Yama Yönetimi

Ar. Gör. Enis Karaarslan, enis.karaarslan@ege.edu.tr
Ege Üniversitesi Kampüs Network Yöneticisi

Patch(yama), yazılım üreticisi şirketlerin, yazılımları güncellemek ve/veya hatalarından arındırmak için hazırladıkları paketlere verilen isimdir.
Özellikle kurumsal ağ yönetiminde, ağ elemanlarının yazılımlarının takip edilmesi ve yama uygulanmasında bazı yöntemlerin kullanması gerekmektedir.

Yamasız Bir Dünya?
Buna özetle ütopya diyebiliriz. Sistemler hiçbir zaman mükemmel değil, olmayacaklar da. Günümüzün şartları, yazılımların çok hızlı üretilmesini ve ne yazık ki yeterince test edilmeden kullanıma geçmesine yol açmaktadır. Yazılımlardaki hatalar yamalarla giderilmekte veya yazılımların yeni sürümleri ortaya çıkmaktadır. Ne yazık ki bu yamaların güncellenmesi çoğunlukla kullanıcının insiyatifine bırakılmaktadır.

Yamaları yüklesek mi, yoksa idare mi etsek?
Aslında bu bir ağ yöneticisinin en büyük sorunlarından biridir. Yamasak mı yoksa bir süre daha mı idare etsek ("Bir sistem çalışıyorsa bırak çalışsın" mı?) ? Acaba yamalar sistemi yavaşlatır mı, yoksa sistem göçer mi? Sistemim güncel (up-to-date) mi? Özellikle büyük ağlarda, takip edilecek birçok sistem olunca bu ciddi bir sorun olarak karşımıza çıkıyor. Sistemde bir açığın bile olması, ağın yavaşlamasına veya çökmesine yol açabilecek bir saldırı için bir başlangıç noktası olabilir.
Bu konuda bazı sistem yöneticilerine bir anket uygulandı. Cevap veren sistem yöneticileri, sistem açıklarının yönetimi konusunda bilgili olmakla beraber, yapılan uygulamalarda bazı eksikliklerin olduğu görülmekte. Bu yazıda bu eksiklerin giderilmesine yönelik bazı önerilerimiz olacak.

Yamalar Sistemi Yavaşlatır Mı?
Her yüklenen yamanın, sistemleri bir miktar yavaşlattığı doğrudur. Bu durumda, yama yüklenme kararından önce şu iki tercihten birisi yapılmalıdır; güvenlik (makinanın kendi kontrolümüzde çalışması) veya biraz daha yavaş çalışmak.
Tabii ki bu durumda, sisteme gereksiz yamaların yüklenmemesi daha iyi bir tercih olacaktır. Özellikle sunucularda, kullanılmayan servislerin kaldırılmasıyla o servisler için gereksiz yere yama yüklenmesi de engellenmiş olacaktır.

Güvenlik Açıklarından ve Yamalardan Haberdar Olmak
Kullanılan ürünler hakkında haber listeleri, forum ve web sayfalarının düzenli olarak takip edilmesi gerekmektedir. Bu bilgi kaynaklarının (nispeten) güncel bir listesine http://bornova.ege.edu.tr/~enis/guvenlik/bookmark.html adresinden ulaşabilirsiniz.

Yama Geçerken Dikkat Edilmesi Gerekenler
Özellikle kritik sistemlere yama geçerken dikkat edilmesi gerekenler:
1. Önce benzer bir sistemde test edilmelidir. Test başarılıysa 2. aşamaya geçilir.
2. Yama geçmeden Öncelikle var olan sistemdeki verilerin yedeği alınmalıdır.
3. Yama işlemi mesai saati dışında yapılmalı, sistem kullanıcıları yaşanacak kesintiden haberdar edilmelidir.
4. Her türlü aksilik de göz önünde bulundurularak, sistemin çalışmaması durumunda yerine konulacak yedek bir sistem hazırda bulundurulmalıdır. Bu durumda uygulanan yamanın geri alınması, yedeklerden sistemin eski haline getirilmesi gerekebilecektir.

Yama Yönetimi Programları

- **Otomatik Güncelleştirme:** Kişisel sistemlerin (Windows, Linux ...vb) sık sık güncellenmesi gerekecektir. Kişisel sistemlerde, kritik yamaların otomatik alınması için ayar yapılabilmektedir. Windows makinalarda bu "auto update" ayarları yapılarak otomize edilebilmektedir. Debian'da "apt-get update", "apt-get upgrade" komutlarıyla sistem güncel tutulabilir. Bu komutlar cron ile çalıştırılarak otomatikleştirilebilir. Her makinanın tek tek yama alması bazı sorunlar getirmektedir:
    - Her makinada bu tür ayarların yapılmamış olma olasılığı
    - Gereksiz yere bandgenişliği harcaması (Proxy sistemleri kullanılarak aşılabilir)
    - Yeterince hızlı olmaması
- **Merkezi Dağıtım:** Kurumsal ağlarda bu yamaların merkezi bir makinaya çekilmesi ve buradan diğer makinalara dağıtılması daha iyi bir çözüm olarak karşımıza çıkmaktadır. Bu aynı zamanda hangi makinalarda yamaların geçildiğinin takibi açısından da önemlidir. "Active directory" kullanılan ortamlarda, sistemlerin domain yöneticisi üzerinde kurulu SUS'dan (Smart Update Services) otomatik güncelleme alması sağlanabilir. "Active directory" olmayan ortamlarda yine de bu tür bir hizmetin çalışmasını sağlayan çeşitli ücretli yazılımlar bulunmaktadır. Tabii ki bu tür sistemlerin çalışması için her makinaya tek tek kurulmaları gerekecektir.

Sisteminizde Bütün Yamalar Güncel mi?
Aslında buna tam bir cevap vermek çok da mümkün değil. Ama yine de zafiyet tarama programları (vulnerability assessment tools) kullanılarak ne tür güvenlik yamalarının eksik olduğunu tespit etmek mümkündür. Bunu da önümüzdeki bölümlerde ele almaya çalışacağız.

SONUÇ
İşletim sistemlerinin, üzerlerinde çalışan servis yazılımlarının, ağ cihazlarının yazılımlarının güvenlik açıklarının, özellikle kritik olanların yama (patch) yüklenmesi gerekecektir. Yukarıda anlattığımız esaslara dikkat edilmesi durumunda, daha sağlıklı çalışan sistemlere sahip olmamız mümkün olabilecektir.