılan bağlantılara izin ver (az güvenli)*" onay kutusu işaretlenir. Uzak masa üstü için "uzak kullanıcıları seç" butonuna tıklanır ve bağlanmasına izin verilecek kullanıcı seçilir. Bilgisayar yöneticisi listede olmasa bile bağlanabilir. Bunun dışında kullanıcılar varsa ekleme işlemi yapılmalıdır.

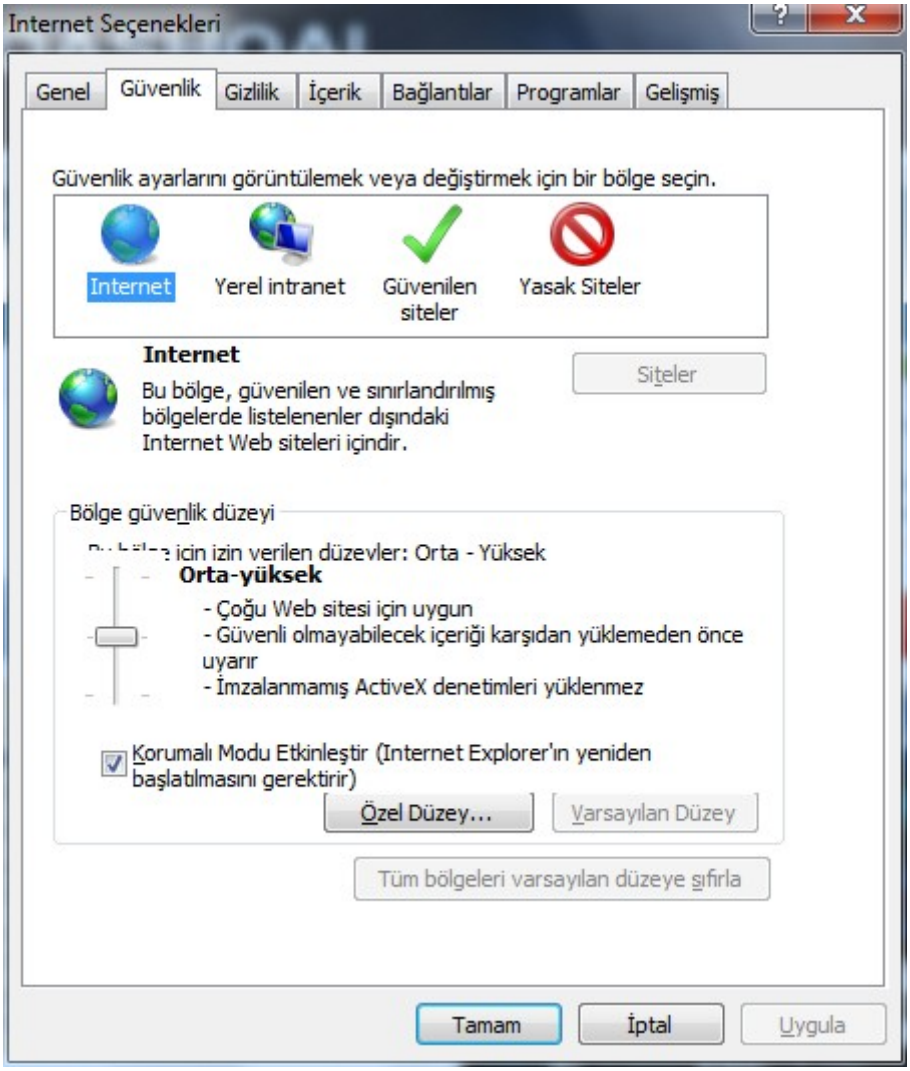
Bilgisayar güvenliğini arttırmak için, eğer gerekmiyorsa uzaktan erişime izin verilmemelidir. Ama kullanılması gerekli ise tüm uzak masaüstü kullanıcılarının zor kırılabilecek bir şifreye sahip olmaları gerekir. Eğer bilgisayar kablolu modem veya ADSL bağlantısı ile internete çıkıyorsa şifrenin düzeyi daha da fazla önem kazanır. Zor şifreler en az sekiz karakterden oluşan, büyük harf, küçük harf ve özel karakterleri (?,!,',^,%, vb...) içeren şifrelerdir.

