Güvenlikte köklü değişimin ayak sesleri!

Sürekli gelişen risk dünyasında şirketler de kendi güvenlik açıklarını tespit etmek için hacker'larla, ama 'etik' olanlarıyla çalışıyor. Bu kitlenin sunduğu hizmeti bir iş modeline dönüştüren ve Innovera'nın Türkiye çözüm ortaklığını yürüttüğü Synack, yeni nesil siber güvenlik anlayışını ortaya koyuyor.

Handan Aybars

Kurumsal siber güvenlikte "kitle hacker kaynaklı" formülüyle 'crowdsourcing' yapısına yeni bir anlam kazandıran Synack, 50 farklı ülkede binden fazla etik hacker'dan oluşan bir toplulukla çalışıyor. Eski bir NSA siber istihbarat uzmanı olan Synack CEO'su Jay Kaplan, Hack the Pentagon programı çerçevesinde Pentagon askeri sistemlerini 4 saat gibi kısa bir sürede nasıl hack'lendiğini anlatmak için Türkiye'ye geldi. Synack'in dört yılda birçok fon desteği alarak büyüdüğü bilgisini veren Jay Kaplan, etik hacker'ların çalışma sistemini ve Türkiye pazarında Innovera güvencesiyle hizmet sundukları şirketlerin bu yeni modelde nasıl ilerlediğini anlattı:

Etik hacker'ların temel özellikleri, kurumsal güvenlik algısına etkileri nedir? Şirketler 'white hat hacker' yapısını kabul etmeye ne kadar istekli?
Şirketlerin karşı karşıya oldukları tehditlerin gözünden yeni bir bakış açısı elde edebilmeleri için beyaz şapkalı hacker'ların büyük önem taşıdığını düşünüyorum. Bu kişiler olmadan, sisteme dışarıdan müdahale etmek isteyen birinin hangi yolu izleyeceğini tespit etmek çok zor. Biz de iş modelimizi bunun üzerine inşa ettik ve şirketlere, sistemlerine girmek isteyen birinin bunu nasıl yaptığı konusunda gerçekçi bir yaklaşım sunmak istedik. Buradaki asıl sorun, yeterli sayıda beyaz hacker olmaması. Çok büyük bir talep var. Araştırmalara göre, 2021 yılına kadar siber güvenlik alanında açık iş pozisyonlarının sayısı 3,5 milyonu geçecek. Bu sorunu çözmek için yeterli sayıda uzman yok ve 'crowdsourcing' tam da bu noktada devreye giriyor. Dünyanın en yetenekli uzmanlarıyla, onları tam zamanlı olarak işe almaksızın, her noktadan çalışabiliyoruz.

Synack Red Team (SRT) bu yapıda nasıl bir yere sahip?
Synack Red Team, dünyadaki en başarılı etik hacker'lardan oluşuyor. Bu topluluğun içine kabul oranımız yüzde 10'un altında. Bu sayede müşterilerimiz güvenlik konusunda zayıf oldukları noktaları tam olarak öğrenerek önemli fayda ve değer elde ediyor. Danışmanlık usulü çalışma modelinde olduğu gibi, bir projeye bir veya iki kişiyi atamakla kalmıyor, her bir projeye 75 ila 100 arası uzmanı atıyoruz. Böylece güvenlik açıklarını tespit etmek mümkün oluyor.

SRT, kurumsal BT ekibi ve güvenlik birimi ile sürekliliği olan nasıl bir ilişkiye sahip? Bu bağlar, kurumsal güvenlik stratejisini nasıl etkiliyor?
Yetenek sıkıntısı, kurumsal BT güvenlik birimlerinin öncelikli sorunu. Siber güvenlik henüz yeni bir sektör olduğu için yeterli insan kaynağı hızlıca bulunamıyor ve teknik açıdan uzmanlık da sınırlı kalıyor. Bu yüzden şirketler Synack'e mevcut siber savunma hattını güçlendirmek ve kendi ekiplerini zenginleştirmek için geliyor. Bu konuda onlara yardım ediyor ve güvenlik süreçlerini iyileştiriyoruz. Şirket çatısı altında uygulama geliştiren, altyapıyı yöneten ekiplerin kendi süreçlerini daha güvenli devam ettirebilmek için bizim yardımımıza ihtiyaçları var.

