

GÜVENLİK KONUSUNDA SON KULLANICILARIN SIKÇA YAPTIĞI HATALAR VE ÖNLEMLER

Bilgi güvenliğinin sağlanabilmesi amacıyla sistem yöneticileri tarafından yürütülen çalışmalar ve alınan teknik önlemler, son kullanıcının bilinçlendirilmesiyle bütünlük oluşturmakta ve bu sayede yürütülen çalışmalarda yüksek verim alınabilmektedir. Bilindiği üzere, güvenlik açıklarının %80'i, bu açıkları kapatmak için gösterilecek toplam çabanın %20'si ile kapatılabilmektedir. Amacımız, son kullanıcının sıkça yaptığı hataları ve alınabilecek basit önlemleri hatırlatmaktır, bir tür kontrol listesi oluşturabilmektir.

1. Masaüstü bilgisayarlar üzerinde sunucu nitelikli işletim sistemleri

Son kullanıcının kullanımına yönelik masaüstü bilgisayarlar genellikle sunucu nitelikli işler için tasarlanmamıştır. Ancak son kullanıcı tarafından sıkça yapılan hatalardan birisi, işletim sisteminin ne kadar kapsamlı olursa o kadar iyi çalışacağı düşüncesidir. Örneğin Microsoft firması tarafından sunulan Windows Server işletim sisteminin ya da Linux Server sürümlerinin Windows 9x/2000/XP Professional/Home ya da Linux Workstation işletim sistemlerinden daha iyi çalıştığına dair yanlış bir kanı vardır. Sunucu nitelikli işletim sistemleri üzerinde kullanıcının bilgisi dışında otomatik olarak kurulan ve çalışan servisler sistem performansını düşürmekte, ciddi güvenlik açıklarına neden olabilmektedir. Kullanıcıların bu konuda bilinçlendirilmesi ve ihtiyaçlarına uygun nitelikte işletim sistemi kurması/kullanması sağlanmalıdır.

2. Masaüstü bilgisayarlar üzerinde sunucu nitelikli uygulamalar

İşletim sistemleri istemci nitelikli olmakla birlikte (Windows 9x/2000/XP Home/Professional ya da Linux Workstation vb.), kullanıcılar özellikle dosya paylaşım ya da web sayfası sunmak için güvensiz FTP sunucuları ya da web sunucuları kurabilmektedirler. Örneğin web sunucusu olarak Microsoft IIS kullanımının geçmişte ve günümüzde çok ciddi güvenlik açıklarına neden olduğu, CodeRed ve Nima virüslerinin bu yazılımın güvenlik açığını kullanarak yayıldığı bilinmektedir. Bu durumun engellenebilmesi için sunucu nitelikli bu servislerin sistem yöneticileri tarafından merkezi olarak, güvenli işletim sistemleri üzerinde güvenli yazılımlar aracılığıyla verilmesi sağlanmalıdır. Örneğin kullanıcılar kendi kullanıcı hesaplarını kullanarak UNIX sunucu sistemler üzerinde web sayfası hazırlayabilmeli, dosyalarını sunucu sistemler üzerinde çalışan FTP programları ile taşıyabilmelidir.

3. İşletim sistemleri güncellemeleri

Son kullanıcıların sıkça yaptıkları hatalardan birisi, işletim sistemini kurduktan sonra kurulumun tamamlanmış olduğunu ve güvenlik açığı bulunmadığını sanmalarıdır. İşletim sistemlerinin piyasaya sürülmesinin ardından sürekli olarak güncellemeleri çıkmaktadır. Bu güncellemeler bir yandan sürücüler ve sorunlu sistem dosyalarını yenileri ile değiştirirken bir yandan ve daha önemlisi işletim sistemindeki güvenlik açıklarını kapatmaktadırlar. Bazı işletim sistemleri kendi güncellemelerini otomatik olarak kurmakta ya da otomatik kurulum için ayarlanabilmektedir. Virüsler genellikle bilgisayarı güncellenmemiş işletim sistemlerinin güvenlik açıklarını kullanarak etkilemekte ve yayılabilmektedir.

4. Uygulama yazılımları güncellemeleri

İşletim sistemleri yanında bazı uygulama yazılımları da güncellenmedikleri durumda güvenlik açıklarına neden olabilmekte, bu açıklar nedeniyle bilgisayar virüsten etkilenebilmekte, bilgi kaybı yaşanabilmektedir. Özellikle Microsoft Outlook vb. e-posta okuma programları, Microsoft Office paketleri, MSN Messenger ve ICQ gibi mesaj programlarının güncellenmesi gerekmektedir.

5. Masaüstü bilgisayarda yönetici hakları

Masaüstü bilgisayar kullanıcılarının en sık yaptıkları hatalardan birisi kullandıkları bilgisayarın yöneticisi olmayı istemeleridir. Masaüstü bilgisayarların kullanılabilmesi için yönetici haklarına gerek bulunmamaktadır. Bununla birlikte sistem yöneticileri de gereksiz telefonlardan ve yapılan gereksiz açıklamalardan kurtulabilmek amacıyla zaman zaman kullanıcıların bilgisayarları yönetebilmesine izin vermektedir. Son kullanıcının yönetici haklarıyla farkına varmadan yaptığı kurulumlar ya da değiştirdiği konfigürasyon parametreleri bilgisayar üzerinde güvenlik açıklarına neden olabilmektedir.

6. Antivirüs yazılımları ve güncellemeler

Bazı kullanıcılar antivirüs yazılımlarının bilgisayarlarını yavaşlattığını düşünmektedir. Gerçekten de antivirüs yazılımları sistem performansında 0,5-2% arasında düşüşe neden olmaktadır. Bununla birlikte bu performans kaybı virüs bilgisayarı etkilediği zaman bilgisayarın performansındaki düşüşle karşılaştırılamayacak kadar küçüktür. Bu nedenle masaüstü bilgisayarlarda antivirüs yazılımı kullanmak virüslere karşı alınacak ilk önlemlerden birisidir. Bunun yanında kullanıcılar tarafından sık yapılan hatalardan birisi antivirüs yazılımı kurulduktan sonra bilgisayarın virüslere karşı güvende olduğunun sanılması, yazılımın güncellenmemesidir. Kullanıcılar antivirüs yazılımlarının nasıl çalıştığı, yeni çıkan virüsleri nasıl tespit ettiği ve virüs tarama motoru (engine), virüs tanım dosyalarının (virus pattern files) nasıl güncelleneceği konusunda bilinçlendirilmelidir.

7. Dosya paylaşımları

Kullanıcılar dosyalarını ağ üzerindeki diğer kullanıcılarla paylaşırken bu dosyaların herkes tarafından görüldüğünün farketmemektedirler. Bunun yanında belirli dizinleri paylaşım açmak yerine işletim sistemi dosyalarının ve programların bulunduğu dizinleri paylaşım açmakta, parolasız olarak açılan bu paylaşımlar sonucunda bir yandan güvenlik açıkları oluşturmakta, bir yandan ağ üzerinden yayılan virüsler için uygun zemin oluşturmaktadırlar. Kullanıcıların dosya paylaşımlarının riskleri konusunda bilinçlendirilmesi, dosya paylaşımı konusunda daha güvenli yolların sunulması gerekmektedir.

8. Dosya alışverişi

Kullanıcılar Kazaa, Imesh gibi P2P dosya paylaşım programları ya da ICQ gibi mesajlaşma programları aracılığıyla tanımadıkları ve güvenilirliği bilinmeyen bilgisayarlardan aldıkları programları bilgisayarlarına indirmekte ve çalıştırmaktadırlar. Bu programlar virüs ya da truva atı nitelikli olabilmektedir. Bu konuda kullanıcıların bilgilendirilmesi gerekmektedir.

9. Web üzerinde bilinçsiz çalıştırılan programlar

Bazı web sitelerinden bilinçsizce indirilen programlar ve program parçacıkları (plug-in) bilgisayarların virüs veya zararlı bir kod tarafından işgal edilmesine neden olabilmektedir. Bu durumun engellenmesi için kullanıcıların Internet tarayıcı programlarında güvenlik ayarlarını yapmaları, web sayfalarına bağlantı yapıldığında çıkan sorulara ancak anladıktan sonra onay vermeleri gerekmektedir.

10. E-posta eklentileri

Virüs tarafından hazırlanmış, kullanıcının kimden geldiğini bilmediği veya sosyal mühendislik eseri olarak çok bilinen bir kullanıcıdan geliyormuş gibi gösterilen e-postaların eklentilerinin kullanıcı tarafından çalıştırılması çokça görülen ve virüsün bilgisayarı etkilemesini sağlayan basit bir hatadır. E-posta yoluyla yayılan virüslerin bilgisayarı etkilemesini engellemek için antivirüs yazılımları ve işletim sistemleri güncellenmeli, güvenli e-posta okuma programları tercih edilmelidir (Microsoft Outlook yerine Netscape Messenger, Pine, Mutt vb).

11. Güvenlik Standartları (Security Baseline) ve Kullanım Politikaları

Sistem yöneticileri tarafından hazırlanan belgeler, belirlenen politikalar genellikle son kullanıcılar tarafından gereksiz görülmekte, bu belgelerde önerilen güvenlik ayarları yapılmamaktadır. Kullanıcıların, bu standartların önemini anlamaları için bilgilendirilmesi gerekmektedir.