2.13 Internet Tarayıcısı Ayarları

Web tarayıcı güvenliği sağlanırken dengeli bir koruma sağlanmalıdır. Fazla kısıtlama konulursa, internetin aktif bir şekilde kullanılamaması,. az kısıtlama yapılırsa internetten indirilen zararlı yazılım ve içeriklerin kullanıcı bilgisayarına ve verilerine büyük oranda zarar vermesi söz konusu olacaktır.

Internet Explorer'ın sunduğu varsayılan güvenlik seviyeleri özel bir durum için gerekmiyorsa düşürülmemelidir. Bir güvenlik ayarı değiştiriliyorsa da nedeni ve oluşturacağı güvenlik riskleri bilinmelidir.

Internet tarayıcı güvenlik ayarlarını yapabilmek için; internet explorer araçlar menüsünden, internet seçeneklerine tıklanır. Açılan ekrandan güvenlik sekmesi açılır. Burada internet, yerel intranet, güvenli ve yasaklanmış siteler seçenekleri görülür. Bütün siteler varsayılan olarak internet sitesi olduğu için buraya site eklenemez.



Şekil 32 Varsayılan ayar

Ayrıca, pop up pencerelerinin çıkmaması için pop up koruma açık olmalıdır. Bu işlemi yapmak için *Araçlar-> Açılır pencere engelleyicisi-> Açılır pencere* seçeneğini aç durumunda olmalıdır.

2.14 Windows 7 Ebeveyn Kontrolü

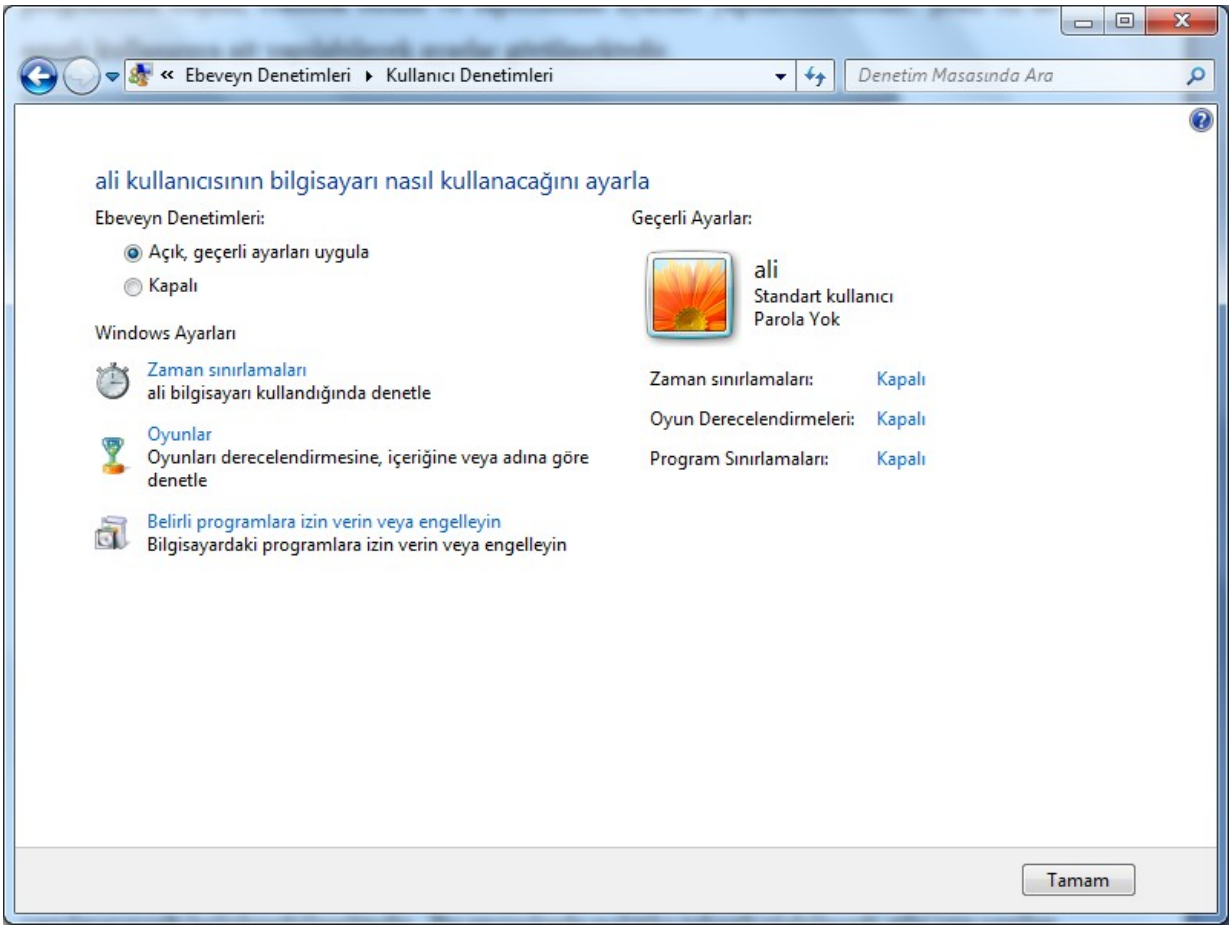
Ebeveyn kontrolü, çocuklarınızın veya bilgisayar ortamında kontrollü olarak çalışmasını istediğinizi kişilerin bilgisayar kaynaklarına ve internete sınırlı yetkilerle erişmesini sağlayan ve bu erişimleri size raporlayan güvenlik aracıdır.

