internet güvenliği

İnternet hayatımıza gireli çok uzun bir zaman olmadı ancak günlük yaşamımızın olmazsa olmazlarından biri oldu bile. Bir çoğumuz internetle daha önceden tanışıyordu zaten. Fakat Bağ-Kur ve Emekli Sandığı sayesinde diğer meslektaşlarımızda bu kervana katıldı.

İnternetin sınırsız bir bilgi ve iletişim yumağı olması kullanım alanlarının da sınırsız olmasını sağliyor. Zaten problemde burada başlıyor. Bu sınırsızlık hayatı çok kolaylaştırabildiği gibi, bazen de tatsız süprizlerle zorlaştırıyor. Peki bu tatsız süprizler nelerdir ve karşılaşmamak için neler yapılabilir?

Bilgisayarınızda kayıtlı kişisel dosyalarınıza ve şifrelerinize ulaşılması veya bilgisayarınıza uzaktan hükmedilmesi, klavyede bastığınız tuşların tespit edilmesi oldukça tatsız süprizlerden başlıcaları. Ancak bunların olabilmesi için öncelikle sizin bilgisayarınıza isteğiniz dışında bir tür programcık yüklenmesi gerekiyor. İnternete bağlandığınızda, bu program size görünmeden, habersiz bir şekilde çalışarak karşı tarafa yukarıda bahsettiğim işleri yaptırabiliyor. Genellikle de bir e-mail ekinde geliyor. Ya da internette *surf* yaparken ziyaret ettiğiniz kötü niyetli bir sayfadan yükleniyor. E-mail ekinde gelen dosyayı merak edip açarsanız yada ziyaret ettiğiniz web sayfası tarafından bilgisayarınıza yüklenmek istenen programamı yüklerseniz olanlar oluyor. **Bu tip programlara TROJAN HORSE (turuva atı) deniliyor.** Bunlardan yüzlerce var ancak en meşhurları *Back Orifice, Sub Seven ve Net Bus.*

Buradan itibaren yazacağım nacizane tavsiyelerim, daha yaygın olarak kullanılan Windows 95 / 98 / 98SE işletim sistemi ve İnternet Explorer web tarayıcıları için olacak. İşe İnternet Explorer'ın ayarları ile başlayacağız. Daha sonra Windows'un kritik güncelleştirmelerinin nasıl yapılacağı anlatıp son olarak da bir **firewall** programı önereceğim.

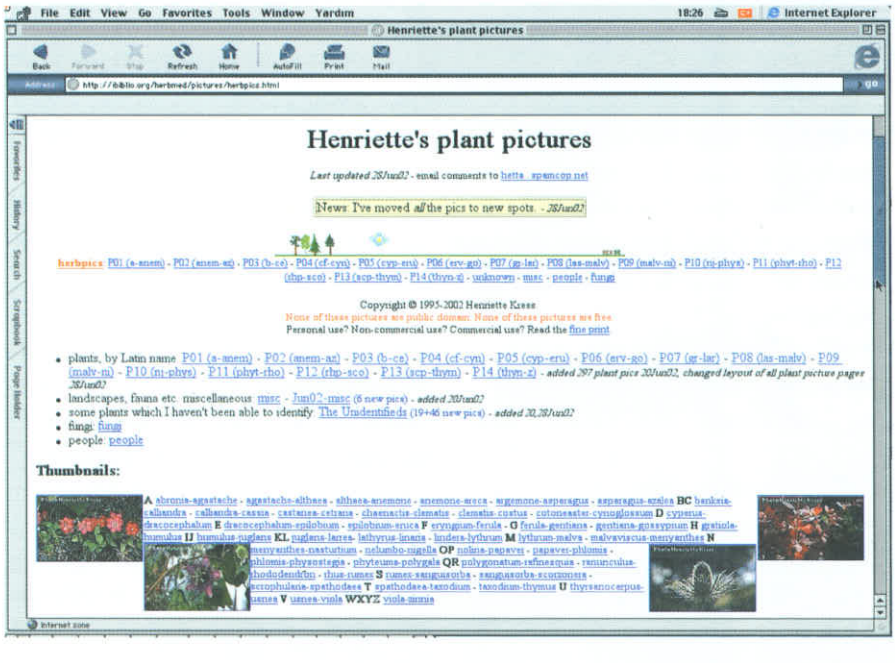
İnternet Explorer 4.0'da **Görünüm**, 5.0 ve 6.0'da **Araçlar** sekmesi altında bulunan İNTERNET SEÇENEKLERİ'ni tıklayınca bir pencere açılacak. Bu pencerede AYARLAR butonuna tıklayın. En üstte görünecek olan SAYFA HER ZİYARET EDİLDİĞİNDE seçeneğinin yanındaki noktayı seçip TAMAM butonuna tıklayın.

Şimdi yukarıdaki GÜVENLİK sekmesini tıklayın. Buradaki güvenlik derecesi ORTA olmalıdır. Eğer değilse ortayı seçip UYGULA'yı tıklayın.

Yukarıdaki sekmelerden İÇERİK'i seçin. OTOMATİK TAMAMLA butonuna tıklayın. Açılan pencereyi sadece WEB ADRESLERİ 'nin yanındaki çentik işaretli diğerleri boş olacak şekilde düzeltip, TAMAM'ı tıklayın.

Son olarak yine yukarıdaki sekmelerden GELİŞMİŞ'i seçin. Sağ taraftaki çubuğu biraz aşağıya kaydırarak GÜVENLİK bölümüne gelin. Bu bölümde eğer işaretli değilse ŞİFRELİ SAYFALARI DİSKE KAYDETME ve TARAYICI KAPATILDIĞINDA TEMPORARY İNTERNET FİLES KLASÖRÜNÜ BOŞALT seçeneklerini işaretleyin ve TAMAM'ı tıklayın.

Bazı web sayfalarında, tarayıcınıza girdiğiniz kullanıcı kodları, şifreler veya bu tarz kişisel form bilgileri daha sonra kolaylık olması için kaydedilir. Tekrar aynı sayfayı ziyaret edip bu bilgilerin ilk birkaç karekterini yazdığınızda otomatik olarak gerisi tamamlanır. Ancak bu bilgilerin tarayıcınızda kalması başkalarının eline geçme riskini doğurur. Yukarıda yaptığımız ayarlarlar ile artık tarayıcınıza bunlar kaydedilmeyecek yada kaydedilse bile tarayıcıyı kapattığınızda silinecek.



Yazılım şirketleri ürettikleri yazılımların hatalarını ve eksikliklerini gidermek için **yama** adı verilen ek yazılımlar hazırlarlar. Microsoft da zaman zaman windows için güncelleştirme yamaları çıkartıyor. Bu yamalar windows'un tespit edilen problemlerini gidermeyi amaçlıyor. Bu yamaların arasında birde kritik güncelleştirmeler paketi var. Bu paket ise Windows'un güvenlik açıklarını kapatıyor.

Bu yamayı yüklemek için internet bağlantınızı yapıp tarayıcınızı açın. **Araçlar** sekmesinin altındaki **Windows update**'e tıkladığınızda Microsoft Windows Update sayfası karşınıza gelecek. Sayfanın adresi *http://windowsupdate.microsoft.com*. Bu sayfada **Ürün Güncelleştirmeleri**'ni tıkladığınızda sisteminiz kontrol edilerek yüklü olamayan kritik güncelleştirmeler belirlenecek. Sol üstteki **Karşıdan yükle**yi tıklayın. Açılan pencerden **Yüklemeyi başlat**ı tıklayınca yükleme başlayacak. Yükleme bitince otomatik olarak **install** edilecek ve bilgisayarı yeniden başlatmanızı isteyecek. Tamam deyip yeniden açılmasını bekleyin. Bu güncelleştirmeyi ara sıra kontrol edip yenisi çıktıkça yapmakta fayda var.

Buraya kadar yaptıklarımız, herhangi bir saldırıya uğrama riskimizi azaltmak veya uğradığımızda göreceğimiz zararı daha aza indirmek içindi. İnternete girdiğinizde bir bigi akışı olduğu için mecburen bazı kanalların açık olması gerekiyor. **Firewall** adı verilen programlar ise bu açık kanalları kontrol ederek izinsiz giriş ve çıkışları engelliyor. Bu programlardan da yüzlerce var. İnternete giriyorsanız bunlardan birisi mutlaka bilgisayaranızda olmalı. Ücretsiz , ayarları basit ve etkili bir program olduğu için ben **Zonealarm** isimli programı kullanıyorum. Ancak internette arama yaparak başka programlara da kolayca ulaşabilirsiniz. Zonealarm'ı *http://download.com. com/3000-2092-8034258.html? legacy=cnet* adresinden bulabilirsiniz. Açılan sayfadan **Download Now**ı tıkladığınızda **zonalm2601.exe** isimli dosya indirilecek. İndirme işlemi bitince bu dosyaya çift tıklayın program kurulmaya başlıyor. Doldurmanız gereken bölümleri doldurup devam edin. Ayarları kendisi yapıyor zaten. Artık çalıştırdığınız programlar internete çıkış yapacaklarsa Zonealarm sizden onay isteyecek. Onay vermediğiniz programların internete çıkışı ise engellenecek. Tam tersi durumlarda da yani dışarıdan sizin bilgisayarınıza izinsiz girilmek istendiğinde de uyarı mesajı alacaksınız ve giriş engellenecek.

Artık kolayca **hack** edilemezsiniz. Fakat yine de mümkün. Güvenlikleri için milyonlarca dolar harcayan firmalar ve resmi kurumlar bile bazen hack edilebiliyor. Ancak hackerlar sizinle uğraşarak vakit kaybetmektense, **port**ları sonuna kadar açık ve korunmasız başka birilerini tercih edeceklerdir.

Ve bir kaç küçük tavsiye daha.

- Bilgisayarınızda mutlaka güncellenebilen bir virüs programı bulundurun ve sürekli güncel tutun.
- Tanıdığınız veya tanımadığınız kişilerden gelen, ekinde .exe ve .bat uzantılı beklemediğiniz dosyalar bulunan e-mailleri açmadan silin (geri dönüşüm kutusundan da silin).
- Bilgisayarınıza ne işe yaradığını bilmediğiniz ve güvenilir olmayan üreticilerin programlarını yüklemeyin.
- İnternetten indirdiğiniz veya e-mail ekinde gelen dosyaları virüs programı ile kontrol etmeden açmayın.
- Önemli datalarınızın sık sık yedeklerini alın. Herşey gönlünüzce olsun.

Ecz. Halis MAVİOĞLU