Güvenlik Testlerinin Önemi

written by Mert SARICA | 1 June 2012

Hayatımızı dijital ortamlarda sürdürmeye başladığımız bu çağda kişisel verilerimize verdiğimiz önem de git gide artmaktadır. Art niyetli kişiler tarafından firmalardan çalınan müşteri bilgilerinin çeşitli sitelerde sayfa sayfa yayınlandığı ve/veya para karşılığı satıldığı şu günlerde müşteri olarak dijital ortamda aldığımız hizmetlerden kullandığımız uygulamalara kadar bir çok noktada güvenliği ister istemez sorgular ve güvenliğimize önem verdiğini bildiğimiz, duyduğumuz ve güvendiğimiz firmalar ile çalışır hale gelmiş bulunmaktayız.

Müşteriler tarafından güvenliğin sorgulanır hale geleceğini, yılda bir veya iki defa güvenlik testi yaparak veya güvenlik testi hizmeti alarak müşteri güvenliğinin sağlanamayacağını, güvenliğin kurumsal rekabet gücünü arttıran bir unsur olacağını öngören vizyoner firmalar yıllar öncesinden güvenliğe yatırım yapmaya başladılar. Sadece güvenlik cihazlarına ve yazılımlarına yatırım yapmakla kalmayıp ethical hackerlar, sertifikalı siber güvenlik uzmanları istihdam ederek, yetiştirerek özellikle güvenlik testleri (vulnerability assessment, penetration testing) başta olmak üzere uzmanlık isteyen birçok alanda (Bilgisayar Olayları Müdahale, Adli Bilişim Analizi vb.) kendilerinden de faydalanmaya başladılar.

Bu vizyona sahip olmayan firmalar güvenlik testlerini, güvenlik zafiyeti tespit eden ve raporlayan Nessus ve benzeri araçlar ile, aynı zamanda sistem yöneticiliği de yapan veya on işi birden yürüten bir çalışanın yan iş olarak da yapabileceği sıradan bir iş olarak görürlerdi ancak ne zaman ki sistemleri, uygulamaları, altyapıları art niyetli kişilerin hedefi olmaya ve kayıplar yaşanmaya başladı işte o zaman güvenlik testlerinin hackerların bilgi ve becerilerine sahip olmayan çalışanlar tarafından gerçekleştirilmesi durumunda yapılan testin firmaya tam anlamıyla bir katma değer sağlamadığını tecrübe ederek öğrenmiş oldular.

Müşteri açısından bakıldığında eğer bir firma bünyesinde siber güvenlik uzmanı, ethical hacker bulunduruyor ise müşterilerine verdiği mesaj çok açıktır, “Güvenliği(n/m)iz için çalışıyoruz”. (Örneğin Google firmasının

güvenliğe verdiği önem, Tavis Ormandy, Michal Zalewski gibi güvenlik dünyasından iki önemli isme bünyesinde yer verdiğinden rahatlıkla anlaşılabilmektedir.) Bunun nedeni hackerların (black hat, grey hat) sahip oldukları bilgi ve beceriler ile güvenlik testi gerçekleştirebilen bu uzmanlar, hackerların gözüyle sistemleri, uygulamaları, ağları denetleyebilmekte, güvenlik zafiyetlerini tespit edebilmekte, zafiyetleri ortadan kaldırmak için çözüm önerileri üretebilmekte kısaca firmanın hack edilme dolayısıyla müşteri bilgilerinin çalınarak kötüye kullanılma ihtimalini en aza indirgeyebilmektedirler. Ayrıca bu uzmanlar güvenlik testi gerçekleştirmenin yanısıra dış firmadan alınacak güvenlik testi hizmeti için firma seçiminde (penetrasyon testi hizmeti adı altında sadece Nessus çıktısı veren firmaların elenmesi) ve hizmetin değerlendirilmesinde (hatalı risk derecelendirmesinin tespiti (düşük seviyedeki bulguların yüksek seviye olarak raporlanması), hatalı (false positive) bulguların tespiti) katkı sağlamaktadırlar.

Firma açısından bakıldığı zaman ise güvenlik testlerinin aslında bir firma için birden fazla artısı bulunmaktadır. Güvenlik testleri;

- Firmanın hacklenme ihtimalini büyük oranda azaltır.
- Firma içinde güvenlik farkındalığını arttırır.
- Riskli noktaların tespit edilmesini sağladığı için risk yönetimi yapılmasını sağlar.
- Hacklenmek, firmaların itibarını ve marka değerini zedeleyebildiği gibi iflaslarına da neden olabilmektedir bu nedenle güvenlik testleri iş sürekliliğinin sağlanmasına yardımcı olur.
- ISO 27001, PCI DSS gibi standartlar yılda en az bir defa güvenlik testi yapmayı zorunlu tuttuğu için bu tür standartlar ile uyumlu olmaya yardımcı olur.

Sonuç olarak günümüzde sadece güvenlik teknolojilerine yatırım yapan, bünyesinde siber güvenlik uzmanı, ethical hacker bulundurmayan veya yetiştirmeyen firmaların, uzun vadede, sürekli artış gösteren siber tehditler karşısında ayakta kalması, müşterilerine güvenli hizmetler ve ürünler sunması, rakipleri ile rekabet etmesi ve piyasada tutunması oldukça zordur. Umarım çağın gerisinde kalmış olan bu firmalar en kısa zamanda bu uzmanları istihdam etmeye başlayarak hem bizler yani müşteriler hem de kendileri için çağa ayak uydurarak güvenli hizmetler/servisler vermeye, uygulamalar, ürünler geliştirmeye başlarlar.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim…