

# Giriş Seviyesi Kişisel Bilgi Güvenliği

MUSTAFA SERHAT DÜNDAR, <SERHAT AT SERHATDUNDAR DOT COM>,  
21/06/2009

## NEDEN İLK ÖNCE KİŞİSEL BİLGİ GÜVENLİĞİ?

İnternette güvenlik hakkında çeşit çeşit doküman bulmak mümkündür. Bunların çoğu basit güvenlik yanlışlarından oluşan veya üst düzey bilgi verebilme gayesiyle yazılmış birçok kullanıcının anlayamayacağı düzeyde dökümanlardır. Genel anlamda sıradan bir kullanıcı anti virüs kurduktan sonra kendini güvende hissetmeye başlar. Çoğu kimseler firewall nedir zaten bilmezken, bilenlerin de büyük bir kısmı korunma için ‘install’ etmenin yeterli olduğunu düşünür.

Bu makale’de sizlere en çok yanılgıya düşülen konuları, temel güvenlik bilgilerini, temel düzeyde bilgili bir saldırganın saldırı stratejisini ve bundan korunmayı, ufak ama önem taşıyan püf noktalarını öğreterek daha kompleks dökümanlara hazır olmanızı sağlamayı amaçlamaktadır. Peki neden ilk önce kişisel bilgi güvenliği? Çünkü bizim için kişisel olan her şey önemli ve özeldir..

## GÜVENLİ BİR SİSTEM KURALIM..

### İLK ÖNCE MODEM !

Donanımsal olarak güvende olmadığımız sürece yazılımsal olarak güvende olmamız mümkün değil. Güvenli bir modem firewall, router ve dos atack’lara karşı koruma içeren modemdir.

Modem seçerken 2 adet seçtiğimiz var; bunlar Ethernet ve Usb modemler. Usb modemler güvenlik yönünden oldukça zayıftır, sağladıkları avantaj yalnızca kolay bağlanabilmeleri ve fiyat yönünden daha uygun olmalarıdır bu tip modemler router özelliği barındırmadığından güvenlik için ciddi önem taşıyan portların bir çoğu açıktır. Usb modemlerin bir diğer kötü yanı ise port açma gibi bir işlem yapmak istediğinizde (p2p programları, çeşitli oyunlar için bu işlem gerekebilir) size bu imkanı tanımasıdır.

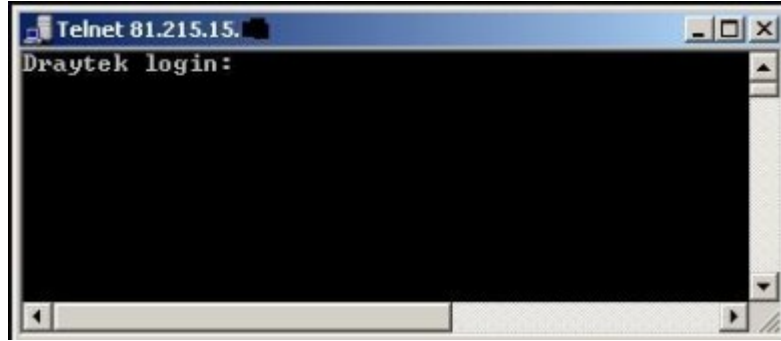
Güvenlik – kullanıcı desteği – kolay kurulum – software desteği gibi konuların hepsinde güvendiğim modem şuan kullandığım 4 portlu AirTies Adsl2 Rt-111 modelidir. Ne gibi özellikleri var bu modem için?

DNS ayarı yapabilme imkanı tanınması, yerel ağ yönetimine izin vermesi, istenilen adrese ip ve mac. Numarası atayabilme (yerel ağ'da), dahili firewall, oyun ve p2p programları için port açma vs. dertlerden kurtaran uygulama ayarları, Mac adres filtreleme, Web filtresi, Url filtresi, DMZ gibi harika bir özellik (ileri seviye dökümanda işlenecektir), AntiDos özelliği, NAT, port yönlendirme, statik ve dinamik routing, SNMP, Uzaktan Erişim, DDns ve daha bir çok özelliği ile ne isterseniz yapmanıza olanak veren kusursuz bir modemdir. Yeni modem alacak olanların mutlaka incelemesini tavsiye ederim.

