Antivirüs Temelleri

Ar. Gör. Enis Karaarslan,
Ege Üniversitesi Kampüs Network Yöneticisi

Bilgisayarımıza zarar veren program kodları aslında en ciddi güvenlik problemlerinden birisi olmaya başladı. Virüs, worm, trojan, spyware ...vb, özetle zararlı program kodları. Eskiden sadece disketlerle bulaşan bu kodlar, artık Internet'in hemen her protokolünü kullanarak makinanıza girmeye çalışıyorlar. Girdiğiniz bir web sayfasından, gelen bir elektronik postadan ve eğer düzgün ayarlanmamışsa paylaşıma açtığınız bir klasör yoluyla makinanıza bir davetsiz misafir misali geliyorlar. Bu nedenle artık günümüzde her bilgisayarda bir antivirüs yazılımı bulunması gerekiyor.

Bu zararlı program kodları bir takım kişiler tarafından yazılıyor. Çok değişik söylentiler var, Rus-Doğu Avrupa'dan Hacker'lar tarafından ya da Antivirüs firmaları tarafından hazırlandığı gibi. Kim tarafından hazırlanırsa hazırlansın, sonuçta ciddi bir antivirüs pazarı yarattıkları kesin. Peki hangi antivirüs yazılımını seçmeli? Bu konuda Olmypos'un forumlarında tartışılanları biraz derledim, kendi düşüncelerimi de ekleyerek size iletmek istiyorum.

Ben kullanıcıları Norton'cular ve Norton düşmanları olarak ikiye ayırıyorum. Özellikle eskiden "Norton Disk Doctor" programı ile deneyim yaşayanlar ciddi bir sempati duyuyorlar Norton'a. Bir de Norton'un sisteme yavaşlık kattığını ve virüsleri temizleyemediğini düşünen ikinci taraf var. Aslında olay bu kadar basit değil. Her ne kadar Norton ("Symantec" eklemeyi unutmayalım) medyayı iyi kullanan bir firma olsa da piyasada çok ciddi rakipleri var. Bunun yanı sıra, antivirüs yazılımları arasında bir uçurum olmadığını ve gerçekten de ürünlerin birbirine yakın sonuçlar sunduğunu düşünüyorum. Ortalama başarı yüzdesi %95 – %99 arasında değişmektedir. Örneğin birisi %98 başarılı olurken, diğeri %99 başarıya ulaşmaktadır.

Kurumsal ağlarda, yerel ağla dış ağ arasında kurulan sistemlerle ağ trafiği üzerinde zararlı program taraması yapılabilir. Bu ağ tabanlı antivirüs sistemleri; HTTP, FTP ve SMTP gibi veri trafiklerini üzerinden geçirerek zararlı program taramasını yapmayı ve kullanıcıya gelmeden önce virüslerden temizlemeyi hedeflemektedir. Ne kadar iyi sistemler kurulsa da virüs taraması bir miktar yavaşlığa yol açacaktır. Büyük ağlarda, DNS ile entegre çalışan ve sadece elektronik posta (smtp) trafiğini tarayan sistemler tercih edilmelidir. Bu tür ağ tabanlı sistemler kurulsa da, her kullanıcının makinasında bir antivirus yazılımı bulunmalıdır. Kullanıcıların kurumsal antivirüs çözümünü kullanması sağlanmalıdır. Kampüs ağında, kullanıcıların bir web sayfasına bağlanıp sadece bir link'e tıklayarak makinasına antivirüs kurması sağlanmalıdır. Kurulacak imza dağıtım sunucusu ile, kullanıcıdan bağımsız otomatik güncelleştirme yapılmalıdır. Özellikle kurumsal ağlarda antivirüs çözümlerine giderken kıstaslar aşağıdaki gibi özetlenebilir:

1.Tanımlanmamış virüsleri bile tanımlayabilme (Heuristic): Bu özelliğinin yani bir nevi Yapay Zeka'sının gelişmiş olması gerekmektedir ki yeni virüsler tanınabilsin.
2.Virüs Temizleme: Tabii ki tespit yeterli değil, virüsleri de temizleyebilmelidir.
3.İmza Dağıtım Sunucusu: Kurumsal kurulumlarda imzayı merkezinden çekecek ve kullanıcılara en kısa zamanda dağıtacak sistemi desteklemesi. İmzaların otomatik güncellenmesi, uzaktan antivirüs tarama gibi opsiyonların eklenmesi daha güvenli bir yapı sağlayacaktır.
4.Web üzerinden kolay kurulum,
5.Ufak güncelleme paketlerine sahip olması,
6.Performans: Hızlı olması ve az sistem kaynağı harcama,

7.Makinanın kapatılıp tekrar açılmasını gerektirmeyen güncelleme,
8.Kullanımdaki windows sistem dosyalarını tarayabilme,
9.Sıkıştırılmış (compressed), kriptografik, polimorfik hatta metamorfik virüsleri yakalayabilme,
10.Kurumsal destek: Yazılımda ulaşabilecek hataların çözümünün ve teknik güncelleme desteğinin sağlanması,
11. Trojan, spyware gibi yazılımları da tespit ve engelleme yeteneği,
12. POP3 desteği,
13.Yıllık güncelleme ücreti.

