XI. "Türkiye'de İnternet" Konferansı
TOBB Ekonomi ve Teknoloji Üniversitesi

KİŞİSEL BİLGİSAYARLAR VE İNTERNET GÜVENLİĞİ

Özgür ZEYDAN
Zonguldak Karaelmas Üniversitesi
Enformatik Bölümü
ozgurzeydan@yahoo.com

ÖZET

Son yıllarda ülkemizde kişisel bilgisayar fiyatlarının ve internet erişim maliyetlerinin ucuzlaması sayesinde bugün internet erişimi olan kişisel bilgisayarların sayısı sürekli artmaktadır. Bununla beraber savunmasız bilgisayarların internet ortamında maruz kalacağı tehlikeler de gün geçtikçe artmaktadır. Bu yazıda internet erişimi olan bir kişisel bilgisayarın karşılaşacağı tehlikeleri ve bunlara karşı alınması gereken oldukça basit fakat etkili yöntemleri açıklamaktır. Ülkemizde şu an için en çok kullanılan işletim sistemi olan Microsoft Windows XP'nin nasıl daha güvenli hale getirileceği de anlatılacaktır. Ayrıca internet ortamındaki her türlü tehlikeden korunmak için gerekli olan güvenlik yazılımlarından "kişisel kullanım için ücretsiz" olan birkaç tanesi önerilecektir.

ABSTRACT

The number of personal computers with internet connection has been increasing recently in our country as a result of decrease in personal computer prices and internet connection costs. At the same time, the threats for unprotected personal computers have been increasing. In this paper, the threats, which personal computer may encounter, and simple yet effective precautions for these threats will be explained. Also, improving the security of Microsoft Windows XP, nowadays the most widely used operating system in our country, will be discussed. Moreover, some "freeware licensed" security software will be recommended in order to protect personal computer for internet threats.

Anahtar Kelimeler: kişisel bilgisayar, internet güvenliği, Windows XP, ücretsiz güvenlik yazılımları

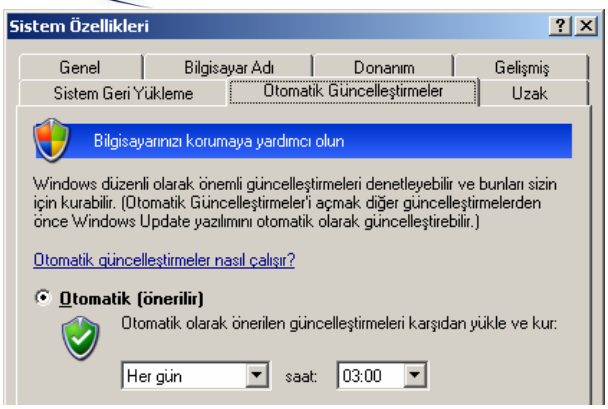
1. GİRİŞ

İnternet erişimi olan kişisel bilgisayarların karşılaşacağı olası tehlikeler şunlardır:

- İşletim sistemi açıkları
- Kullanıcı hesapları açıkları
- Paylaşımlar ve hizmetler
- Web tarayıcılarının açıkları
- Güvensiz yazılımlar ve casus yazılımlar
- Ağ ve internet üzerinden gelebilecek tehlikeler: virüsler, solucanlar, truva atları ve hacker saldırıları
- Tuş kaydediciler ve olta yöntemleri
- Numara çeviriciler
- Diğer olası tehlikeler

2. İŞLETİM SİSTEMİ AÇIKLARI

Her işletim sisteminde mutlaka açık kodlar vardır. Üretici firma bu açıkları fark ettiğinde kendi web sitesinde yama ve güncelleme dosyaları yayınlar. Microsoft Windows XP işletim sisteminin açıklarını kapatmak için http://windowsupdate.microsoft.com web sitesi ziyaret edilmeli ve buradaki açıklamalar takip edilmelidir [1]. Hackerların en son yayınlanan yama ve güncellemeleri takip ederek güncel olmayan bilgisayarlara saldırdıkları unutulmamalı ve bu nedenle "Otomatik Güncellemeler" mutlaka etkin olmalıdır. Otomatik güncelleştirmeleri etkinleştirmek için *Denetim Masası => Sistem Özellikleri => Otomatik Güncelleştirmeler* yolu izlenmelidir (Şekil–1). Ayrıca işletim sistemi bilgisayara ilk defa yükleneceği zaman mutlaka en son güncellemeleri ve yamaları içeren servis paketinin bulunduğu CD ile yüklenmelidir.