Ebeveyn kontrolü etkinleştirebilmek için bilgisayar yöneticisi (Administrator) sınırlı yetkilere sahip bir kullanıcı yaratmalıdır. Daha sonra yönetici kısıtlı yetkilere sahip kullanıcının bilgisayar üzerindeki erişim haklarını ebeveyn kontrolü aracı ile kontrol edebilir. Eğer bilgisayarda sınırlı haklara sahip kullanıcı yoksa *Başlat->Denetim Masası->Kullanıcılar* ikonu kullanılarak sınırlı haklara sahip kullanıcı yaratılabilir. Eğer kullanıcı varsa ona ait haklar sınırlanabilir.

Ebeveyn kontrolü *Başlat->Denetim Masası->Ebeveyn* Kontrolü ikonuna tıklanarak çalıştırılır. Çalıştırıldığında bilgisayarda tanımlı olan kullanıcılar görülür. Şekil 33'de bilgisayarda tanımlı kullanıcılar görülmektedir.

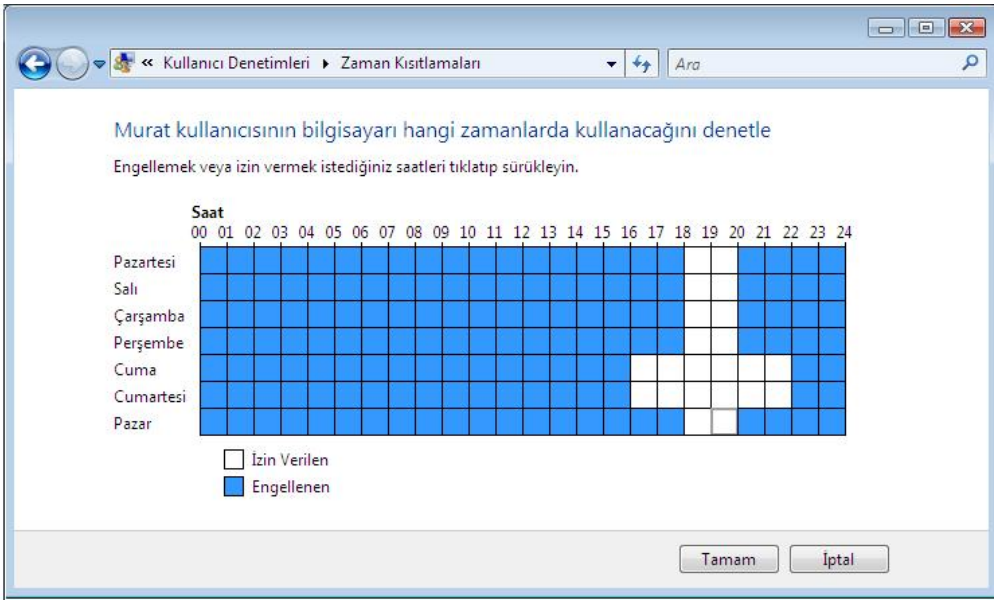
Şekil 33 Bilgisayarda tanımlı kullanıcılar