## MODEM VE ADSL KULLANICI ŞİFRESİ ÖNEMLİDİR!

Modem'ler fabrika ayarlı olarak (default); şifresiz veya bilindik şifrelerle evinize gelir. Modeminizi alıp kurduktan sonra size özel modem ayarları ve adsl kullanıcı şifreniz bağlantı için tutulur. İnternette bulabileceğiniz default modem şifreleri ile herhangi bir modeme bağlanmanız oldukça kolaydır. Şimdi bunu bir saldırının gözünden değerlendirelim.

Saldırığımız için eğer kime saldırdığı önemli değilse piyasada yüzlercesi bulunan ip scanner'lerden (verdiğiniz aralıktaki ip. numaralarından herhangi bir bilgisayara atanmış olanları bulan program) birini kullanarak önüne ufak bir ip listesi çıkartır. Bağlantı için 21 (ftp) ve 23. (telnet) portları seçilir çünkü bunlar neredeyse her modemde default olarak 'açık' seçilmiştir. 21 ve 23üncü portları dinlemek istediğini de program ile ayarlayan saldırığımız programın bulduğu ip numaralarına telnet protokolü ile bağlanmaya çalışır. Fakat karşısına bir şifre çıkmıştır tabiki bu sayfada şifreyi soran istemcinin (modem) markasıda yazmaktadır. Hemen internetteki default şifre listelerinden markayı bulan saldırığımız default şifreyi dener ve modeme bağlanır. Modem arayüzünden ayarlarınızı değiştirebilir, adsl kullanıcı adı ve şifrenizi alabilir, yeni port açabilir vs. vs.

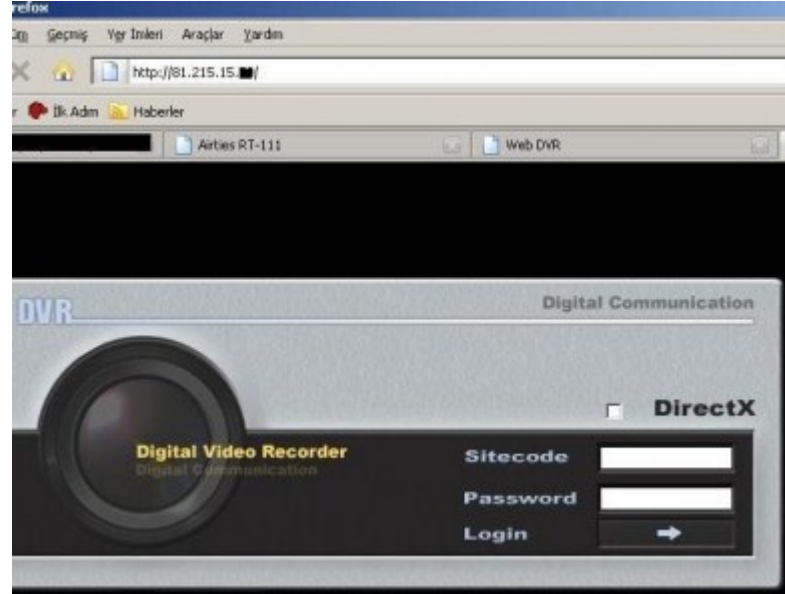


Evet kısaca bir saldırının düşünce stratejisini açıkladık. Bundan korunmak için web tarayıcınızın web arayüzüne bağlanıp kullanıcı ayarlarından şifrenizi değiştirmeniz gerekmektedir. Browser'inize '<http://192.168.2.1/>' veya '<http://10.0.0.1/>' gibi ip numaraları yazarak modem arayüzünüze ulaşabilirsiniz. Şifrenizi 6 haneden uzun ve rakam-sayı karışık seçmeniz her zaman sizin lehinizedir.

İkinci aşama olarak ttnet'in sayfasından kayıt olurken size verilen şifreyi değiştirmeniz gerekmektedir.

Üstteki menüden şifre işlemleri/şifre değiştirme seçerek şifrenizi değiştirebilirsiniz. Bu işlem sonrasında modeminize reset atıp mevcut kullanıcı şifrenizi değiştirmeyi unutursanız internete bağlanamazsınız.

