Işletim Sistemlerinde Güvenlik Tartışması

Linux mu daha güvenli Windows mu?

Huzeyfe ÖNAL <huzeyfe@lifeoverip.net>

12/4/2009

[Bu yazı günümüzde yaygın kullanılan işletim sistemlerinin güvenlik yönünden yorumsal karşılaştırmasını içermektedir. Tartışmaya daha çok açık kod, kapalı kod, yazılım yönünden bakılmıştır.]

Not: Bu yazı bugüne kadar çeşitli amaçlarla kullandığım işletim sistemleri üzerinde edindiğim tecrübelerin sonucudur ve kesin doğruluk içermez.

Cevap aradığımız sorulardan bazıları;

- Bir işletim sisteminin güvenliğini hangi unsurlar belirler?
- Güvenlik düzey belirlemesi için standart var mı?
- Açık kodlu olmak bir sistemi daha güvenli kılar mı?
- Bir sistemin daha yaygın olması daha fazla açıklık aranmasına sebep olur mur?

Güvenlik denilince olaya tek bir noktadan bakmak yanlıştır, bir işletim sisteminin ağ yapısı oldukça zayıf tasarlanmış olabilir fakat çok kullanıcılı yapısı üzerinde kullanıcı haklarında ileri düzey kontrol ve güvenlik imkanları sağlamış olabilir. Bunun için karşılaştırma yaparken tek bir noktaya odaklanmak yerine resmin genelini değerlendirmek daha doğrudur.

Yazılımlar insan ürünüdür ve insan, doğası gereği hata yapar(yapabilir değil, yapar). Önemli olan hatanın ne kadar sürede giderilebileceği ve sonuçlarının neler olacağıdır.

Bir yazılımcı hata yapar , yazdığı program istenildiği gibi çalışmayabilir. Bu, çoğu zaman kısa sürede giderilebilecek bir eksikliktir. Fakat bir protokolün tasarımında ya da yazılımın tasarımında hata yapılırsa bu kolay kolay giderilebilecek bir husus değildir.
Nitekim son yıllarda özellikle Microsoft Windows işletim sisteminin tabiri caizse göbeğinde çıkan açıklar kanımca tasarım ve tasarımın getirdiği yazılımsal eksikliklerdendir. Öyle olmasa çıkan bir açığın kapatılması ardından , açığı istismar için yazılmış kodlarda yapılan değişiklikler ile işletim sistemi aynı açıktan defalarca etkilenmezdi.

Aynı şekilde Internet trafiğini üzerinde taşıyan işletim sistemi IOS'da çıkan ve bazı işletim sistemlerinde(OpenBSD) yıllar önce giderilmiş olan basit mantık hataları bugün varolmazdı.

İşletim sistemlerinde güvenlik düzeyini belirleyen resmi, yansız bir kurum yok. Aslında var ama günümüz işletim sistemlerini analiz etmekten çok uzak bir yapı. Bu sebeple işletim sistemlerinin firmaları genellikle çeşitli güvenlik firmalarına testler yaptırarak en güvenli işletim sistemlerinin kendilerininki olduğunu söylerler.

Burada atlanılan diğer bir konuda, işletim sistemi güvenliğine sadece yazılımsal olarak bakmaktır. Oysa birçok sistemin temel olarak kullandığı donanım mimarisi üzerinde yazılabilecek programların özelliklerini kısıtlar. Mesela günümüzde güvenlik açıklarının büyük çoğunluğunun sebebi Buffer overflow denilen bellek taşırma hadisesidir. Bir VMS sistem üzerinde kullanılan dile bağlı olarak Buffer overflow yapmak imkansızdır. Zira yazılımın üzerinde koştuğu donannım mimarisi bunu engellemektedir.

Açık Kaynak Kodlu sistemler neden daha güvenlidir?

Ya da tam tersi..

Son yılların popüler ama bilinçsizce(?) yapılan tartışmalarından biri de açık kod yazılımlar üzerinedir. Bu tartışmada taraflar genelde ikiye ayrılarak siyah ve beyazı oynamaktadır.

Bir taraf için bu sorunun cevabı tartışılmayacak kadar kesindir. Ever açık kaynak kodlu bir ürün her zaman kapalı koddan daha güvenlidir... Diğer taraf da kendince öne sürdüğü kıstaslara göre açık kodlu yazılımların kesinlikle güvenli olamayacacığını belirtir.

Bu tartışmada 3. olarak sayılabilecek ama sesi cılız kalan bir taraf daha vardır. Bu taraf ise yazılan bir sistemin açık kaynak kodlu olmasından öte yazılanın nasıl yazıldığını irdeler ve sistemden ziyade onu yönetinin güvenlikde daha önemli rol oynadığına inanır.

Eğer bir yazılım gerçekten iyi tasarlandı ve yazılan kodlar işini bilen mühendisler tarafından incelendi ise bu yazılımın güvenli olması için kodlarının açık olması gerekmez. Önemli olan yazılımın ne amaçla yazıldığıdır.

Siz bir Firewall'u musterileriniz kolay kullansın önceliği ile tasarlar sonrada hayata geçirirseniz, müşterileriniz kolayca kullanacaktır fakat olaya müşteri gözü ile bakmayanlar (hackerlar) daha farklı şeyler bulacaklardır…

Bir sistemin, yazılımın açık kaynak kodlu olması birçok avantajı yanında getirir. Genel olarak bakıldığında dezavantaj oluşturacak bir yanı yoktur. Yazılan kod işini bilen, bilmeyen onbinlerce(?) insan tarafından incelenerek belirli bir olgunluğa daha kısa sürede ulaşır. Eğer bu kapalı kod üzerinde sağlanabilirse aynı oran o yazılım için de geçerlidir.

