# Siber güvenlik sektöründeki uzman açığı nasıl telafi edilecek?

***Siber suçlular her geçen gün kendini geliştirip daha sofistike yöntemler kullanmaya başlarken, güvenlik güçlerinin de bu hıza ayak uydurması kritik önem taşıyor***

Gökhan Say, Innovera CEO

Los Angeles'taki Kaliforniya Üniversitesi, 26 Ekim 1969 akşamı saat 22:30 sularında tarihinin en hararetli koşuşturmasına tanık oldu. Geleceği değiştirmek üzere olduklarından habersiz olan görevlilerin amacı aslında oldukça basitti: Bir sunucudan bir diğerine ulaşıp, bağlı olan bilgisayara giriş yapmak. Bunun için önce iki sunucu arasında bir mesaj iletim ağı oluşturuldu. Diğer makineye giriş yapmak için anahtar kelime "Login" olarak belirlenmişti. Klavyenin tuşlarına sırasıyla basıldı ancak kelime daha tamamlanamadan sistem hata vererek çöktü. Karşıdaki bilgisayara yalnızca "Lo" metni ulaşmıştı ki bu iki harf, aynı zamanda internet üzerinden gönderilen ilk mesaj olarak tarihe geçti. Yaklaşık 1 saat sonra sistem yeniden devreye alınarak "Login" gerçekleştirildi.

O gün internet ve bilgisayar donanımları, kötü niyetli insanlar için kârlı bir hedef oluşturamayacak kadar kısıtlıydı. Bugün sadece internet ve bilgisayarlar değil, IP adresi alabilen her türlü akıllı cihaz siber tehditler için kusursuz bir hedefe dönüştü. Zaman içinde siber güvenlik sektörüne hayat veren bu tehdit, gerekli önlemler alınmazsa içinde bulunduğumuz dijital çağın Nuh Tufanı'na dönüşebilir.

Frost & Sullivan ve ISC2'nin yaptığı analiz gösteriyor ki, 2020 yılına kadar siber güvenlik alanındaki iş gücünde 1,5 milyondan fazla doldurulmamış pozisyon olabilir. Bu büyük açığa, sektörde yeterince nitelikli personel yetiştirilememesi sebep oluyor. Eğer kontrol altına alınmazsa, nitelikli personel ihtiyacıyla arz arasındaki fark hızla büyüyecek. Peki, bu alanda neden doğru sayıda ve nitelikte personel yetişmiyor?

## Geleneksel profiller aranıyor

En büyük nedenlerden biri güvenlik şirketlerinin geleneksel teknoloji kimliklerini tercih etmesi. Örneğin belirli bir okulu belirli bir derece ile bitirmek gibi şartlar yüzünden siber güvenlik alanında hizmet verebilecek önemli bir iş gücü sistemin dışına itiliyor. Halbuki geleneksel profilin dışında şirketlere ve sistemlere yeni bakış açıları getirebilecek sayısız yetenek dışarıda bekliyor. Siber güvenliğin yeni fikirlere ihtiyacı var ve bu fikirler pek çok farklı akademik seviyeden gelebilir.

## Eğitim için zaman yaratmak kritik önem taşıyor

Bir diğer sebep de stratejik planlama ve eğitim. ESG şirketi ve Uluslararası Sosyal Güvenlik Teşkilatı'nın yaptığı bir araştırmaya göre, siber güvenlik uzmanlarının yüzde 70'i problemin örgüt yapısında olduğunu savunuyor. Elinizdeki iş gücüne yeni nitelikler kazandırarak şirket içinde yapılabilecek yeni konumlandırmalar, daha az riskli pozisyonlara işe almalar yapabilmenize olanak tanıyabilir. Çok az şirket çalışanlarına eğitim için yeterli zamanı harcıyor olsa da bu noktada çalışanlar için de tablo pek olumlu değil. Araştırmaya katılan siber güvenlik uzmanlarının yüzde 67'si, mesleki becerilerini geliştirmek ve eğitimlere katılmak için fazlasıyla yoğun olduklarını vurguluyor.

## Yerel siber güvenlik ekosistemi kurulmalı

Şirketler donanımlı siber güvenlik personelleri oluşturmak için şimdiden geleceğe yatırım yapmalı ve bir siber güvenlik ekosistemi oluşturmalı. Devlet kurumları ve eğitim kurumlarıyla bağlantı kurularak, örneğin yerel bir orta öğretim kurumuyla çalışarak, genç yaşlarda mesleğe ilgi uyandırıp, geleceğin uzmanlarının yetiştirilmesine başlanabilir. Bu sayede çok da uzak olmayan bir gelecekte nitelikli personel gücünüzde belirgin bir artış olacaktır.