Yazılım Açıkları

Bilg. Y. Müh. Tahir Emre Kalaycı
emre.kalayci@emo.org.tr

17.12.2008 tarihinde basında ve televizyonlarda Internet Explorer yazılımında bir açık olduğu haberi yoğun bir şekilde yer aldı. Haber içeriğinde dünyanın en çok kullanılan internet tarayıcısı olan "Microsoft Internet Explorer" ürününde ortaya çıkan bir açık yardımıyla "kötü" kullanıcıların bilgisayar üzerinde diledikleri gibi kod çalıştırabilecekleri ve böylece bilgisayardaki tüm önemli verilere ulaşabilecekleri söylendi. Basında Microsoft'un kullanıcılara geçici olarak başka bir tarayıcı kullanmalarını önerdiği iddiaları yer aldı[1,2,3,4].

Yazılımlar insanlar tarafından üretilen, insan hatası veya başka nedenlerle hatalar, açıklar barındırabilir. Bu hataların ve açıkların olması bütün yazılımlar için olasıdır. **Önemli olan yazılımı üretenlerin bu açıkların ve hataların az sayıda olmasına ve ortaya çıktığı zaman en kısa sürede kapanmasına yönelik olarak gösterdiği çabadır.** Basının daha sonra duyurmasıyla yoğun bir çalışma sonucu Microsoft'un kısa süre içinde açığı kapatan yamayı yayınladığını öğrendik. Microsoft zamanında müdahale ederek açığı kapatmış oldu [5]. Acaba açık gerçekten kapandı mı?

İşte bu noktadaki kilit soru budur. Microsoft'a güvenimizi sorgulayan bir soru. Çünkü açığın kapanıp kapanmadığını anlamak için kaynak kodu açıp incelememiz olanaklı değildir, sadece o açığı devreye sokan işlemleri gerçekleştirip deneyebiliriz. Peki açık geçici olarak "görünmez" hale getirildiyse? Şeytanın avukatlığını yaparak sorduğumuz sorular, kapalı ve sahipli yazılımların aslında güvenilir yazılımlar olup olmadığını sorgulamayı barındırmaktadır.

Bu noktada Microsoft'un Internet Explorer tarayıcısının ne kadar güvenli olduğu sorgulanmaya başlarsa, güvenlik firmalarının yaptığı çalışmaları incelemesi gerekmektedir. Secunia firmasının web sayfasındaki sık kullanılan tarayıcılara yönelik açık ve açıkların kapanma oranı bilgisi aşağıdaki tablodan incelenebilir (Tablo-1).

Yazılımlar	Rapor Sayısı	Açık Sayısı	Yamalanmayan Rapor Sayısı
IE 7	33	70	9
IE 6	135	142	22
Firefox 3	8	39	1
Firefox 2	29	154	3
Opera	21	42	0
Google Chrome	0	0	0
Windows Vista	51	80	6
Ubuntu Linux 8.10	26	72	0
Fedora 9	160	357	0
Kaynak : http://secunia.com/advisories			

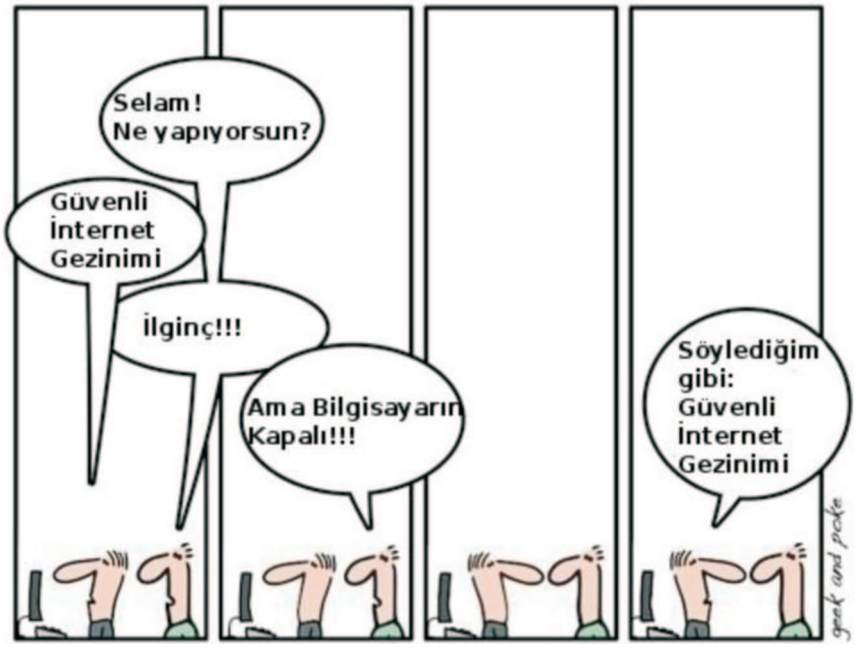
Tablo 1. Güvenlik raporu, açık ve yamalanma sayıları

Bu tablo incelendiği zaman, en fazla açığın hangi yazılımda çıktığı ve açıkların kapanma çalışmasının hangi yazılımlar üzerinde daha çabuk yapıldığı gibi bir öngörüye sahip olunabilir. İnsanlar herhangi bir tanıtımın etkisi altında kalmadan hangi tarayıcının daha güvenli olduğunu bu tip firmaların çalışmalarıyla değerlendirmektedirler(*).