Açıkçası burada ilk alım fiyatını dile getirmedim. Unutulmaması gereken şudur, önemli olan antivirüs'ün ilk alım ücreti değil, sonraki senelerde güncelleme için ne kadar ücret ödeneceğidir. Antivirüs, virüs tanıma motoru(engine) ve tanıma imzaları(signature) ile bütündür ve güncel olması gerekir. Bu da farklı firmaların ürünlerinde, aslında çok da farklı olmayan yıllık ücretler anlamına gelebilmektedir. Binlerce makinaya kurulan bir yazılımın bir başkasıyla değiştirilmesi, özellikle domain yapısı yoksa, hiç de gözüktüğü kadar kolay değildir. İlk karar aşamasında yazıda dile getirdiğimiz unsurlar dikkatle ele alınmalıdır. Bir ürün, ömür boyu imza güncellemesine sahip olabilir ama bu durumda virüs tanıma motoru(engine) ve programın yeni sürümleri sağlanmayacaktır. Bu da yeni tür virüslerin tanın(a)maması anlamına gelebilecektir.

Virüsler hakkında kurumsal ağlarda dikkat edilmesi gereken diğer noktalar ise özetle şunlardır:

- Mail sunucularda eklenti kontrolü yapılmalı ve (.exe, .bat, .pif, .scr, .vbs ... vb) uzantılara sahip eklentiler otomatikman silinmelidir. Geçtiğimiz yıllara kadar bu tür uzantıların silinmesi ile virüslerin çoğu bloklanabiliyordu, şu an ise virüsler .zip gibi uzantılarla geldiğinden eklenti bloklaması bu türler için geçersiz kalmaktadır.
- Kullanıcılar bilinçlendirilmeli, kendilerine gelen eklentileri açarken dikkatli olmaları gerektiği hatırlatılmalıdır. Örneğin bu bir .zip dosya ise, öncelikle gönderenden bu dosyanın içeriği teyit edilmelidir.
- Kullanıcıların sistemlerinin güvenlik güncellemelerini düzenli olarak yapmaları sağlanmalı, mümkünse yama yönetimi yapılmalıdır. Yama yönetimi hakkında detaylı bilgi için: http://agguvenligi.hakkindabilgi.com/
- Eğer virüsler belirli bir tcp/udp port üzerinden yayılıyorsa, ağ üzerinde bu porttan iletişimin engellenmesi için gerekli erişim listeleri devreye alınmalıdır.
- Virüslü makinaların tespiti ve karantinaya alınma sürecinin nasıl olacağı belirlenmelidir. Örneğin ağ erişiminin kısıtlanması, sadece antivirüs kurulum makinasına erişim yapmasının sağlanması ve antivirüs yazılımı kurulduktan sonra merkezden taranması gibi süreçler belirlenmelidir.
- Mümkünse virüs yayılmasını kolaylaştırılan protokollerin (netbeui...vb) kullanılmaması sağlanmalı, yazıcı paylaşımı için IP Printer'lar, dosya paylaşımı için domain sunucular – dosya sunucuları kullanılmalıdır.
- Bilgisayar kullanırken yönetici(admin) kullanıcısı yerine kısıtlı hakka sahip kullanıcı hesapları kullanılmalıdır. Böylece zararlı kodların kalıcı olarak bilgisayar üzerine kendini kayıtlaması engellenebilecektir.

Antivirüs yazılımları, özellikle kişisel güvenlik duvarı ve saldırı tespit sistemleri ile birlikte tek bir ürün olarak satılabilmektedir. Bu durumda özellikle trojan'lar engellenebilmekte, msn gibi

sohbet programları ve dosya paylaşım programları üzerinden gelebilecek saldırılara karşı sistem daha güvenli tutulabilmektedir.

Virüsler hakkında güzel bir kaynak için Virüs Bulletin http://www.virusbtn.com sayfası incelenebilir. Verdiğimiz bilgiler ışığında, internetten ulaşabileceğiniz çeşitli test raporlarını da inceleyerek kurumunuz veya kişisel kullanımınız için en iyi ürünü kendiniz seçebilirsiniz.