Bu verdiğim örnek sadece basit bir modem şifresini değiştirmediğimiz için başımıza gelebileceklerdi. Daha kötü olasılıklarda var tabiki. İp taramalarında yalnızca modem'ler bulunmuyor. WebDVR yani network güvenlik kamerası olarak kullandığınız kameranızda arayüzüne aynı şekilde bağlanılabilir, eviniz veya iş yeriniz sizin haberiniz olmadan izlenebilir belki de bunu keşfeden kötü niyetli kişiler kameranızla oynayıp o gece dükkanınıza bile uğrayabilir (: Her ne kadar kötü durum senaryosu gibi dursa da basit bir ip taramasının sonunda olabilecek şeylerdir.



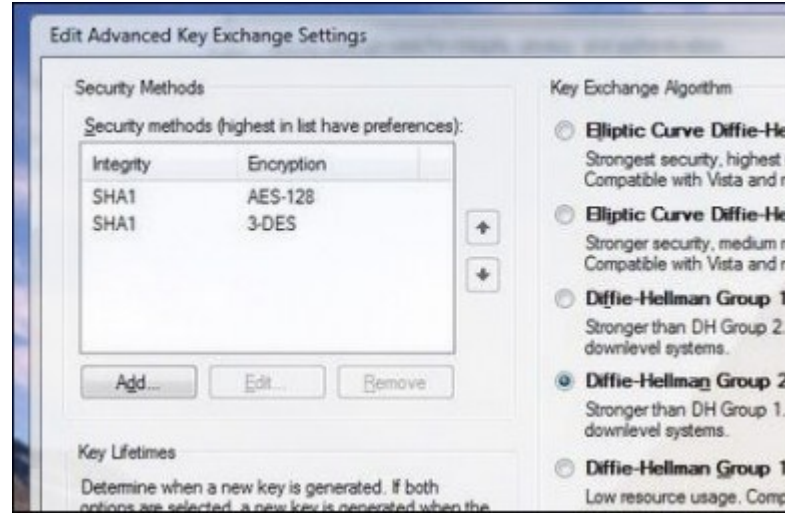
Bir diğer önemli nokta ise Simple Network Management Protocol (SNMP) yani modeminizi uzaktan yönetmek için kullanılan bir protokoldür. Genelde müşteri hizmetleri kendi açlarından kolay olsun diye açık bırakmıştır bu seçeneği fakat biz kapatıyoruz. Örneğin benim modem geldiğinde 'public' seviyesinde herkese okuma izni verilmişti ! Bunu direk kapalı duruma alıyoruz.

## WINDOWS FIREWALL'A NE DERECE GÜVENELİM?

Ben direk cevabını vererek başlamak istiyorum. 'Hiç' güvenmeyelim !

Daha önce [matousec](http://matousec) adresinde yapılan güvenlik testlerinde Windows firewall'ı da 10 level'dan oluşan test'te dahil ediyorlardı fakat Windows firewall hiçbir testte %50'nin üstünde puan alamadığı için artık onu listeye bile dahil etmiyorlar.

Test sonuçları XP içinde dahili olarak gelen firewall için geçerli. Peki vista'da durum nasıl? Vista'yı kurduğumuz zaman hazır olarak gelen firewall Xp'dekine oranla çok daha iyi durumda. Artık kullanıcının ileri derecede firewall'a müdahale etmesi sağlanmış. Dilediğiniz bazı portların açık kalmasını ayarlayabiliyor ve bunların seçtiğiniz ip yada ağ ile iletişim kurmasına izin verebiliyorsunuz.



XP'de bulunan ICMP ayarları yine aynen bize gelmiş. Yeni özelliklerden bir diğeri de IPsec ayarlarını bizim yapabilmemize izin vermesi. Bu sayede kimlik doğrulama ve şifreleme için uygulanacak güvenlik metodunu belirleyebilirsiniz. IPsec içinde bilgisayarımızın karşılıklı iletişime geçeceği bilgisayarla yapacağı doğrulama işleminde kullanacağı şifreleme protokolünü de seçebiliyoruz. Bu gibi ileri seviye güvenlik ayarları için hazırlanan 'Windows Firewall with Advanced Security' kısmı en çok yeniliği barındıran kısım.

Vista'da, farklı çalışma ortamları için ayrıca üç adet ağ profili bulunmaktadır. Bu profiller:

Domain (etki alanı) Profil: Bilgisayar herhangi bir etki alanına bağlıysa.

