

ODTÜ ANTİVİRÜS ÇÖZÜMLERİ

Mevcut Durum

ODTÜ yerleşkesinde yaklaşık 30,000 kullanıcı, 5,000 civarı tanımlı IP, B-sınıf IP bloğu, Bilgi İşlem Daire Başkanlığı sorumluluğunda UNIX merkezi sunucu sistemler, bölüm koordinatörleri sorumluluğunda bölümlere ait sunucular, ATM omurga ağı, ATM uplink Ethernet bağlantısı aracılığıyla omurga ağına bağlanan yerel Ethernet ağları bulunmaktadır.

Antivirüs Çözümleri:

ODTÜ antivirüs çözümleri iki aşamada incelenebilir: virüs yerleşkede etkili olmadan önce ve virüs yerleşkede etkili olduktan sonra yapılan çalışmalar.

1. Virüs yerleşkede etkin olmadan yapılan çalışmalar

- i. *Antivirüs filtresi* : Merkezi e-posta sunucularındaki antivirüs filtresi açık kaynak kodlu yazılımlar olan SendMail ve ProcMail ile birlikte çalışan GPL lisanslı bir yazılım olan Trophie ve yine GPL lisanslı Virge ikilisinden oluşmaktadır.
- ii. *Elektronik listelerde çalıştırılabilir eklentili dosyalar* : Yeni bir virüs ortaya çıktıktan sonra yaklaşık 6-10 saat içinde virüs tanımını içeren antivirüs yazılımı güncelleme dosyası çıkmaktadır ancak bu süre içinde virüsün yayılım hızını azaltmak amacıyla yapılan çalışmalar kapsamında elektronik listeler yardımıyla yayılmasını engellemek için virüslerin genelde kullandıkları eklentiler liste yöneticisi program tarafından elenmektedir (exe, .pif, .scr vb).
- iii. *Port kısıtlamaları* : Ağ üzerinden yayılan virüsleri engellemek amacıyla belirli portlar üzerinden gerek yerleşke dışı, gerekse yerleşke içinde birimler arası erişim engellenmektedir (135/tcp, 135/udp, 139/tcp, 139/udp, 445/tcp (NetBIOS portları), 1434/UDP (win32/Slammer), 4156/UDP (Linux/Slapper)).
- iv. *Zayıflık taraması testleri*: Zayıflık tarama programları ile yerleşkedeki bilgisayarlar düzenlik olarak güvenlik açıklarına karşı kontrol edilmektedir (Nessus, Retina vb).
- v. *Antivirüs Yazılımları* : Masaüstü bilgisayar için antivirüs yazılımları temin edilmekte, güncel virüs tanımlarını içeren güncelleme dosyalarının yerel ftp sitesinden dağıtılmaktadır.
- vi. *Virüse özel temizleme programları* : Virüse özel olarak antivirüs yazılım şirketleri tarafından hazırlanan küçük boyutlu temizleme programları ortak kullanıma yönelik ftp sitesinden dağıtılmaktadır (fixsobig.exe, fixbugbear.exe vb).

Bu çalışmalar bazı durumlarda özellikle sosyal mühendislik tasarımı sonucunda hazırlanmış virüsleri durdurmakta yeterli olmayabilir (W32/Mimail vb). Bu nedenle bu mekanizmalarla birlikte çalışacak ve insan faktöründen doğacak sorunları engellemeyi sağlayacak mekanizmalara ihtiyaç duyulmaktadır.

- vii. *Bilinçlendirme* : Kullanıcıları masaüstü antivirüs yazılımlarını ve işletim sistemlerini güncel tutma, bilgisayarlarını güvenlik tehditlerine karşı koruyabilecek bilgi seviyesine getirebilmek amacıyla doğrudan kullanıcılara ve bölüm/birimlerde kullanılan bilgisayarlardan sınırlı ölçülerde sorumlu olan bilgisayar koordinatörlerine yönelik eğitimler verilmekte, seminerler düzenlenmektedir.
- viii. *Bilgilendirme* : Kullanıcılar yeni çıkan bir virüs ile ilgili haberleri bilgisayar koordinatörlerine gönderilen e-postalardan ve antivirüs web sitesinden edinebilmektedirler (<http://antivirus.metu.edu.tr>).
- ix. *Geribildirim* : Kullanıcılar kendilerine gelen virüslü mesajları geribildirim adreslerine gönderebilmekte, önlem alınmasını sağlayabilmektedirler (hotline@metu.edu.tr, virus@metu.edu.tr, security@metu.edu.tr).

2. Virüs yerleşkede etkin olduktan sonra yapılan çalışmalar

Yeni çıkan bir virüs için güncelleme dosyası üretilinceye kadar geçen süre içinde virüs yerel ağ üzerinde etkili olabilmektedir. Bunun yanı sıra, gerek güncellemesi yapılmamış işletim sistemlerinin varlığı gerekse bilinçsiz kullanıcıların çalıştırdıkları e-posta eklentileri nedeniyle virüs zaman zaman yerel ağda yayılmayı başarabilmektedir. Virüsün yerel ağ üzerindeki etkisini azaltabilmek amacıyla,

- i. Yerleşke içinde virüs tarafından etkilenmiş bilgisayarın kullandığı IP, e-posta sunucusu üzerinde çalışan virüs filtresi aracılığıyla ya da ağ trafiği denetlemeleri ile belirlenmekte ve sorumlu bilgisayar koordinatörüne iletilmektedir.
- ii. Acil durumlarda virüs tarafından etkilenmiş bilgisayarın IP erişimi kısıtlanmaktadır.

Sonuç:

Virüsler yerleşkede etkin olmadan önce yapılan çalışmalar emek/zaman alan kısım gibi görünmekle birlikte, bu çalışmaların yapılmaması sonucu virüs etkin hale geldiğinde harcanacak çaba ve alınacak risk / bilgi kaybı fazla olacaktır. Bu nedenle öncül tedbirler almak zorunluluğu bulunmaktadır.

Sonucu sistemler üzerinde yapılan çalışmalar zorunlu olmakla birlikte bu önlemler sosyal mühendislik eseri virüsleri durdurmakta yetersiz kalabilmektedir. Bu çalışmaların etkili olabilmesi için kullanıcıların basit hatalar sonucu virüsler tarafından etkilenmesini engellemek ve bilgisayarlarını koruyabilir hale gelmelerini sağlamak amacıyla belirli bir bilinç düzeyine çıkarılması gerekmektedir. Bu nedenle kullanıcı eğitimi, öncül çalışmalar kadar önem taşımaktadır.

Antivirüs çözümleri, firmalar tarafından üretilen paket çözümlerle sınırlı değildir. ODTÜ, sonucu sistemler üzerinde yapılan çalışmalarda gerek üniversite olmanın getirdiği araştırmacı yaklaşım, gerekse firma tekeli/bağımlılığının önüne geçebilmek amacıyla özellikle açık kaynak kodlu yazılımları tercih etmektedir.