Örneğin burada Murat isimli kullanıcı seçerek ona ait hakları sınırlamak isteyelim. Murat kullanıcısını seçip iki defa tıkladığımızda ona ait sınırlama ekranı gelir ve gerekli sınırlamaları yapabiliriz. Bu kullanıcı ile ilgili web kullanımı, oyun kullanımı, zaman sınırlaması, belli programlara erişim, etkinlik birimi ve raporlaması ayarları yapılabilmektedir. Şekil 34'de sınırlı kullanıcıya ait yapılabilecek ayarlar görülmektedir.



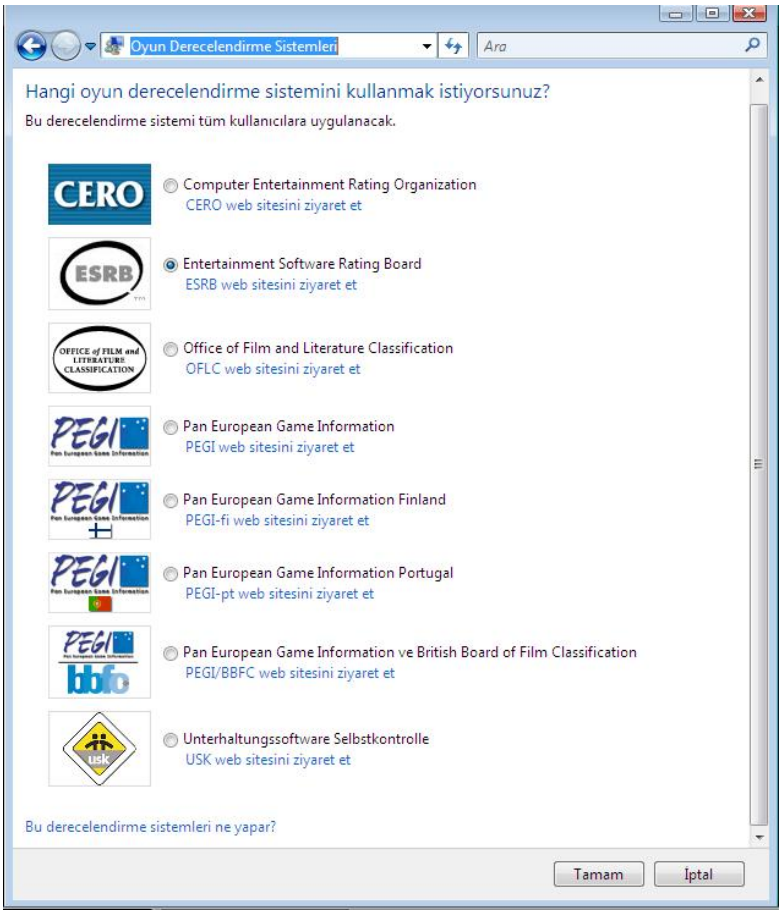
Şekil 34 Sınırlı kullanıcı ayarları

Zaman Sınırlamaları: Sınırlı yetkilere sahip kullanıcının hangi saatlerde bilgisayara login olabileceği tanımlanabilir. Bu grafikte beyaz kısımlar izin verilen saatleri mavi kısımlar ise izin verilmeye saatleri göstermektedir. Mouse tıklayarak istediğiniz saati mavi ya da beyaz yapabilirsiniz. Şekil 35'de zaman kısıtlaması görülmektedir.