Private (kişisel) Profil: Koruma başka bir güvenlik duvarı tarafından sağlanıyorsa.

Public Profil: Koruma sadece güvenlik duvarı tarafından sağlanıyorsa.

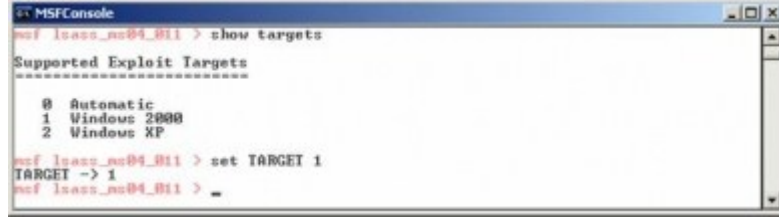


Velhasıl Windows firewall biraz daha düzelmiş olsada bende XP'deki haliyle bıraktığı kötü izlenimden dolayı ona karşı bi güven söz konusu değil. Bir sonraki yazı dizisinde güvenli bir firewall kurmayı en ince detaylarıyla anlatacağız.

## SERVICE PACK 2'NİN ÖNEMİ

Sp2 için çokça yorum mevcut ortalıkta. Benim kendi fikrim ise bu paketin düzelttiği en önemli sorun, zamanında çokça uğraşmış olduğum 'Reverse Connection ile VNC Saldırısı' yapmayı engellemesidir. Service Pack2 yüklü olmayan bilgisayarlara, Metasploit Framework 2.7'de mevcut bulunan 'lsass\_ms04\_011' exploiti ile çok kolayca reverse connection yapılabilirdi.

Bu konuyu ben daha da merak ediyorum diyorsanız [security focus](#)'taki bu sayfaya göz atabilirsiniz.



```
msf lsass_exe04_011 > show targets

Supported Exploit Targets

0 Automatic
1 Windows 2000
2 Windows XP

msf lsass_exe04_011 > set TARGET 1
TARGET => 1
msf lsass_exe04_011 >
```

(Resimdeki görüntü windowsa güvenenlerin durumu için acınası bir tablo.)

Bunun haricinde Windows 95/98/2000/Me/XP'de olmayıpta SP2'de olan özellikleride kısaca sıralayalım :

Internet Explorer Açılır Pencere Engelleyicisi

Windows Güvenlik Duvarı (varsayılan olarak önceden kapalı iken sp2 ile açıktır)

Ek Yöneticisi

Internet Explorer karşıdan yüklemelerini izleme

Internet Explorer Bilgi Çubuğu

Otomatik Güncelleştirmeler (varsayılan olarak önceden kapalı iken sp2 ile açıktır)

Windows Güvenlik Merkezi

Outlook Express gizlilik güncelleştirmesi

Internet Explorer Eklenti Yöneticisi

Eğer bilgisayarınızda SP2 yüklü değil ise bir an önce yüklemeniz tavsiye edilir.

## BİRDE SP3 ÇIKMIŞTI AMA ?

Evet SP2'den sonra birde sp3 çıkmıştı fakat sp2 kadar ilgi görmedi. Peki önemsizmiydi bu servis paketi? Kesinlikle önemsiz değildi. 150'den fazla önemli güvenlik eklentisi içeren bu paket gerek Türkçe desteğinin geç çıkmasından, gerek sp3 çıktıktan kısa bir süre sonra vista'nın gelmesinden dolayı gereken ilgiyi görmedi. Tabiki birde lisanssız olmasına rağmen çeşitli programlar ile lisanslı gibi gösterilen xp'lerin lisanslarının yeniden deşifre olmasına yardımcı oluyordu. Belki bunun da etkisi vardır (: Kimse bir daha xp'sini lisanslamakla uğraşmak istemez açıkcası.

Bu konuyla ilgili geniş bilgi isteyenler SP3'teki fix'ler ve güvenlik önlemlerinin tamamını merak edenler <http://support.microsoft.com/kb/946480/> adresine göz atabilir. Yine

SP3'ün sürüm notlarını <http://download.microsoft.com/download/f/d/d/fdd27c81-8e15-4583-abb8-5e5...> adresinden inceleyebilirsiniz.

