Sızma Testi Uzmanlığı ve Kariyer

written by Mert SARICA | 9 March 2015

Yıllardan beri, sıradışı bir meslek olan sızma testi uzmanlığı (ethical hacker / penetration tester) ile ilgili çok sayıda e-posta alıyorum. E-postaların çoğunda da, sızma testi uzmanı olmak istiyorum, nereden ve nasıl başlamalıyım sorusunun sorulduğunu görüyorum. Her birine itinayla cevap yazarken çoğu mesajımda, 2011 yılında yazdığım "Nasıl Ahlaklı Korsan Olunur?" başlıklı yazımı da okumalarını tavsiye ediyorum. Bir sızma testi uzmanı olarak bu yazı ile son yıllarda oldukça popüler ve çekici olan bu meslekte kariyer yapmanın biraz da zorluklarına değinmek istiyorum.

Bu alanda kariyer yapmanın aslında ülkemizde diğer meslek dallarına göre biraz daha zor olduğunu söyleyebilirim. Örneğin tıp fakültesinden mezun olsaydınız, uzmanlık eğitimi için Tıpta Uzmanlık Sınavı'na (kısaca TUS) girdikten sonra belli bir branş üzerine kariyer yapabilir ve bu branşa özel iş ilanlarına başvurabilirdiniz. Ancak mevzu sızma testi uzmanlığı olunca işler bu kadar kolay olmuyor.

Kolay olmuyor çünkü ülkemizdeki iş ilanlarına bakacak olursanız hala sızma testi uzmanlığının, on görevi olan bir güvenlik uzmanının on birinci görevi olabileceğine inanan firmalar olduğunu görebilirsiniz. Halbuki diğer ülkere bakarsanız, sızma testi uzmanlığının kendi içinde bile ayrı uzmanlık dallarına (örnek: web application penetration tester, network penetration tester) ayrıldığını ve bu spesifik alanlarda uzmanların arandığını (#1, #2, #3) görebilirsiniz.

Tabii aynı anda hem güvenlik cihazı yöneten (yoğun bir şekilde operasyon yapanlar), hem PCI denetimi yapan hem de güvenlik politika ve prosedürü hazırlayan bir kişinin sızma testi uzmanı olabileceğine inanan, yıllarca çalışanlarına yatırım yapmak yerine güvenlik cihazlarına, ürünlere yatırım yapan kurumlar, günün sonunda ciddi bir sorun yaşadıkları zaman doğru yolu (uzmanlaşma) ağır bedeller ödeyerek buluyorlar. Halbuki onlardan 5-10 yıl önde olan diğer ülkelere ve kurumlara bakacak olsalar, yıllar sonra başlarına neler gelebileceğini, ne tür uzmanlıklara ihtiyaç duyacaklarını, nelere ve nerelere yatırım yapmaları gerekeceğini az çok görebilirler. (Vizyon)

Özellikle tek kişilik dev güvenlik uzmanı kadrosu arayan kurumların iş

ilanlarını gördüğümde çoğu zaman üzülerek tebessüm ediyorum. Bu ilanları, bir hastanenin on farklı alanda, on farklı uzman doktor (ortopedist, kardiyolog vb.) aramak yerine tek bir pratisyen hekim aramasına ve çalıştırmasına benzetiyorum. Olur mu, olur ama günün sonunda sağlık sorunu yaşayanların, daha doğru teşhis ve tedavi adına pratisyen hekimler yerine uzman doktorlara kontrole gittiklerini biliyoruz. (Specialist vs Generalist)

Tabii bu durumun biraz da, sızma testinin sadece araçlarla yapıldığının, bilgi ve birikimin çok da önemli olmadığının düşünülmesinden kaynaklandığını düşünüyorum. Halbuki bu alanda uzmanlaşmak pek o kadar kolay olmuyor. Sadece araçlarla bu işi yapan da kendine sızma testi uzmanı diyor, yıllardır bu alanda araştırma yapan, okuyan ve kendini geliştiren bir kişi de diyor. Eğer iyi araç kullanan o işin uzmanı olabilseydi bugün direksiyon başına geçip iyi araba kullanan herkesin Michael Schumacher olması gerekirdi. Veya sadece bir işi icra etmek, kişiyi o işin uzmanı yapabilseydi, şarkı söyleyen Ajdar ile Sezen Aksu arasında fark olmazdı.