Şekil–1: Otomatik Güncelleştirmeler

3. KULLANICI HESAPLARI AÇIKLARI

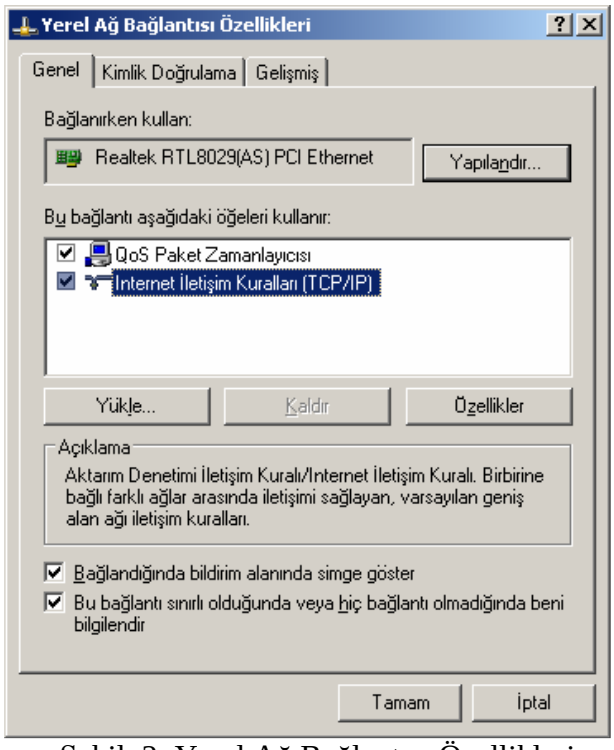
Microsoft Windows XP işletim sistemindeki gereksiz bütün kullanıcı hesapları silinmelidir [1]. *Denetim Masası => Kullanıcı Hesapları* yolunu izleyerek buradan yeni ve sınırlı yetkilere sahip olan bir kullanıcı tanımlamak ve interneti bu sınırlı kullanıcı hesabı ile kullanmak bizi internet üzerindeki olası zararlı yazılımların bilgisayarımızdaki bazı önemli ayarları değiştirme tehlikesine karşı koruyacaktır. İnternet kullanılacağı zaman yönetici haklarına sahip kullanıcı ile oturum açmaktan kaçınmak her zaman faydalıdır. Hatta risk altındaki bilgisayarlarda yönetici hesabı mutlaka şifrelenmeli ve eğer mümkünse hedef şaşırtmak için sahte administrator hesabı oluşturulmalıdır. Sahte administrator ve diğer kullanıcı hesapları ile ilgili detaylı bilgi için Tablo-1'i inceleyiniz.

Tablo–1: Sahte administrator hesabı ile işletim sisteminin korunması

Hesap Adı	Hesap Türü	Açıklama
Administartor	Sınırlı kullanıcı	Sahte yönetici hesabı, güçlü bir şifre ile korunmuş yanlış hedef. Şifresi kırılsa bile bilgisayarımızın önemli ayarları değiştirilemez
user1	Sınırlı kullanıcı	Günlük kullanım ve internet kullanımı için
user2	Sistem yöneticisi	Gerçek sistem yöneticisi hesabı