Güvenlik risklerinin nasıl çeşitlenmesini bekliyorsunuz? Şirketler bu risk gelişiminin ne derece farkında?
Saldırılar her geçen gün daha sofistike hale gelecek. Şirketler de güvenlik açıkları ve sızıntılar konusunda reaktif yaklaşımlar yerine, daha proaktif bir anlayışı benimsemeye başlayacak. İnovasyon hiç olmadığı kadar önem kazanacak. Büyük ölçekli güvenlik danışmanları yerine, daha yenilikçi metotları kullanan yeni nesil güvenlik girişimlerine yönelim başlıyor, bu şirketlerin çözümleri tercih ediliyor. Hatta şirketler konsolide çözümlere yöneliyor. Yani bir sorun karşısında 20 ayrı şirketten çözüm almak yerine, birkaç pazar liderinin çözümleri tercih edilecek. Bugün güvenlik pazarında gördüğümüz manzara önemli ölçüde değişecek ve bu dönüşüm büyük oranda 2018 içinde gerçekleşecek.

Synack olarak bu gelişen risk dünyasında stratejiniz, Ar-Ge'de odaklandığınız başlıklar hakkında bilgi verir misiniz?
Şu an öncelikli hedefimiz iş modelimizi genişletmek. Sadece uzman güvenlik araştırmacıları değil, kullandığımız teknoloji de şirketler için önem taşıyor. Araştırmacıların yaptığı rutin işleri otomasyona alarak, daha verimli bir şekilde işimizi ölçeklendirmek önceliklerimiz arasında. Synack, bu açıdan bakıldığında sadece en iyi uzmanların yer aldığı bir pazaryerinden fazlasını sunuyor. İş modelimizde insan ve makine kullanımı yarı yarıya oranlanabilir. Bu da bizim için çok önemli. Crowdsourcing, güvenlik sektörü için en çok tercih edilen uygulamalar arasına girecek. Kuzey Amerika'da ve Avrupa'nın çeşitli bölgelerinde bu gelişmeleri görmeye başladık bile. Yine de bu henüz çok yeni bir konsept ve eğitimlerle desteklemek şart.

Küresel bazda Türkiye'de tüm sektörlerde güvenlik farkındalığını, artı ve eksi yönlerini nasıl değerlendiriyorsunuz?
Türkiye de tıpkı dünyanın geri kalanı gibi siber güvenlikle yeni yeni tanışıyor. Bu konsepte alışması için zamana ihtiyacı var. Bunun en somut örneği, özellikle kurumsal firmalarda çalışıp, tek işi siber güvenlik olan uzmanların sayısı... Elbette nitelikli insan kaynağının henüz yetişmemiş olması burada önemli bir unsur. Bu tür uzmanları bulmak ve tam zamanlı olarak istihdam etmek hem maliyetli hem de zor. Öte yandan, siber güvenlik başlı başına yeni sayılabilecek bir sektör. Bence Türkiye, trendleri takip etme konusunda geride sayılmaz. İnovasyona önem veriliyor, yeni çıkan çözümler ve modeller hızla benimseniyor. Türkiye bazı noktalarda Avrupa ülkelerinden ileride. Ama siber güvenlikte ön saflarda yer alsa da, bu alandaki çalışmaların artırılması gerek. Bu konuda Türkiye pazarındaki çözüm ortağımız Innovera, uzun yıllara dayanan tecrübesiyle yanımızda yer alıyor. Innovera, siber güvenlik perspektifinde yaşanan bu dönüşüme öncülük etmek gibi önemli bir rol üstleniyor.