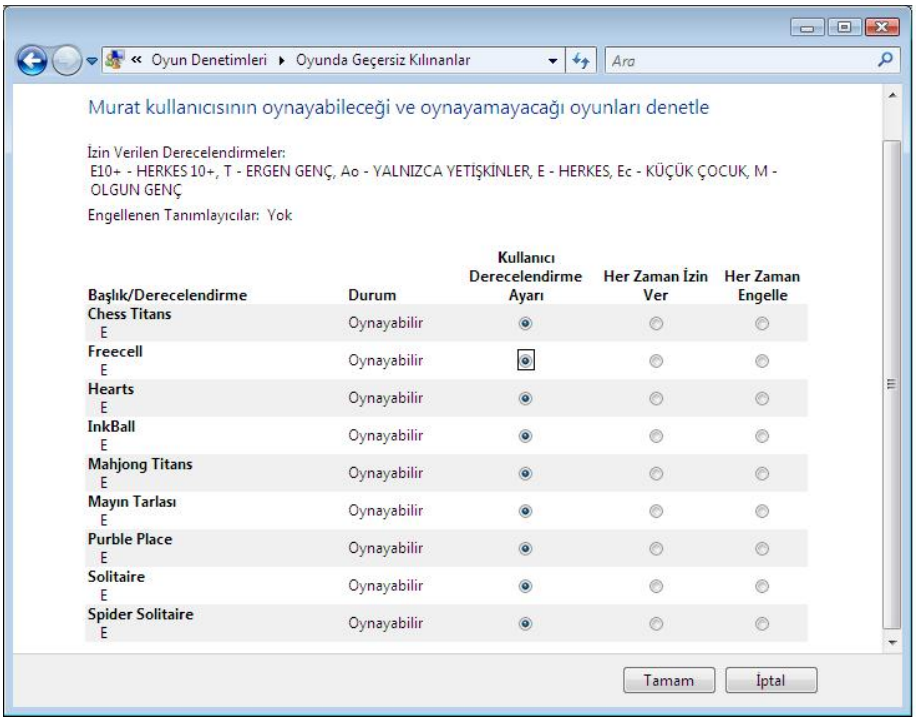
Şekil 35 Zaman kontrolü

Oyunlar: İnternet üzerinden oyun oynanıp oynanmayacağını ve bilgisayarda bulunan oyunlara erişimi kontrol eder.