4. GEREKSİZ PAYLAŞIMLAR, PROTOKOLLER VE HİZMETLER

Kişisel bilgisayarımız bir bilgisayar ağının parçası değilse veya dosya ve yazıcı paylaştırma gibi servisler kullanılmıyorsa bu servisler mutlaka kapalı tutulmalıdır. Hatta dosya paylaşımı sürekli yapılmıyor, çok ender olarak kullanılıyor ise bu servisler yine kapalı olmalı sadece ihtiyaç duyulduğunda etkinleştirilip sonra tekrar devre dışı bırakılmalıdır. Kişisel bilgisayarımız herhangi bir bilgisayar ağının parçası değilse ve sadece internete bağlanmak için kullanılıyorsa ihtiyaç duyduğumuz tek protokol TCP/IP protokolüdür. Denetim Masası'ndan Ağ Bağlantıları'nı açıp Yerel Ağ Bağlantısı özelliklerini görüntülediğimizde bağlantının kullandığı öğelerde TCP/IP ve QoS Paket Zamanlayıcısı dışındaki protokollerin bulunması gereksizdir ve güvenlik açıklarına neden olacaktır (Şekil–2) [2,3]. QoS Paket Zamanlayıcısı protokolü arka planda sistem güncellemeleri için gerekli olan bir protokol olup kullanımda olmasında herhangi bir sakınca yoktur.



Şekil–2: Yerel Ağ Bağlantısı Özellikleri

Microsoft Windows XP işletim sisteminde aynı protokollerde olduğu gibi kullanılmıyorsa mutlaka devre dışı olması gereken hizmetler mevcuttur [4,5]. Bu hizmetler Tablo-2'de

gösterilmiştir. *Denetim Masası =>Yönetimsel Araçlar => Hizmetler* yolunu izleyerek çalışmasını istemediğimiz hizmeti devre dışı bırakabiliriz.

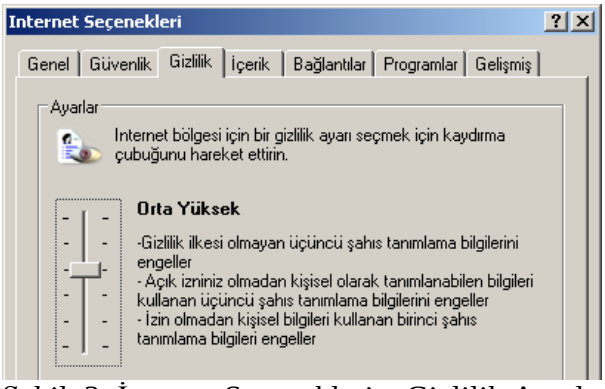
Tablo–2: Kişisel bilgisayarlarda kullanılmıyorsa devre dışı olması gereken hizmetler

Hizmetin Adı	Açıklamalar
Messenger	Bu hizmet kapatılarak sistemimizi spam e-postalara ve reklamlara karşı koruyabiliriz.
Uzaktan Kayıt Defteri	Başka bir kullanıcının ağ üzerinden kayıt defterini değiştirmesini sağlar, kullanılmıyorsa devre dışı olmalıdır
Netmeeting Remote Desktop Sharing	Başka bir bilgisayarı ağ üzerinden yönetmeye yarayan bu hizmet kullanılmıyorsa devre dışı olmalıdır.

5. WEB TARAYICILARININ AÇIKLARI

Microsoft Windows XP işletim sistemine entegre olarak bilgisayarımızda bulunan ve bugün internet ortamında en çok kullanılan web tarayıcısı olan Microsoft İnternet Explorer ile yine en yaygın olarak kullanılan e-posta istemcisi Outlook Express de hackerların hedefi olmakta ve güvenliğimiz için tehlikeleri içinde barındırmaktadır. Aynı işletim sisteminde olduğu gibi web tarayıcısının ve e-posta istemcisinin de en güncel halde olması çok önemlidir. Microsoft İnternet Explorer ve Outlook Express için en son yama ve güncellemeler yine http://windowsupdate.microsoft.com web sitesinde bulunabilir.

Microsoft İnternet Explorer ile daha güvenli sörf için internet seçeneklerinde bulunan gizlilik ayarı en az "Orta Yüksek" seviyesinde olmalıdır (Şekil–3) [2,6]. Microsoft İnternet Explorer'ı zararlı web sitelerine karşı korumak için ücretsiz olan SpywareBlaster adlı yazılımı http://www.javacoolsoftware.com web sitesinden indirip kullanmak mümkündür. Ayrıca Mozilla Firefox (http://www.mozilla.com/en-US/firefox/) ve Opera (http://www.opera.com) gibi alternatif web tarayıcıları ile Mozilla Thunderbird (http://www.mozilla.com/en-US/thunderbird/) gibi alternatif e-posta istemcilerini kullanmak en popüler yazılımları hedef alan hackerlara karşı bizi hedef olmaktan çıkaracaktır [1].