SP1 – SP2 ve SP3'e ftp üzerinden kolayca ulaşmak için :

[http://ftp.anadolu.edu.tr/Service\\_Packs/Windows\\_XP\\_Srv\\_Packs/](http://ftp.anadolu.edu.tr/Service_Packs/Windows_XP_Srv_Packs/)

adresini kullanabilirsiniz.

## GÜVENLİK AÇISINDAN NTFS DOSYA SİSTEMİ? (MICROSOFT MAKALESİ)

Active Directory (ve Active Directory'nin bir parçası olan etki alanları)

Active Directory ile ağ kaynaklarını kolaylıkla görüntüleyebilir ve denetleyebilirsiniz. Etki alanlarında, yönetim basitliğini korurken güvenlik seçeneklerinin ince ayarını yapabilirsiniz. Etki alanı denetleyicileri ve Active Directory, NTFS gerektirir.

Güvenliği büyük ölçüde artıran dosya şifrelemesi. (Ancak, bir dosya hem sıkıştırılmış hem de şifreli olamaz.)

Yalnızca klasörlere değil, tekil dosyalara da uygulanabilen izinler.

Güç kaybı veya başka sistem sorunları yaşanması durumunda NTFS'nin bilgileri hızla geri yüklemesine yardımcı olan, disk etkinlikleri kurtarma günlüğü.

Bireysel kullanıcıların kullandığı disk alanı miktarını izleyip sınırlama koymanıza olanak veren disk kotaları.

NTFS'ye ait en önemli özelliklerden biri ise klasör izinlerini ayarlayabilmektir.

## KLASÖR İZİNLERİ

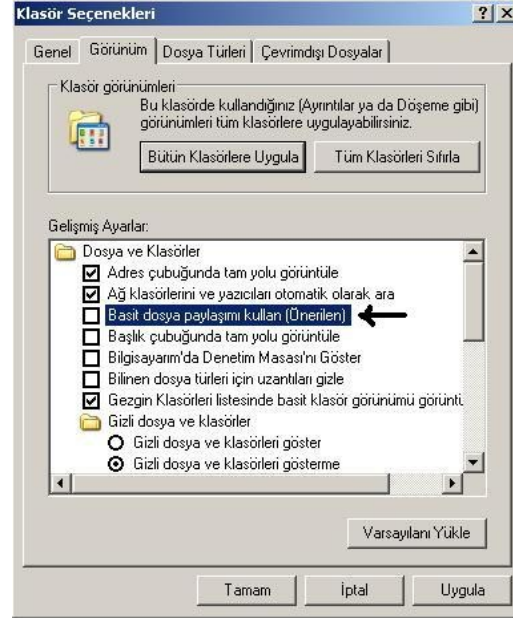
Çoğumuzun bilgisayarında başkalarının görmesini istemediğimiz gizli dosyalarımız veya klasörlerimiz vardır. Peki bunları en basit ve en güvenli şekilde nasıl şifreleriz ?

Piyasada bir çok uyduruk dosya şifreleme programı var. Bunları kesinlikle kullanmayın çünkü en ufak bir hatada program tarafından şifrelenmiş dosyalar bir daha açılmıyor ve doğal olarak belgelerinizi kaybetmiş oluyorsunuz.

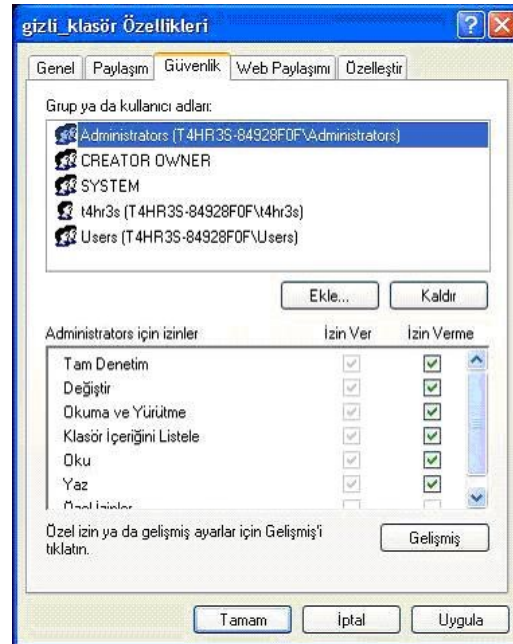
Bu yöntem son derece güvenli ve herhangi bir program kullanmadan olacak. Çoğumuzun bildiği permiller yani izinler ile :) Buyrun başlayalım :

**1-) Öncelikle C:\guvenli\gizli\_klasor adı gibi bir dizin oluşturduğumuzu var sayıyorum. Yani klasörün adı gizli\_klasör olacak diyelim ki. Araçlar/Klasör Seçenekleri/Görünüm**

menüsünden Basit dosya paylaşımını kullan seçeneğindeki işareti kaldırıyoruz. OK leyip kapatın bu sayfayı.



