IoT ile birlikte DDoS saldırıları geçtiğimiz yıl **yüzde 97 oranında** arttı

Siber güvenlik saldırılarında son 5 yıldır ezber bozan bir değişim olduğunu söyleyen Innovera CEO'su Gökhan Say, "Fidye yazılım ile birlikte sadece şirketler değil, bireysel kullanıcılar da ilk defa bilgisayarın bozulması dışında bir tehditle yüzleşmek zorunda kaldı: Siber suçlulara fidye ödemek! Suçlular açısından ne yazık ki son derece erişilebilir ve kârlı bir yöntem olan fidye yazılım saldırıları, özellikle son iki yılda patlama mertebesinde artış gösteriyor. Bu saldırılarda kullanıcıların bilgisayarındaki belirli bir klasör veya dosyaların tümüne erişim kilitleniyor. Dosyalarına erişmek isteyen kullanıcıların, siber hırsızlara belirli bir fidye ödemesi gerekiyor. Bireysel kullanımda göz ardı edilme ihtimali bulunan bu tür saldırılar, söz konusu bir şirket yöneticisinin bilgisayarı ve kritik kurumsal dosyaları barındıran klasörler olduğunda yıkıcı darbelere neden olabiliyor. Siber güvenlikte son 5 yılın bir diğer değişimi de DDoS saldırılarındaki artış oldu. Nesnelerin İnterneti trendinin bu konuda bir katalizör işlevi gördüğünü belirtmek durumundayız. Zira IoT henüz yeni gelişen bir teknoloji ve her cihazın, her sensörün, her kameranın internete bağlı olarak çalışmasını esas alıyor. İnternete bağlı olmak demek, bir IP adresine sahip olmak, olası saldırılara karşı açık olmak demek... Bu konuda çok ciddi önlemler alınması, tüm IoT üreticileri genelinde standartların hızla belirlenmesi gerekiyor. Oysa şu an IoT'nin güvenliğinden ziyade, konforuna odaklı bir gelişme söz konusu. Endüstriyel üretimden savunmaya, otomotivden telekomünikasyona kadar pek çok sektörde kullanıma alınan IoT cihazları siber suçlular için 'kolay hedef' olarak görülüyor. Bu tür cihazlar ele geçirilip, bir botnet ağına bağlandığında ise çok sayıda adresten belirli bir web sitesi ya da internet servisine istek göndermeye dayalı DDoS saldırılarının gücü muazzam derecede artıyor. Araştırmalar, DDoS saldırılarının geçtiğimiz yıl IoT sayesinde yüzde 97 arttığını gösteriyor. Yaklaşık 200 bine yakın IoT cihazıyla gerçekleştirilen saldırılar, Ekim ayında ABD'de internetin neredeyse durmasına neden olmuştu" diyor.

Innovera CEO'su Gökhan Say

Şirketlerin dijital dönüşüm süreçlerine hız vermesinin son derece doğru ve yerinde bir karar olduğuna işaret eden Say, dijital dönüşüm yolculuğunda doğru altyapının seçilmesi, bulut dönüşümünün güvenli bir şekilde gerçekleştirilmesi ve personelin dijital enstrümanlar üzerinde kabiliyetlerini geliştirmelerinin sağlanmasının büyük önem taşıdığını belirtiyor. Gökhan Say şöyle devam ediyor: "Şirketlerin siber güvenlik politikalarında gözlemlediğimiz en büyük açık, siber güvenlik uygulamalarının birbirinden bağımsız, koordine olmayan bir biçimde kullanılması. Oysa siber güvenliği bir bütün olarak ele almak, tüm süreçleri ilgili ürün ve servislerle uçtan uca birbirine bağlamak gerekiyor. Firmalar bunu sağlayamadıklarında, bir saldırı anında sorumluluğu üstlenip, destek sağlayacak bir iş ortağı bulmaları neredeyse imkânsız hale geliyor. Bu nedenle Innovera gibi siber güvenliği uçtan uca kapsayan çözümler üzerinde tecrübeli, onlarca farklı üreticinin ürün ve servislerini portföyünde bulunduran, güvenilir bir çözüm ortağıyla çalışmak gerekiyor."

Günümüzde siber güvenlik alanında başarının entegrasyondan geçtiğini dile getiren Say, "Güvenlik alanında pek çok üretici bulunuyor ve bunların her biri, siber güvenlik süreçlerinin belirli noktalarına odaklanıyor. Zafiyet tespiti, erişim yönetimi, ağ güvenliği ve benzeri konularda en ideal çözümleri bir araya getirerek, uçtan uca bir entegrasyon kurmak gerekiyor. Nitelikli güvenlik uzmanı açığı büyük olduğu için, şirketlerin atacağı en iyi adım tüm bu çözümler üzerinde uzmanlaşmış, siber güvenlikte tecrübesi uzun yıllara dayanan bir çözüm ortağıyla çalışmak olacaktır. Innovera olarak uçtan uca tüm siber güvenlik ihtiyaçlarını en iyi karşılayacak altyapıyı oluşturmada, kapsamlı portföyümüz ve sektörel tecrübemizle kurumlara danışmanlık sunuyoruz" diye konuşuyor.