Şekil–3: İnternet Seçenekleri – Gizlilik Ayarları

6. GÜVENSİZ YAZILIMLAR VE CASUS YAZILIMLAR

Güvensiz yazılımlar illegal olarak kopyalanmış veya internetteki korsan sitelerden indirilmiş yazılımlar olup içlerinde bilgisayarımıza zarar verebilecek virüs, truva atı, tuş kaydedici ve her türlü casus yazılımı barındırabilen yazılımlardır. Casus yazılımlar ise internette gezdiğimiz web sitelerinin kayıtlarını tutup bizden habersiz başkalarına gönderen, karşımıza istemediğimiz reklam pencerelerinin gelmesini sağlayan, bilgisayarımızdaki şahsi dosyalarımızı başkalarına gönderebilen, bilgisayarımızın performansını düşüren ve internet erişimini gereksiz yere meşgul eden istenmeyen yazılımlardır. Bu tip yazışlımlar çoğu zaman sistemimize bizden habersiz olarak yüklenirler [7]. Casus yazılımlardan korunmak için yapılması gerekenler şu şekilde listelenebilir:

1. Korsan yazılım kullanmaktan kaçınmak, lisanslı yazılım kullanmak
2. Korsan web sitelerinden yazılım indirmemek
3. İnternetten yazılım indireceğimiz zaman güvenli web sitelerini kullanmak. Güvenli dosya indirme sitelerinde mutlaka "No ad-aware, no-spyware" gibi uyarılar mevcuttur.
4. Sırf bedava olduğu için ne olduğunu bilmediğimiz yazılımları bilgisayara yüklememek. Casus yazılımların çoğu bedava yazılımlarla bilgisayara yüklenir.

5. Yazılım yüklerken "son kullanıcı lisans sözleşmesi"ne göz atmak. "Ad-supported" olarak desteklenen yazılımları bilgisayarımıza yüklememek.
6. "Son kullanıcı lisans sözleşmesi"ni incelemek için EULAlyzer adlı yazılım kullanılabilir (http://www.javacoolsoftware.com/eulalyzer.html)

Bilgisayarımıza bulaşan casus yazılımları temizlemek için de özel yazılımlar mevcuttur. Anticasus yazılımların içinde ücretsiz olan Windows Defender (http://www.microsoft.com/athome/security/spyware/software/default.mspx), Ad-Aware (http://www.lavasoft.com) ve Spybot Search & Destroy (http://www.safer-networking.org/tr/index.html) casus yazılımları tanıyıp temizleme konusunda oldukça başarılıdır.

7. AĞ VE İNTERNET ÜZERİNDEN GELEBİLECEK TEHLİKELER

Bir ağa veya internete bağlı olan bilgisayar buradan gelebilecek her türlü tehlikeye karşı korumasızdır. Ağ veya internet üzerindeki korunmasız bilgisayara virüsler, truva atları, solucanlar, tuş kaydediciler ve casus yazılımlar bulaşabileceği gibi kişisel verilerimize erişmek isteyen hackerlar da saldırıda bulunabilir. Bütün bu tehlikelerden korunabilmek için bilgisayarımızda hem antivirüs yazılımı hem de güvenlik duvarı yazılımı bulunmalıdır [3]. Antivirüs yazılımları bilgisayar virüslerine karşı güvenlik sağlamakla birlikte sistemimizi solucanlara, truva atlarına ve tuş kaydedicilere karşı da korurlar. Microsoft Windows XP işletim sistemi için önerilen ücretsiz antivirüs yazılımları şunlardır [8,9,10]:

- AVG Antivirus Free (http://free.grisoft.com)
- Antivir Antivirus (http://www.avira.com)
- Avast Home Edition (http://www.avast.com)
- Comodo Antivirus (http://www.antivirus.comodo.com)

