



Geçmişten günümüze güvenlik:  
Peki ya gelecek?

Labris Teknoloji

Tarihçiler, insanoğluna kötülüğün bulaşmasını Kabil'in Habil'i öldürmesine dayandırır. Ve ardından bugünlere yaklaştıkça, insanların kendilerini güvende hissetmemeleri için sebepler çeşitlenmiş ve insanoğlu kendini güvende hissetmek için devamlı yeni arayışlar içine girmiştir.



Kapıların gece-gündüz açık bırakıldığı günlerin artık geçip gittiği gibi, bilişim sistemlerinin, bunların bulunduğu ağların kapılarının da açık bırakıldığı günler de geçip gitmek zorundadır.

Bundaki motivasyonumuz ise yalnızca ve yalnızca sistemimizin çalışırılığının güvence altında olması değil, aynı zamanda verinizin ve sırlarınızın da güvenliği olmalıdır.

Bir ağ topolojisinde birçok bileşen olabilir. İnternet altyapısı sunucularından aktif cihazlara, özel uygulamaların üzerinde koştuğu sunuculardan kullanıcı masaüstlerine kadar tüm bileşenleri içeren bir güvenlik politikasının oluşturulması zorunlu hale gelmiştir.

Sistem güvenliği çalışmaları, danışmanlık hizmetleri ile güvenlik politikalarından başlayarak en uca doğru her adımda maksimum gözden geçirme ile gitmek zorundadır.

Güvenlik politikası hem kullanıcıların nasıl hareket etmeleri gerektiğini belirlerken diğer yandan da açıkça güvenilecek ve güvenilmeyecek nesnelere tanımlamalı, güven seviyelerini belirlemelidir. Bir güvenlik politikası ancak uygun güvenlik araçları ile desteklendiği zaman tam olarak çalışır duruma konabilir.

Bu güvenlik araçlarını, ateş duvarları, güvenlik tarayıcıları ve saldırı tespit sistemleri olarak gruplayabiliriz.

### Ateş Duvarları (Firewalls)

Ateş duvarları, oldukça uzun süreden beri varolmakla birlikte zaman geçtikçe çok önemli teknik ilerlemeler

kaydettiler. En başta sınırlı sayıda arabirim desteği ile basit IP filtreleme yapan güvenlik duvarları bugün durumlu paket incelemeyen, ağ adres dönüşümüne(NAT) kadar birçok yeni özelliğe sahip olmuşlardır.

Bir ağda, vazgeçilmez unsurlardan olan güvenlik duvarları sayesinde, giden gelen tüm erişimleri denetleyen, ve kullanıcılarınızı çeşitli verim düşürücü erişimlerden kısıtlama olanağı sağlayan bir sisteme sahip olursunuz.

Uygulamalarınıza özel bölgeler (DMZ) oluşturabilir, bunlara erişimi tek ya da çift kademeli güvenlik duvarları ile engelleyebilirsiniz. Diğer yandan birden fazla yerel ağa sahip ortamlarda ağlar arasındaki erişim kontrollerini de ateş duvarı üzerinden yapabilmek mümkündür.



### Güvenlik Tarayıcıları

Ağdaki sistemlerin hem donanımsal hem de üzerlerinde koşan işletim sistemleri bakımından çeşitlenmesini, uygulama alternatiflerinin artması ve bu ağ bileşenleri üzerinde çalışan uygulamalarının da dolayısıyla çeşitlenmesi izlemiştir. Ancak hiçbir yazılımın olmadığı gibi, ağ tabanlı yazılımların da %100 güvenli(secure) olması beklenmez. Yazılımlardaki çeşitli güvenlik açıkları nedeniyle yazılımların işlevselliği için gereken özellikler, örneğin basit bir şifre giriş ekranı, yazılımı, sistemdeki veriyi ve hatta sistemi ele geçirmeye kadar gidebilen etkiler üretebilir. Her ne kadar yazılım üreticilerinin bu konudaki bilinçleri gün geçtikçe artsa da özellikle kapalı kodlu yazılımlarda ve işletim istemlerinde ciddi güvenlik açıkları her zaman bulunabilir.

Bu durumda heterojen ağımızdaki farklı içerikteki sistemleri tarayacak ve ağdaki olası güvenlik açıklarını tespit edecek, bu açıklar hakkında sistem ve yazılım yöneticilerini uyaracak ve güvenlik açıklarını kapatmanın yollarını gösterecek yazılımlar kullanılmalıdır. Bu yazılım grubuna genel olarak Güvenlik Tarayıcıları adı verilir.

Labris Teknoloji açık kaynak kod temelli ve yüksek sıklıkta güncellenen güvenlik açığı verisi ile sunduğu çözümleri, güvenilir danışmanlık desteği ile bunların tamamını sağlayabilecek çözümleri ile bu alanda her zaman kurumların yanındadır.

## Saldırı Tespit Sistemleri

Olay öncesinde yapılan güvenlik taramalarının yanında olay sırasında ya da olayın oluşmasının öncesindeki olası ön araştırma saldırılarında, saldırının tespiti mümkündür. Saldırı tespit sistemleri (Intrusion Detection Systems) de işte bu amaçla kullanılan güvenlik bileşenleridir.

İşletim sistemi bağımlı olarak bulunduğu makine için saldırı tespit sistemi olarak çalışabileceği gibi, ağ üzerindeki herhangi bir makineye yapılan saldırıları da ağdaki paketleri dinleyerek de çalışabilir. Dolayısıyla saldırı tespit sistemleri iki grupta toplanabilir.

HTTP Decode, portscan tespiti, frag2 gibi birçok ön işlem özelliği kullanabilen ağ saldırı tespit sistemi, bilinen saldırı türlerinin karakteristiklerinden tanınarak yakalanabilir.

Diğer yandan nokta saldırı tespit sistemi olarak yani bulunduğu işletim sistemi seviyesindeki saldırıları tespit etmekle yükümlü olan sistemler ise sistemdeki her türlü standart olmayan değişikliği gözler ve herhangi bir terslikte gerekli alarmları verirler.

Standart internet altyapısı yazılımlarında olduğu gibi açık kaynak kodlu yazılımların tercih edilmesi gerekliliği güvenlik yazılımlarında daha ön plana çıkmaktadır. Çünkü; açık kaynak kodlu yazılımlar birçok insanın kontrolünden geçtiklerinden yazılım hatası (bug) ve güvenlik açıkları hemen hemen hiç olmayan yazılımlardır. Diğer yandan, güvenliğinizi emanet edeceğiniz sistemin kodunu görmek size verinizin yanlış ellere ulaşmayacağı yönünde de bir güven sağlayacaktır.