

Ađ ve Web Uygulamaları Teknik Güvenlik Denetimi

Bilgi güvenliđi teknik denetim hizmet içerikleri çođunlukla muđlak ifade edilmekte ve yanlış anlaşılabilir. Teknik denetim türleri ve karakteristikleri aşağıdaki gibidir:

- Attack & Penetration Testi olarak adlandırılan “Sızma Testi” çalışması yetkili erişim haklarına sahip olmayan saldırgan perspektifiyle gerçekleştirilir. Sızma testi hacker olarak tabir edilen saldırgan kitlenin kullandığı yöntem ve araçlar (açık kod, ticari, ve kendi geliştirdiğimiz uygulama ve betikler) ile gerçekleştirilir. Testin amacı kritik kaynaklardan herhangi birini veya çalışma kapsamına bađlı olarak mümkün olan tüm kaynakları ele geçirmektir. Bu çalışma en ölümcül zayıflıkları tespit etmek, bu zayıflıklar aracılığıyla sistemi elde etmekle sınırlıdır.
- Vulnerability Analysis olarak adlandırılan “Zayıflık Tarama” çalışması Sızma Testi ile çok yakın ilişkili olmasına rağmen çalışmanın amaç ve kapsamı önemli oranda farklıdır. Zayıflık taramasının amacı kapsam içindeki tüm sistemler için en önemlisinden en önemsizine kadar tüm zayıflıkların, yetkisiz (saldırgan profili ile) ve yetkili erişim hakları ile tespit edilmesidir. Testin amacı sistem ele geçirmek değildir. Daha çok Zayıflık Tarama çalışmalarının, belli ölçüde de Sızma Testi çalışmalarının yan çıktılarında birisi de yönetimin bilgisi dahilinde olmayan erişim kaynaklarının (internet, kablosuz, dial-in, iç bilgi ađı kontrolsüz erişimleri gibi) tespit edilmesidir. Bu kaynaklar kurumun saldırı yüzeyini genişletmektedir.
- “Sistem Denetimi” hizmeti kritik sunucular ve pratik olması kaydı ile tüm bilgisayar sistemleri üzerinde uygulanabilecek gerçek uygulama - en iyi uygulama karşılaştırmasıdır. Bu denetimin etkin olarak yapılabilmesi için sistemlere sistem yöneticisi hakları ile erişilmesi gerekmektedir. Amaç sadece doğrudan kullanılabilir zayıflıkların tespiti değil, zaman içinde zayıflıklara neden olabilecek hatalı uygulamaların (şifre politikası, dosya sistemi erişim hakları, sistemler arası güven ilişkileri, sistemler üzerindeki filtreleme uygulamaları gibi) tespitidir. Diğer testlerden en önemli farkı sadece Sistem Yöneticisi haklarıyla yapılmasıdır.

Genellikle Zayıflık Tarama ve Sızma Testleri aynı kapsam içinde sunulur. Böylece hem Zayıflık Testi çıktıları Sızma Testine girdi oluşturur, hem de bilinen tüm zayıflıkların tespiti sağlanmış olur.

Kapsamlı bir bilgi güvenliđi teknik denetimi, bahsedilen denetim türlerinin tümünün gerçekleştirilmesini gerektirir. Ancak böyle bir çalışma hem yetkisiz hem de yetkili erişim yöntemlerini gerektireceğinden, belli bir sıra ile yapılması gerekmektedir;

1. Aşama: Saldırgan profilini simule eden ilk aşamada sistemlere yetkili erişim hakkı olmaksızın erişim hakkı elde edilmesi, veya istenmeyen işlemlerin yapılabilmesi hedeflenmektedir. Saldırgan perspektifinden, sistem hakkında yetkili kişilere nazaran daha kısıtlı bilgiye sahip olunacağından önce bu aşamanın gerçekleştirilmesi daha gerçekçi sonuçlar üretecektir. Daha önce bahsedildiđi gibi bu çalışmanın alt bileşenleri Zayıflık Tarama ve Sızma Testi'dir.