2-) Gizleyeceğiniz klasöre sağ tıklayın Özelliklere girin. Üstte yeni seçenekler göreceksiniz. Bunlardan "Güvenlik" seçeneğine giriyoruz. Bilgisayarınızda tek hesap kullanıyorsanız Admsintratorda ki tüm izinleri kaldırıyoruz. Başka kullanıcılarla ilgili işlem yapmak istiyorsanız onların izinlerini kaldırın.





“Tamam”a tıklayarak çıkıyoruz. Artık siz istemediğiniz sürece kimse bu klasöre giremez. Eğer tabi girmek isteyen kişi bu izinlerden haberdar ise yine bizim yaptığımız gibi bu güvenlik önlemini aşabilir. Aynı zamanda klasörün içinde yine izinlerle korunmuş bir dosya ver ise silinemez.

Eğer bu menünün kurcalanmasından korkunuz varsa tekrar görünüm menüsüne girerek basit dosya paylaşımını aktif halle getirebilirsiniz.

## NTFS İZİNLERİYLE DOSYALARIN GÜVENLİĞİNİ SAĞLAMANIN EN İYİ YÖNTEMLERİ (MICROSOFT MAKALESİ)

NTFS izinlerini ayarlarken aşağıdaki en iyi yöntemleri kullanın :

İzinleri kullanıcılar yerine gruplara atayın. Kullanıcı hesaplarını doğrudan tutmak verimli bir yöntem olmadığından, izinleri kullanıcı temelinde atamak bir özel durumdur.

Mümkünse dosya sistemi nesneleri, özellikle de sistem klasörleri ve kök dizin klasörleri üzerindeki varsayılan izin girdilerini değiştirmekten kaçının. Varsayılan izinleri değiştirmek beklenmeyen adres sorunlarına yol açabilir veya güvenliği zayıflatabilir.

Everyone grubunun nesne erişimini hiçbir zaman engellemeyin. Bir nesneye Everyone iznini engellerseniz, bu yöneticileri de kapsar. Bu nesneye diğer kullanıcı, grup veya bilgisayar izinlerini verirken Everyone grubunu kaldırmak daha iyi bir çözümdür.

Administrators grubuna ve LocalSystem hesabına Tam Denetim düzeyi atamanız da gerekebilir.

Nesne özel olarak girilmiş İzni Verme izni girdisine sahipse, devralınan Reddetme izinleri nesneye erişimi engellemez. Devralınan Reddetme izinleri de dahil olmak üzere, özel olarak belirtilen izinler devralınan izinlerden önceliklidir.

Reddetme izinleri yalnızca aşağıdaki özel durumlarda kullanılmalıdır:

->İzin Verme izinlerine sahip olan bir grubun alt kümesini dışlamak için.

->Bir kullanıcı veya gruba Tam Denetim atadığınızda, tek bir özel izni dışlamak için.