Fakat solucanlar, truva atları, tuş kaydediciler ve casus yazılımlara karşı etkili önlemler almak için sistemimizde mutlaka internet trafiğini denetleyen bir güvenlik duvarının bulunması şarttır. Bu sayede internet erişimini kullanmak isteyen zararlı yazılımlar tespit edilebilmekte ve önlenebilmektedir. Aynı zamanda güvenlik duvarları internet üzerinden bilgisayarımıza yapılacak olan saldırılara ve sistemimize bulaşmak isteyen tehlikeli yazılımlara karşı bilgisayarımızı koruyacaktır. Burada dikkat edilmesi gereken nokta Microsoft Windows XP işletim sistemine servis paketi 2 ile dahil edilen güvenlik duvarının sadece tek yönlü olduğudur. Bu güvenlik duvarı sadece internet üzerinden bilgisayarımıza gelen tehlikelerden bizi korur fakat bilgisayarımızdaki interneti kullanmak isteyen zararlı yazılımları engelleyemez. Microsoft'un 2007 yılında piyasaya süreceği Microsoft Vista işletim sisteminde de güvenlik duvarı bu şekilde çalışmaktadır. Bu nedenle bilgisayarımızda mutlaka ayrı bir güvenlik duvarı yazılımı bulunmalıdır [11]. Microsoft Windows XP işletim sistemi için önerilecek ücretsiz güvenlik duvarı yazılımları şunlardır [12]:

- ZoneAlarm (http://www.zonelabs.com)
- Sunbelt Kerio Personal Firewall (http://www.sunbelt-software.com/kerio.cfm)
- Comodo Firewall (http://www.comodogroup.com)
- NetVeda Safety.Net (http://www.netveda.com/consumer/safetynet.htm)
- SoftPerfect Personal Firewall (http://www.softperfect.com/products/firewall)
- Ashampoo FireWall FREE (http://www.ashampoo.com)

8. TUŞ KAYDEDİCİLER VE OLTA YÖNTEMLERİ

Tuş kaydediciler genellikle kredi kartı numara ve şifrelerini, internet bankacılığı hesap şifrelerini vb. önemli bilgileri çalmayı amaçlayan, kullanıcıdan gizli olarak arka planda çalışan ve klavye üzerinden basılan her tuş ile farenin hareketlerini anlık olarak kaydeden zararlı yazılımlardır. Tuş kaydedicilerden korunmak için mutlaka sistemimizde bir antivirüs yazılımı ve bir de güvenlik duvarı yazılımı bulunmalı ve ikisinin de aktif korumaları etkin olmalıdır.

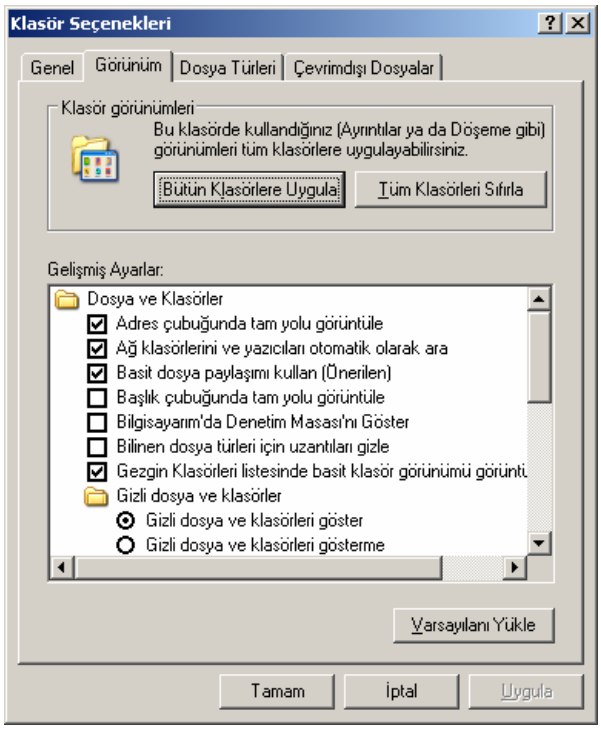
Olta yöntemleri ise internet bankacılığı şifresi, e-posta şifresi gibi bilgileri çalmak için oturum açma sayfalarının sahtelerini yapmak ve kullanıcıyı bu sahte sayfaya yönlendirip şifrelerini çalmak için kullanılan yöntemlerdir. Bu tip yöntemlerden korunmak için Microsoft Windows XP işletim sisteminde dikkat edilmesi gereken en önemli şey "hosts" dosyasının (C:\WINDOWS\system32\drivers\etc\hosts) bilginiz olmadan değiştirilmesini önlemektir. Anticasus yazılımlar örneğin Windows Defender (http://www.microsoft.com/athome/security/spyware/software/default.mspx) sistemimizde yüklü ve aktif koruması etkin halde ise bu dosyada yapılacak olan her türlü değişikliğe karşı kullanıcıyı uyaracaktır. Ayrıca Spyware Blaster adlı yazılım da hosts dosyasını şifreleyerek korumaktadır.