2. Aşama: teknik denetim hizmetinin 2. aşamasında kritik sistemlere (veritabanı, web, uygulama, e-posta, yönlendirici, DNS, izin sunucuları gibi) sistem yöneticisi hakları ile (sistem yöneticilerinin gözetimi altında) güvenlik kontrol testleri yapılır. Bu aşama Sistem Denetimi olarak adlandırılmaktadır.

Sızma Testleri'nde sistem ve güvenlik yöneticileri açısından 2 farklı yaklaşım vardır.

1. Yaklaşım: Saldırı tespiti ile ilgili kontrollerin ve organizasyonun etkinliğinin değerlendirilebilmesi için habersiz Sızma Testleri yapılabilir. Bu yaklaşımın olumsuz yanı sistem ve güvenlik yöneticilerinin Sızma Testi nedeniyle oluşabilecek kesintilere karşı hazırlıksız olmasıdır.

2. Yaklaşım: Haberli testtir. Bu yaklaşım 1. yaklaşımla ilgili risk yüksek veya saldırı tespit kontrolleri yok ise düşünülmalıdır.

Sızma Testleri'nin doğasında TCP/IP ağlarının dışında erişim yollarının kullanımı da bulunmaktadır. Bunlar;

1. Sosyal mühendislik yöntemleri
2. Telefon hatları ile erişim
3. Kablosuz yerel ağlar üzerinden erişimdir.

Sızma testlerinin genellikle sadece internet'e açık sistemlerin internet'ten test edilmesi şeklinde talep edilir ve yapılır. Ancak yukarıda da belirtildiği gibi kararlı bir saldırganın kullanabileceği diğer alternatifler de bulunmaktadır. Sadece internet tabanlı gerçekleştirilen güvence çalışmaları riskin bir bölümünü bertaraf etmektedir. Hizmet alanların tehdit vektörlerini gerçekçi değerlendirmesi gerekmektedir.

Bilgi ağı güvenliği ve Web uygulama güvenliği

Bilgi ağı güvenlik bölgelerini ayıran (ki internet bağlantısı bunlardan en önemlisidir) noktalarda IP ve port bazındaki kısıtlamalar kurumun iş ihtiyaçlarına göre uygulanmalıdır. Böylece kurumun saldırıya maruz kalabilecek alanı daraltılmış olur. Kısıtlamalar her arayüz için iki yönlü uygulanmalıdır. Bu esaslar bilgi güvenliğinin en temel prensiplerindedir.

Burada kritik ifade "iş ihtiyaçları"dır. Eğer iş ihtiyaçları tahmin edilebilen veya edilemeyen kullanıcıların kurum bilgi sistemlerine erişimini gerektiriyorsa bu kanalın açılması gerekir. İşte sadece firewall ile bilgi güvenliği sağlanamaz iddiasının temeli buradadır. Eğer kurum internet üzerinden iş yapmak niyetinde ise ilgili portları internet'e açmak zorundadır. Sadece IP ve port bazında filtreleme yapan firewall'ların web hizmetleri için sağladığı güvenlik neredeyse yok gibidir.

Web uygulama platformları

Web uygulama hizmeti internet ve iç bilgi ağları üzerinden sunulan en önemli ve en yoğun kullanılan bilgi teknolojileri hizmetlerindedir. Veritabanı bağlantıları, yoğun kullanımı destekleyecek yedekleme ve optimizasyon özellikleri, hem sunucu hem de istemci taraflarında dinamik içerik sunma ihtiyacı yüzünden web uygulamaları çok katmanlı ve belki de bilgi ağı hizmetlerinin en karmaşığıdır.

Sıradan bir web uygulaması tüm bilgi ağı hizmetlerinin ihtiyaç duyduğu bilgi ağı iletişimine, işletim sistemine, web sunucusuna, muhtemelen uygulama ve veritabanı sunucularına ve en önemlisi uygulamanın kendisine ihtiyaç duyacaktır. Bu çok katmanlı yapı ihtiyacı tıpkı bilgi ağı erişiminde olduğu gibi uygulama kullanıcısının serbestçe tüm bu katmanlardan geçebilmesini gerektirmektedir. Her katmanın farklı teknolojiler ile geliştirilebileceği ve kendilerine has zayıflıklar içerebileceğini düşünürsek web uygulama güvenliğinin ne kadar karmaşık olabileceğini anlamak zor olmaz.