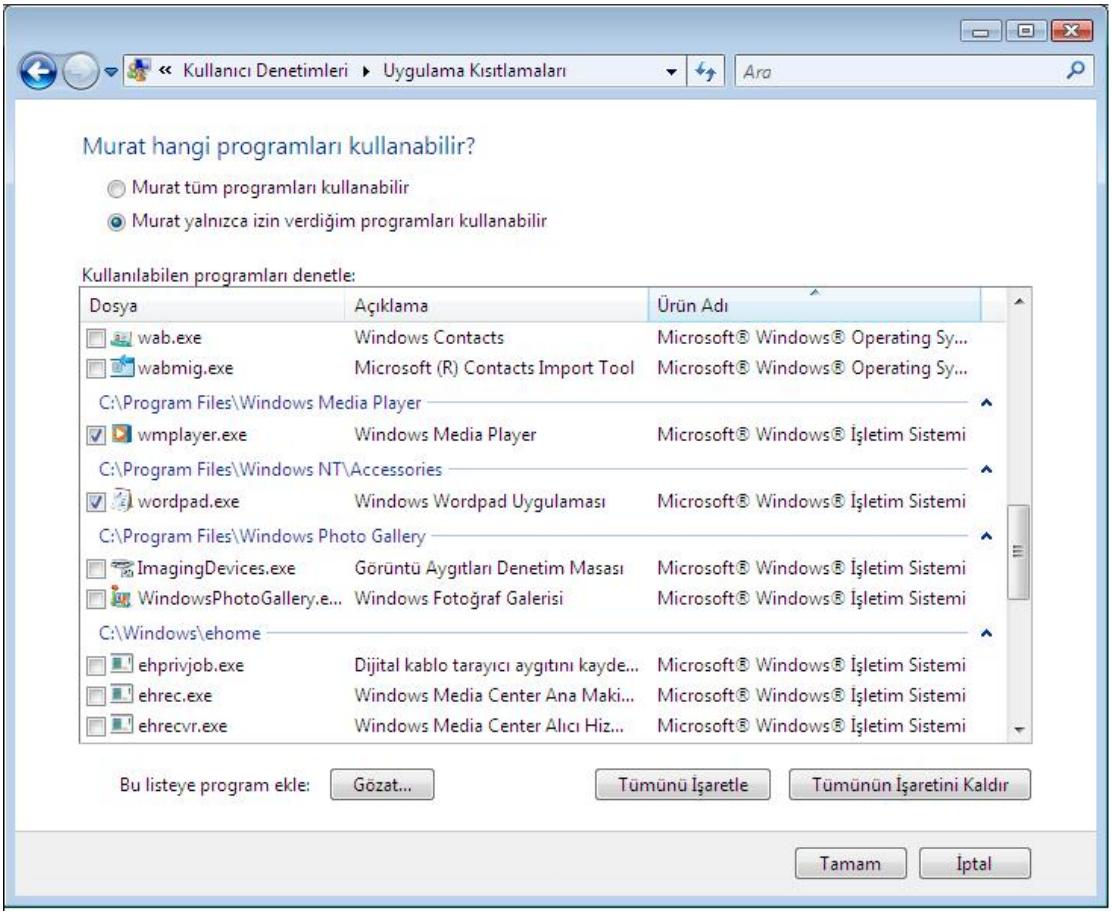
Şekil 36 Oyun derecelendirme siteleri

Eğer oyun oynanabilir seçilirse bağlanacak siteler belirlenir. Hangi oyun sitelerine bağlanabileceği tanımlanır. ESRB (Entertainment Software Rating Board) içeriğe, yaşa göre oyun değerlendirme sitesidir. ESRB seçilirse sınırlı yetkili kullanıcı için oradan bir seviye seçilebilir. İnternet üzerindeki oyunlar yanında bilgisayar üzerindeki oyunlara erişim de denetlenebilir. Şekil 37'de bilgisayardaki oyunlara erişim arayüz görülmektedir.



Şekil 37 Oyun kontrolü

Belli programlara izin verilmesi veya engellenmesi: Sınırlı kullanıcının bilgisayar kaynaklarına erişimini denetleyen en önemli araçlardan biri "Programlara İzin Verin veya Engelleyin" seçeneğidir. Bu arayüzle sınırlı kullanıcının hangi programlara erişebileceği kolay bir şekilde seçilebilir. Şekil 38'de kullanıcı program kontrol arayüzü görülmektedir.