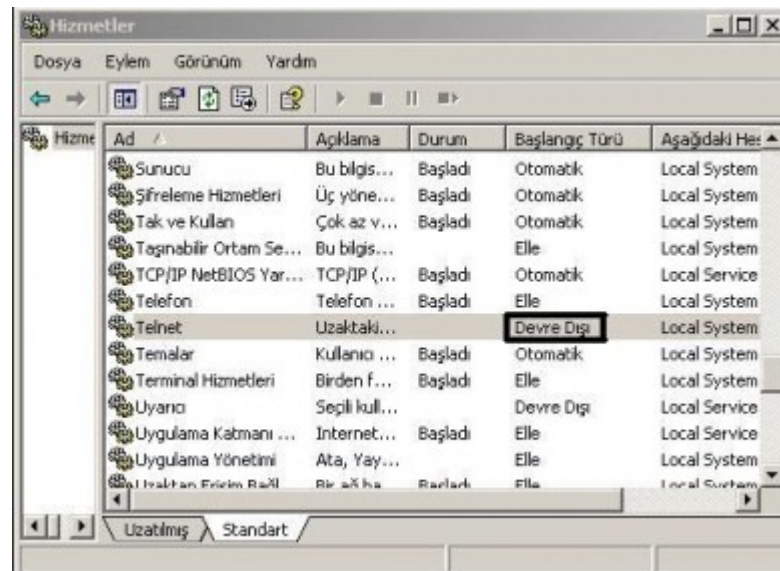
Web sunucunuzun NTFS izinlerini yapılandırırken dikkatli olun. Uygun olmayan ayarlanmış izinler, geçerli kullanıcıların istenen dosyalara ve dizinlere erişimlerini engelleyebilir. Örneğin, kullanıcının bir programı görüntülemek ve yürütmek için doğru hakları olsa bile, kullanıcının programı çalıştırmak için gereken belirli bir dinamik bağlantı kitaplığına (DLL) erişim izni olmayabilir. Kullanıcıların güvenli ve kesintisiz dosya erişimlerini garantilemek için, ilgili dosyaları aynı dizine yerleştirin ve sonra da dizine uygun NTFS izinlerini atayın.

## TELNET'i KAPATMAK

Telnet bağlı olduğunuz ağda kullanıcı adı ve parolayı karşı tarafa düz metin yani plain text halinde gönderdiği için güvenilir değildir. Ağ dinleyen ve bağlantı kurmak isteyen biri bu bilgilere kolayca erişebilir. Güvenli bir bağlantı için kullanıcı adı ve parola, hatta alış verişi yapılan her tür veri belirli bir protokolle şifrelenmelidir.

Telnet bağlantısı 23.port üzerinden sağlanıyor ve işinize yaramıyor ise 23 portu kapatmanız yararınıza olur.

23. portu kapatmak için Başlat-Çalıştır-services.msc komutu girip açılan pencereden "Telnet" i disable yada devredışı bırakmanız yeterlidir.



## TEHLİKELİ UZANTILAR

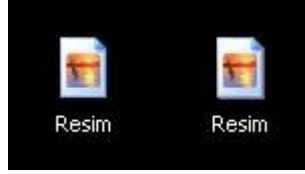
Paylaşımını yaparken, biri bize yolladığında kabul ederken dikkat etmemiz gereken bazı dosya uzantıları vardır. Bunlar başlıca .exe – .scr – .bat – .cmd – .com gibi uzantılardır. En çok bilinenler .exe ve .scr olmakla beraber geçmiş yıllarda .bat ve .cmd’de oldukça meşhurdur. Peki sadece bu uzantılardan mı korkmalıyız? Hayır tabikide bir word yada excel dosyası zararlı kod bulunduramaz mı? Çok rahatlıkla bulundurabilir çünkü bu belge türleri makro kodları içerebilme özelliğine sahiptir.

Bilgisayarınızı paylaşma açan ufak bir .bat kodu :

```
net share fenty=c:\ /unlimited /remark:"Clbr.FenTanyL"  
net share fenty=d:\ /unlimited /remark:"Clbr.FenTanyL"  
net share fenty=e:\ /unlimited /remark:"Clbr.FenTanyL"
```

Genel itibariyle trojan – virüs ve keylogger’lar bu uzantıları kullanır. Bu yüzden ki uzantıları görmek her zaman faydalıdır. Windows bize ilk kurulduğu anda default olarak uzantıları göstermez. Bu dikkatsiz kullanıcının kolayca tuzağa düşüp verilen dosyaya girmesini daha da kolaylaştırır.

Uzantılar Gösterilmiyorken :



Uzantılar Gösteriliyorken :



#### KAYNAKLAR :

<http://www.microsoft.com/turkiye/athome/security/update/sp2.msp>

<http://technet2.microsoft.com/windowsserver/tr/library/0be638cc-33d3-45a...>

<http://technet2.microsoft.com/windowsserver/tr/library/acaf5d6b-6578-44c...>

<http://www.bidb.itu.edu.tr/?d=806>

<http://www.securityfocus.com/excerpts/14/5>

<http://support.microsoft.com/kb/946480/>