Web uygulamaları ile diğer bilgi ağı hizmetlerinin farkı

Aslında tüm bilgi ağı hizmetleri birer uygulamadır. Örneğin ftp uygulaması da belli komutları bekler, bu komutları yorumlar ve yanıt verir. Hatta "ftp bounce scan attack" gibi günümüzde pek görülmesi de uygulama seviyesinde diğer bilgi ağı hizmetlerinin de zayıflıkları bulunmaktadır. Ancak web uygulamaları dışındaki bilgi ağı uygulamalarının saldırıya açık yüzeyleri web uygulamalarına nazaran daha dardır. Bu yüzden bu hizmetlerin uygulama zayıflık denetimleri çoğunlukla genel Zayıflık Tarama ve Sızma Testlerinin içinde yer alır.

Web uygulama denetimleri pek çok farklı sistem ve uygulama katmanları için denetim yapılmasını gerektirir. Web uygulamalarını diğer bilgi ağı uygulamalarından ayıran en önemli özelliklerden biri de HTTP protokolünün "stateless" yani her bir iletişimin diğerlerinden bağımsız olmasıdır. Temel protokol oturum takibi sağlamadığından uygulama seviyesinde ve bazı değişkenlerin gönderilip geri alınması şeklinde oturum takibi yapılmaya çalışılmaktadır. Bu durum da saldırganların başka oturumları çalma ihtimalini doğurmaktadır. Oturum çalma tüm bilgi ağı hizmetleri için TCP/IP seviyesinde bir risk iken, web uygulamaları için bu durum uygulama seviyesinde de görülmektedir.

Web uygulama güvenlik denetim yaklaşımları

Genel farklı güvenlik denetim yaklaşımları (yani yetkisiz uzaktan denetim ve yetkili erişimle güvenlik kontrolleri denetimi) web uygulama platformları'nın bilgi ağı, işletim sistemi, web sunucusu ve uygulama sunucusu katmanlarında yapılacak denetim için de geçerlidir.

Ancak web uygulama güvenlik denetimi, uygulama katmanı ile ilgili daha detaylı bir çalışma gerektirmektedir. Her kurum kendi ihtiyaçlarına göre farklı uygulama dilleri ile geliştirilmiş uygulamalara, farklı uygulama mimarilerine, farklı uygulama dillerine ve veritabanı sunucularına sahiptir. Bu durumda yetkisiz erişim ile yetkili erişim arasında uygulama içeriği ve mekanizmalarına ilişkin bilgi edinme farkı çok daha yüksek olabilir.

Yukarıdaki nedenle web uygulama güvenlik denetiminde kara kutu ve kristal kutu olarak adlandırılan 2 tür yaklaşım vardır. Kara kutu uygulama ile sadece kullanıcı olarak etkileşimi öngürür. Bu şekilde yapılacak bir test ile dahi edinilebilecek bilgi miktarı önemlidir. Ancak daha kapsamlı bir denetim için uygulama kodunun ve mimarisinin gözden geçirilmesi gerekmektedir. Bu yaklaşım da kristal kutu yaklaşımı olarak adlandırılmaktadır.

Genel web uygulama güvenlik riskleri

Web güvenliği ile ilgili işletim sistemi, web sunucusu, uygulama sunucusu gibi sistem yazılımlarındaki riskler ayrı tutulmak kaydı ile uygulama seviyesindeki genel riskler;

- Kod enjeksiyonu
- SQL enjeksiyonu
- Oturum güvenliği riskleri
- Kimlik doğrulama riskleri
- Değişken ve bellek sınır aşımı
- HTML kodu içinde elde edilebilecek hassas bilgiler
- Hassas bilgi içeren hata ve yönlendirme mesajları
- İstenmeyen dosyalara erişim
- Web ve uygulama sunucu yönetim arayüzlerine istenmeyen erişim
- İstemci tarafında kod çalıştırma
- Kritik bilgilerin açık metin olarak iletilmesi
- Yetersiz girdi kontrolleri olarak sayılabilir.