Belki amatör bir düşünce ama yazılımın amacı kalitesini belirler. Bir tarafta patronun soluğunu ensesinde hisseden yazılımcı, bir an önce bitsinde nasıl olursa olsun düşüncesinde. Diğer yanda bu işten zevk alan , belki normal işinin haricinde geceleri uykusundan zaman ayırarak bu işi yapan yazılımcı.

Bunun için de önemli olan yazılımın esnekliği, tasarımıdır. Önünde kaygısı yok, hep daha iyi nasıl yapabilirim düşüncesi var. Ortaya çıkacak yazılımların kalitesi biraz da buna bağlıdır...

Yaygın kullanım ne getirir?

Linux mu daha güvenli Windows mu? tartışmalarının ana konularından biri de yaygın kullanım oranıdır. Genelde savunulan, bir işletim sisteminin yaygın kullanılması onun daha fazla insan tarafından kurcalanması, risk altında olması demektir. Bu fikir itiraz kabul edilmeyecek kadar doğrudur. Bu çerçeveden bakıldığında windows işletim sistemlerinde çıkan açıkların Linux sistemlerden çok olması doğaldır. Fakat burada genellikle hesaba katılmayan bu açıkların öyle bilgisayar meraklısı gençler tarafından rastgele bulunmadığıdır.

Bu açıkları bulmak(basit olanları değil) genellikle o konu üzerinde ileri düzey bilgi gerektirir. Ve işletim sistemlerinin mazisine baktığımızda UNIX sistemlerden anlayan "uzmanların" daha çok olduğunu görebiliriz. Gerçi günümüzde olay biraz daha farklı mecralarda seyrediyor, insanlar para için ya da farklı amaçlar için uzmanı oldukları konularda işletim sistemlerini, yazılımları zorluyorlar ve buldukları açıkları internette paylaşıyorlar.

Sonuç olarak bir işletim sisteminin yaygın kullanılması onun daha fazla risk altında olduğunu gösterir fakat çıkan açıkları tamamen bu sebebe bağlamak işin kolayına kaçmak olur.

Hangisi daha güvenli?

Yukarıda açıklamaya çalıştığım temel bilgiler ışığında günümüzdeki işletim sistemlerinin çoğu sınıfta kalıyor…

Öncelikle Microsoft firması ağzı güvenlik yönünden çok yandığı için bu konuya oldukça önem veriyor. Yeni nesil işletim sisteminin çıkış tarihini de eklenecek güvenlik özellikleri sebebi ile erteliyor..Windows 2003 Microsoft'un güvenliğe ne kadar önem verdiğinin iyi göstergelerinden. İşletim sistemi kurulduğunda default olarak herhangi bir servis aktif edilmiyor… Web sunucusu aktif edilecekse içerisinde istismar edilebilecek scriptler vs kaldırılmış.

Bütün bunlar kullanıcı tarafında zorluk çıkaracak işlemler. Mesela sistem yöneticisi web sayfasında asp çalıştırabilmesi için A modülünün yüklü olması gerektiğini bilmelidir.

Benzer durumları Linux dünyasında da görmek mümkün, işletim sisteminin çekirdeği olan "Linux" için bunu söylemek o kadar kolay olmasa da Linux'u çekirdek olarak kullanan dağıtımlar genelde kötü durumda. Bunlar genellikle kalitesiz yazılımların denetimsiz bir şekilde işletim sistemine eklenmesinin sonucu. Hatırladığım kadarı ile Fedora Linux işletim sisteminin bir sürümünde ilk çıktığı gün 16 adet yama çıkarılmıştı.

Red Hat, Ubuntu, Debian, Slackware gibi işini daha ciddiyetle yürüten Linux dağıtımlarında durum biraz daha iyi. Bu projeler genellikle belirli sorumluluklar altında geliştirildiği için sisteme eklenecek yazılımların kotnrolü daha iyi bir şekilde yapılmaktadır.

Resmin diğer yarısında ise başka işletim sistemleri var. Özgür UNIX dağıtımı BSD'ler... Her biri farklı ve öz bir amaç için yola çıkmış bu işletim sistemleri ticari kaygıdan uzak bir şekilde yollarına devam etmekteler.

İşlerini iş olsun, göz doldursun diye değilde gerçekten o işi yapmış olmak için yaptıklarından çok bilinmiyorlar. Bunların içinde temel amacını güvenlik olarak belirlemiş ve bugüne kadar yaptıkları yapacaklarının teminatı olmuş bir işletim sistemi var: Adı OpenBSD.

Yazdıkları her satır kodu tekrar tekrar inceleyen, bir yerde suistimale yer veren bir kod bulduklarında tüm sistemi bu kod için tarayan hatta bunu daha da geliştirip işletim sisteminin derleyicisine ekleyen bir sistem… Sitesinde yazdığı gibi "108 yılda uzaktan iki güvenlik açığı".

OpenBSD gerçek güvenlik arayanların birgün mutlaka uğrayacağı, uğramak zorunda olduğu bir işletim sistemi olarak biz güvenlik uzmanlarını bekliyor.

Kaynaklar

http://www.linuxplanet.com/linuxplanet/interviews/4495/1/
http://www.operatingsystems.net/
http://www.theregister.co.uk/security/security_report_windows_vs_linux/
http://www.commercialventvac.com/~jeffs/OS_comparison.html