9. NUMARA ÇEVİRİCİLER

Numara çeviriciler özellikle internete çevirmeli bağlantı ile bağlanan kullanıcıların dikkat etmesi gereken zararlı yazılım türüdür. Bu tip yazılımlar internet bağlantısını keserek milletler arası telefon numarası çevirir ve bilgisayarı internete yeniden bağlar [7]. Daha sonra kullanıcı çok yüksek bedelli telefon faturaları ödemek durumunda kalabilir. Bu tip yazılımlardan korunmak için her şeyden önce dikkatli olmak gereklidir. Herhangi bir web sitesinde "sitemizdeki mp3leri bilgisayarınıza yüklemek için bu programı çalıştırın" veya "şifreli sayfalara erişebilmek için bu programı çalıştırın" şeklinde bir yazı gördüğünüzde bunun numara çevirici olduğu kesindir. Kullanıcılar hiçbir şekilde bu yazılımları çalıştırmamalıdır. Bazı anticasus yazılımlar numara çeviricilere karşı da koruma sağlamaktadır. Ayrıca çevirmeli bağlantı ile internete erişilen telefon hattının milletler arası telefon görüşmelerine kapatılması da çözüm yöntemi olarak düşünülebilir.

10. DİĞER OLASI TEHLİKELER

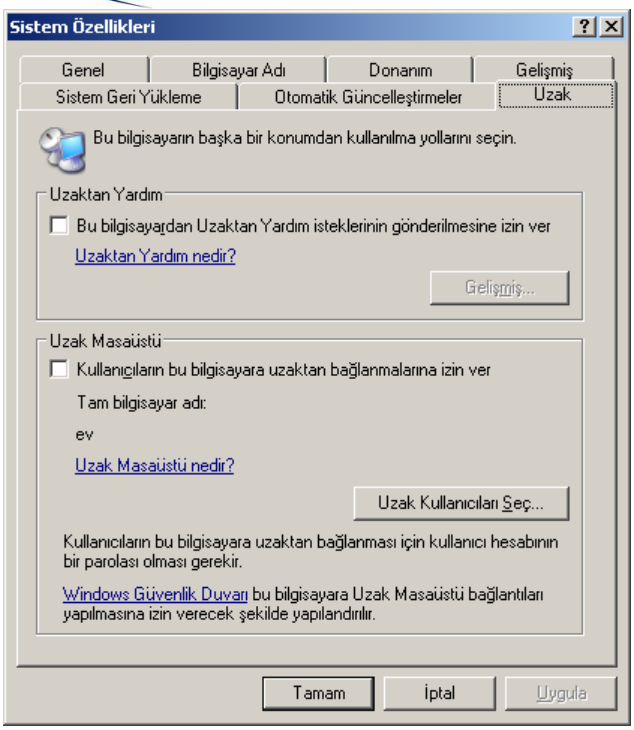
Microsoft Windows XP işletim sisteminde klasör seçeneklerindeki "Bilinen dosya türleri için uzantıları gizle" seçeneği zararlı bazı kodların gizlenmesine yardımcı olduğu için olası bir tehlikedir. Örneğin "resim.jpg.vbs" şeklindeki zararlı bir script kodu bilinen dosya türleri için uzantılar gizlendiğinden "resim.jpg" şeklinde bir resim dosyası olarak gözükecektir. Kullanıcı resim dosyasını açtığını zannederek bu dosyayı çalıştıracak fakat bu sırada zararlı olan script kodu çalışacak ve sistemimize zarar verecektir. Bilinen dosya türleri için uzantıları gizle seçeneğini devre dışı bırakmak için Windows gezgininde klasör seçeneklerinden bu ayar devre dışı bırakılmalıdır (Şekil–5).