Sızma testi uzmanı olmak için bol bol okumak (2000'li yılların başından bu yana kadar 60 tane teknik kitap okumuşum), bol bol pratik yapmak ve her daim bilgileri güncel tutmak gerekiyor. Misal bir önceki yılın web uygulama zafiyetleri ile bir sonraki yılın zafiyetleri aynı olmayabiliyor dolayısıyla zafiyetlere yol açan kök sorunları anlamak, tespit ve çözüm konusunda önemli bir rol oynuyor. Ayrıca değişen teknolojileri yakından takip etmek ve hızlıca adapte olmak gerekiyor. 4-5 yıl öncesine kadar mobil uygulama sızma testlerine ihtiyaç duyulmazken, bugün en az web uygulama sızma testleri kadar ihtiyaç duyuluyor. Bu gelişim sürecinde, işverenin size özellikle eğitimler konusunda yatırım yapmasının oldukça önemli olduğunu söyleyebilirim. Örneğin bugün SANS firmasından online (on demand) bir eğitim almak istediğinizde eğitim ücretlerinin 4000$ – 5000$ arasında olduğunu görebilirsiniz.

Evet, artık çoğu kurum sızma testi uzmanı arıyor ama kolay kolay bulamıyor. Neden çünkü sızma testi uzmanları ne yazık ki dalda yetişmiyorlar ve kendilerini yetiştirmeleri hiç de kolay olmuyor. Vizyoner kurumlarda çalışan sızma testi uzmanlarının ise değerleri bilindiği ve kendilerine gerekli yatırımlar yapıldığı için kolay kolay iş değiştirmiyorlar. Uzman yetiştirmeyen, çalışanına yatırım yapmayan, maaş konusunda da sıradan bir çalışan ile aynı maaşa sızma testi uzmanı arayan firmaların iş ilanlarının, 6 ay ila 1 sene boyunca açık kaldığını görebiliyoruz. Kimi zaman 6 ay içinde, ne aradığını bilmeyen 4-5 farklı insan kaynakları danışmanlığı firmasından aynı pozisyon için birkaç defa arandığınız bile olabiliyor.

Düşüncelerimin sizleri karamsarlığa sürüklemesini istemem. Siber güvenlik ve sızma testi uzmanlığına artık ülkemizde çok daha fazla önem veriliyor. Eskiden kurumunda sızma testi uzmanı bulundurmayanlar, bugün 5 kişilik sızma testi ekipleri oluşturuyorlar. Talebin arttığı bu yıllarda, bu alanda iyi bir kariyer yapmak isteyen adaylara, tek kişilik dev kadro (nicelik) olmak yerine uzmanlaşmaya (nitelik) önem veren, vizyoner kurumları tercih etmelerini tavsiye edebilirim. Ne de olsa yıllar içinde gideceğimiz nokta Amerika ve Avrupa'dan (uzmanlığa önem veren ülkeler) farklı olmayacak ve uzmanlık daha da kıymetli olacaktır.

Unutmayın, sızma testi uzmanlığı aşçılık gibidir. Günün sonunda elinizde onlarca malzeme (araçlar, istismar kodları, zafiyetler vs.) olur ve bunlardan ortaya gerçekten lezzetli bir yemek çıkarmanız beklenir. Lezzetli yemekler ortaya çıkarmak için ise hem tarifleri (bilgi) iyi bilmeniz hem de kıvamı (beceri) iyi tutturmanız gerekir ve bu da yıllarınızı alır.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.