Teknik Güvenlik Denetimleri Ne Kadar Güvence Sağlar

Teknik güvenlik denetimlerinin güvence mekanizmasındaki yeri son derece önemlidir. Ancak tek başına belli bir zamanda gerçekleştirilen teknik denetim mümkün olan en yüksek güvenceyi sağlayamaz. Teknik denetimler en ideal durumda bilgi teknolojileri ve güvenlik süreçlerinin tasarım ve operasyonel yeterliliklerinin denetimi ile desteklenmelidir.

Pek gerçekçi olmasa da çok iyi tasarlanmış, periyodik olarak gözden geçirilen bilgi teknolojileri ve güvenlik süreçlerini (ki bu süreçler oldukça kapsamlıdır) çok iyi uygulayan kurumların teorik olarak teknik zayıflıklarla karşılaşmaması gerekir. Ne yazık ki kontrol olgunluğu çok yüksek kurumlarda bile bir takım aksaklıkların yaşanması muhtemeldir. Buna ek olarak teknik testler güvenlik kontrollerinin etkinliğinin testi işlevini de görür.

Güvenlik literatüründe çok sık rastlandığı üzere “derinlemesine savunma” bilgi güvenliğinin en önemli prensiplerinden biridir. Bu nedenle mümkün olduğunca fazla katmanda kontrol güvencesi sağlamak güvenlik seviyesini artıracaktır.

Otomatik ve Manuel Yöntemler

Özellikle zayıflık taramasında ve şifre kırma testlerinde otomatik yöntem ve araçların kullanılması etkinlik açısından zorunluluktur. Otomatik araçlar çalışma süresini kısaltmakta ve etkinliği artırmaktadır.

Ancak kapsamlı bir zayıflık tarama ve sızma testinde otomatik araçların tek başlarına gerçekleştiremeyeceği adımlar vardır. Bunlar testin ilk aşamalarındaki bilgi toplama ve hedef tayin etme adımları ve çalışma sırasında çeşitli kaynaklardan edinilen pek çok bilginin bir araya getirilip yorumlanmasıdır. Bu sayede önemsiz gibi görülen bilgiler yardımıyla başarılı bir saldırı gerçekleştirmek mümkündür. Otomatik araçlar “aggregation” adı da verilen bu anlamlandırmayı oldukça sınırlı derecede

yapabilir. Gerçek tehditin bir insan olması durumunda bu tehdiye hazırlık da insan katkısını içermelidir.

Kapsamlı bir çalışma hem otomatik hem de manuel yöntemleri gerektirmekle birlikte, sadece otomatik taramalar hiç test yapılmamasından daha iyi, ayrıca ekonomik bir çözümdür.

Ticari Yazılımlar ve Açık Kaynak Kodlu Yazılımlar

Açık kaynak kodlu yazılımlar (işletim sistemleri dahil) güvenlik testlerinin olmazsa olmazıdır. Güvenlik testlerinin en temel adımları için pek çok kişi tarafından geliştirilmiş, ve zamanın testinden geçmiş güvenlik test yazılımları bulunmaktadır. Zayıflık taraması ve web uygulama güvenlik testi için de açık kaynak kodlu yazılımlar bulunmaktadır. Bu araçların zayıflık veritabanları dünya çapında güvenlik uzmanları tarafından güncellenmektedir.

Buna karşın özellikle zayıflık tarama ve saldırı kodu alanlarında ticari uygulamalar bulunmaktadır. Bu uygulamalar tabiatları itibarı ile daha profesyonel ekipler tarafından desteklenmektedir. Kullanıcı arayüzleri daha kullanışlı tasarlanmış ve destek imkanı bulunmaktadır. Sistem ve web uygulaması zayıflık taraması konusunda ticari yazılımların açık kaynak kodlu alternatiflerinden daha zengin olduğunu söyleyebiliriz.

Genel kanı, maliyet ve pek çok kişinin deneyimini içermeleri açısından açık kaynak kodlu yazılımların kullanılması, ancak güvenlik riski yüksek kurumlar için ticari yazılımların da gerekli alanlarda kullanılması yönündedir.

Fatih Emiral