Şekil–5: Bilinen dosya türleri için uzantıları gizle seçeneğini devre dışı bırakmak

Diğer bir olası tehlike de kablosuz ADSL modemlerdir. Bu tip kablosuz modemlerde eğer şifreleme uygulanmazsa modemin etki alanı içindeki yabancı bir kablosuz ağ özelliği olan bilgisayar ağımıza erişebilmekte, internet bağlantımızı kullanabilmekte ve hatta özel verilerimize erişebilme imkanına sahip olmaktadır. Bu nedenle kablosuz modemlerde mutlaka şifreleme işlemi kullanılmalıdır [1].

Uzaktan erişimin de eğer kullanılmıyorsa kapalı tutulması Microsoft Windows XP işlerim sisteminin daha güvenli olmasını sağlayacaktır. Bunun için yapılması gereken *Denetim Masası => Sistem => Uzak* yolunu izlemek ve uzaktan erişim özelliklerini devre dışı bırakmaktır (Şekil–6) [1].



Şekil–6: Uzaktan Yardım ve Uzak Masaüstü seçeneklerini devre dışı bırakmak

11. SONUÇ

Savunmasız bir kişisel bilgisayar internete bağlandığı andan itibaren birçok tehlike ile karşı karşıyadır. Bilgisayarımızı güvenli olarak kullanabilmek için mutlaka antivirüs, güvenlik duvarı ve anticasus yazılımlarını bilgisayarımıza yüklemeli, bu yazılımlar olmadan internete bağlanılmamalıdır. Ayrıca güvenlik yazılımlarını, işletim sistemimizi ve web tarayıcısı ile e-posta istemcisi gibi internet yazılımlarının en güncel hallerini kullanmak kişisel bilgisayar güvenliği için çok önemlidir. İnternet kullanırken de zararlı sitelere girilmemeli, güvenilir olamayan yazılımlar bilgisayara yüklenilmemeli ve çalıştırılmamalıdır. Microsoft Windows XP işletim sistemi de birkaç basit fakat etkili ayarları yaparak daha güvenli hale getirilebilir. Bütün bu önlemler alındıktan sonra çok daha kişisel bilgisayarımızda güvenli bir şekilde interneti kullanabiliriz.

KAYNAKLAR

[1] 2004 Hacker Raporu Gerçekten Güvenli Bir Pc İçin, CHİP, sayı.2004/04, Nisan 2004, pp.44-61.

[2] Her Şeyin Başı Güvenlik, CHİP, sayı.2003/11, Kasım 2003, pp.30-35

[3] Hacker Dünyası, PCnet, sayı.103, Nisan 2006, pp.62-76

[4] Services Guide for Windows XP, http://www.theeldergeek.com/services_guide.htm

[5] Tam Gaz Windows, CHİP, sayı.2004/10, Ekim 2004, pp.154-162

[6] Karslıoğlu, M., Bakımlı Bir Windows, CHİP, sayı.2002/11, Kasım 2002, pp.118-122

[7] CHOICE - Test: Anti-spyware software, http://www.choice.com.au/printFriendly.aspx?ID=104425

[8] http://www.firewallguide.com/anti-virus.htm

[9] Mary Landesman, Review: Free Antivirus Software, http://antivirus.about.com/od/antivirussoftwarereviews/a/freeav.htm

[10] Rob Pegoraro, 2 free virus stoppers worth using, http://seattletimes.nwsource.com/html/businesstechnology/2002691520_btsoho19.html

[11] Pınar, M., Gözler Vista'da, CHİP, sayı.2006/10, Ekim 2006, pp.106-107

[12] http://www.firewallguide.com/software.htm