Şekil 38 Kullanıcı program kontrolü

Etkinlik Raporları

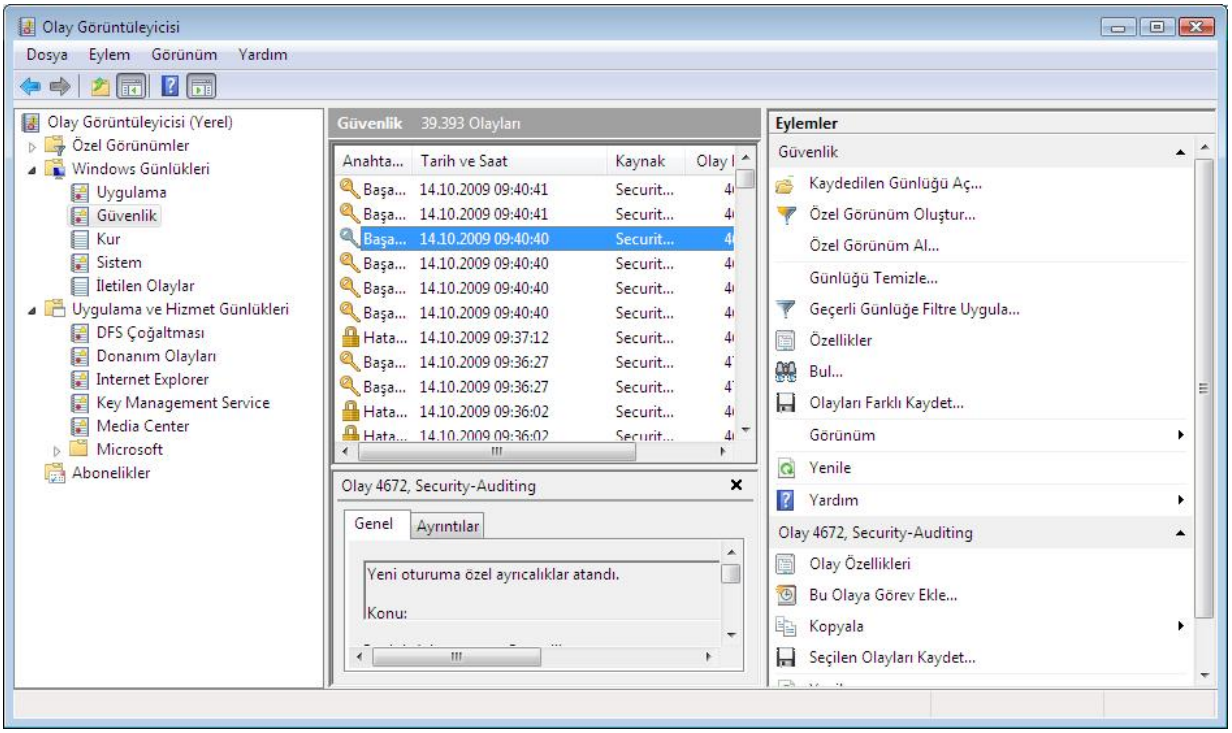
Sınırlı yetkilere sahip kullanıcıların yapmış oldukları aktiviteler, ebeveyn kontrolü açılıp ilgili kullanıcı seçildikten sonra gelen ekranda Etkinlik Raporlarını Görüntüle seçeneği seçilerek kullanıcıya ait aktiviteler görüntülenebilir.

2.15 Olayların Günlük Kayıtlarının Alınması (Event Log)

Olay Günlükleri Microsoft Windows 7 işletim sistemi için önemli olan kullanıcı veya uygulama aktivitelerinin kaydedilmesini ve sonradan incelenmesini sağlayan bir servistir. Uygulama, güvenlik, kurulum, sistem, iletilen olaylar, uygulama/hizmetlere ait günlükler ve aboneliklere ait kayıtları tutar. Bilgisayarda bu alanlarda olay olması durumunda onları kaydeder ve sonradan kullanıcının bu kayıtlara bakarak işletim sistemindeki olay ya da problemi yönetmesini sağlar. Abonelikler seçeneği uzaktaki bir veya daha fazla bilgisayardaki istediğimiz olayları toplayıp incelememizi sağlar.

Olay görüntüleme aracında olayları incelemek için; *Denetim Masası→Yönetimsel Araçlar →Olay Görüntüleyicisi* tıklanır.

Microsoft 7 olay görüntüleyicisinin arayüzü Şekil 39'de görülmektedir.



Şekil 39 Olay görüntüleyicisi arayüzü

2.16 Bilgisayarda Meydana Gelen Güvenlik Olayının İncelenmesi

Kullanıcı bilgisayarında meydana gelen bir güvenlik olayının incelenmesi aşamasında ilk olarak bu olayın tespit edilmesi ve analiz edilmesi gerekir. Sistemde meydana gelen aksaklıklar doğrultusunda araştırma yapılmalıdır. Gerçekten sistemde yaşanan olayın güvenlik olayı olduğundan emin olunmalıdır. Sistemde güvenlik olayı olduğunun tipik belirtileri aşağıdaki gibidir:

- Bilgisayarın normalden daha yavaş çalışması
- İnternette bir yere bağlantı yapmamanıza karşın bilgisayarın ağ bağlantısının sürekli yanıp sönmesi

- Bilgisayarınızın kendi kendine kapanıp açılması ya da ekranda beklenmeyen mesajlar görmeniz
- Bilgisayarınız diskinin hızlı bir şekilde dolması
- Bilgisayarınızdaki bazı dosyaların kaybolması
- Bilgisayarınızda bulunan güvenlik duvarı, antivirüs programı, otomatik güncelleme gibi güvenliğe yönelik programların sizin bilginiz dışında kapatılmış olması

Eğer bilgisayarınızda bir güvenlik olayı olduğu düşünüyorsanız internetten ne olduğunu bilmediğiniz bir programla çözmeye çalışarak yeni bir ajan program yüklemek yerine ya önemli dosyaların yedeğini aldıktan sonra bilgisayarınızın işletim sistemini yeniden kurup yukarıda anlatılan güvenlik önlemlerini alarak kullanmalı ya da bilgisayar güvenliği konusunda hizmet veren bir firmadan ya da kişiden teknik destek almalısınız.

3. SONUÇ

Bilgisayar ağlarının yaygınlaşmaya başlamasıyla birlikte bilgisayar ağları üzerinde güvenlik olayları da görülmeye başlanmıştır. İlk zamanlarda görülen açıklıklar çoğunlukla bilgisayarlar arasında iletişimi sağlamak için kullanılan TCP/IP protokollerinden ve ürün geliştiricilerin yazılımları geliştirirken güvenlik için yeterli önlemi almamalarından kaynaklanmaktaydı. Fakat günümüzde hem TCP/IP protokollerinde hem de yazılım geliştirme yöntemlerinde güvenlik adına oldukça büyük iyileştirmeler yapılmıştır. Bu da bilgisayar iletişiminin önemli bir kısmının güvenli olmasını sağlamaktadır. Yeni çıkan ataklar ya da açıklıkların temelinde iki neden vardır:

Birincisi kullanıcıların, bilgisayar ya da modem gibi ağ iletişim cihazlarını yanlış ya da eksik yapılandırmalarıdır. Bunun sonucunda bilgisayar korsanları (Hacker) uzaktan modeme ya da bilgisayara erişerek bilgisayarı, modemi ya da kullanıcıya ait önemli dosyaları ele geçirebilmektedir. Eğer ele geçiremiyorsa internete erişimini engellemektedir.

İkincisi ise kullanıcıların güvenlik konusundaki bilgi eksikleridir. Kullanıcı bilgi eksiklikleri kullanılarak bilgisayarına başka bir programmış gibi gösterilerek zararlı yazılımlar yükletilmekte, sosyal mühendislik atakları kullanılarak bilgisayara, kullanıcıya, modeme ait önemli bilgiler kullanıcıdan doğrudan elde edilebilmektedir.

Yukarıda anlatılan bilgilerin büyük bir kısmı işletim sistemi tarafından bize sunulan güvenlik seçenekleridir. Bunları kullanarak güvenliği önemli derecede sağlayabiliriz, fakat sürekli yeni açıklıklar ve atak teknikleri çıkmaktadır. Bunlarla başa çıkmanın temel yolu bilgisayarı ve ağ cihazlarını her zaman güvenli olarak yapılandırmak, temel güvenlik yamalarını yapmak ve en önemlisi bilgisayar güvenliği konusunda bilinçli olmaktır.

KAYNAKÇA

[1] Windows 7 security Guide, http://www.microsoft.com

[2] Guide to Securing Microsoft Windows XP Systems for IT Professionals A NIST Security Configuration Checklist(Draft), NIST Special Publication 800-68 Revision I, July 2008

[3] Brain Livingston, Paul Thurrott, Windows Vista Secrets, Wiley Publishing, 2007

[4] http://www.pcworld.com/businesscenter/article/171979/a_guide_to_windows_7_security.html

[5] Microsoft Security Tech Center