Kullanıcıların dikkat etmesi gereken çalışmalar, "tarafsız" firmaların bu tür çalışmaları gibi olmalıdır. Açıklar oluşabilir, önemli olan bu açıkların az sayıda olması ve en kısa sürede kapatılmasıdır.

Güvenlik?

Genel olarak önerdiğimiz güvenlik önerileri neler olabilir? **Öncelikle virüs, solucan, truva atı vb. saldırılara karşı daha güvenli ve güvenilir olan [6,7] özgür ve açık kaynak yazılımların kullanılması gerekir.** Özgür ve açık kaynak kodlu yazılımlar, kaynak kodunu



inceleyebildiğimiz için şeffaflığı sağlamaktadır. Yapılan bir araştırmada [8] kusurlar açısından yapılan analizde, değişme oranı veya değiştirilen işlevlerin toplam işlevlere oranının açık kaynak projelerinde kapalı kaynak projelerine göre yüksek olduğu bulunmuştur. **Bu sonuç kusurların açık kaynak projelerinde kapalı kaynak projelerine göre daha hızlı bulunup çözüldüğü hipotezini desteklemekte ve açık kaynak yazılım geliştirme modeli kullanmanın ek bir faydası olarak görülebilmektedir.** Yapılan her değişikliği, yapılan her işlemi, eklenen her kodu açıp inceleyerek ne kadar güvenli olduğunu kendiniz ölçebilirsiniz. Açık kapandı denildiği zaman gerçekten açığın kapanıp kapanmadığını sadece deneyerek değil, hatanın oluştuğu ilgili kodu inceleyerek de öğrenebilirsiniz (internet üzerinde aynı yazılımı kullanan daha uzman kişiler hataları, yamaları ve hataların çözülüp çözülmediğini izliyor). Bütün bu nedenlerden dolayı GNU/Linux işletim sistemini; virüslere, solucanlara, diğer güvenlik sorunlarına karşı kullanıcılara öneriyoruz. Sadece bu yazılımları kullanmak güvenliği sağlamaya yetecek mi? Çoğu sorunu önlese de yetmeyecektir. Kullanıcıların ayrıca internet kullanırken her zaman için güvenliği en üst düzeyde göz önünde bulundurmaları gerekiyor. Güvensiz sitelere girmemeleri, güvensiz yerlerden indirilmiş dosyaları kullanmamaları, güvensiz kişilerden gelen postalara inanıp, postada yazılanları uygulamamaları gerekmektedir. Güvenliğin birinci koşulu kullanıcının öncelikli olarak güvenliği düşünerek interneti kullanmasıdır.

Bilişim, barındırdığı verilerin korunması mühendisler ve kullanıcılar açısından son derece hassas irdelenmesi gereken bir konudur. Bu tür önemli bilgilerin bulunduğu her bilgisayarın ve bu bilgisayarlarda bulunan yazılımların özgür ve açık kaynak kodlu olması güvenilirlik açısından önemlidir. Özgür yazılım olarak adlandırılan şeffaf yazılımlar, tamamen topluma mal edilerek üretildiği için insanların ve kurumların ücretsiz biçimde kullanmaları olanaklıdır. Ayrıca istenen teknik destek gibi hizmetleri de istenen kaynaktan sağlama konusunda, özgür yazılımları kullanarak iş kurmak, yeni yazılımlar geliştirmek gibi konularda da koşulsuz özgürlük bulunmaktadır. Türkiye'de ve dünyada milyonlarca kişi bu yazılımların geliştirilmesi için çalışmaktadır. Elektrik Mühendisleri Odası uzun yıllardır bir çok platformda özgür yazılımları desteklemekte, özgür yazılım geliştiren ve yaygınlaştırılmasına destek olan üçüncü kişilerle birlikte çalışmaktadır[9]. Bütün kullanıcıları güvenli bilgisayar ve internet kullanımı pratiklerine uymaya ve güvenli olduğu araştırmalar tarafından da desteklenen GNU/Linux kullanmaya çağırıyoruz.

(*)Ayrıntılı bir tablo için :
http://en.wikipedia.org/wiki/Comparison_of_web_browsers#Vulnerabilities

Kaynaklar

[1] Explorer'da açık var rakip yazılım kullanın, 17.12.2008,
[2] İnternet Explorer'da Ciddi Açık, 13.12.2008,
[3] İnternet Explorer'da çok kritik güvenlik açığı, 16.12.2008,
[4] İnternet şifreleri tehdit altında, 17.12.2008,
[5] İnternet Explorer'daki açık nasıl kapatılır?, 19.12.2008,
[6] Trend Micro: Open source is more secure, 13.06.2007,
[7] Free Software is More Reliable!,
[8] Succi, Paulson, Eberlein. An Empirical Study of Open-Source and Closed-Source Software Products, IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, V.30/4, april 2004
[9] Bilişimde güvenlik ancak şeffaflıkla sağlanır,