DDOS karşısında diz çökmek kader değildir!

Türkiye'ye yapılan saldırının çok daha büyüğü 2013 yılında engellenmişti. Kaderciliği bırakıp siber savaş politikamızı oluşturmak zorundayız.

Eylem CÜLCÜLOĞLU
eylemc@gmail.com

Bundan 8 ay önce, 175. Sayımızda "Kritik Altyapılar Tehdit Altında" başlığıyla siber savaş tehlikesini kaleme almıştım. O zamanlar ne Rusya ile gerginliğimiz vardı ne de DDOS saldırıları (Dağıtık Servis Kesintisi Saldırısı) gündemdeydi. Görünen o ki yazı gerekli çevreler tarafından önemsenmedi. Aralık ayında Türkiye, tarihinde görülmemiş bir DDOS saldırısına hedef oldu. Nic.TR çöktü. Com.tr uzantılı sitelere uzun bir süre erişim sağlanamadı. Bu saldırının hemen ardından bankalar hedef alındı ve Türkiye'nin önde gelen bankalarının internet siteleri saatlerce hizmet veremedi.

Nic.TR'nin yönetimini elinde tutan Orta Doğu Teknik Üniversitesi (ODTÜ), yaptığı basın duyurusunda saldırının boyutunu şu cümlelerle açıkladı: "Birden fazla 40 Gbps kapasiteli iletişim hattında taşmalara yol açan, bazılarında zaman zaman 200+ Gbps yoğunluklarına erişen bant genişliği saldırıları gözlenmiştir. Bu toplu saldırının, bugüne değin dünya üzerinde yaşanmış en yoğun saldırılardan biri olduğu bilinmektedir."

ODTÜ, Türk internetinin gelişiminde büyük rol oynamış değerli bir üniversitemizdir. Yaptıkları açıklama da kısmen doğrudur. Evet, bu saldırı çok büyük ölçekli olmuştur. Söyledikleri gibi 200 Gbps üzerinde bir hıza ulaşmıştır. Ama bu, Nic.TR'nin dolayısı ile Türk internetinin çökmesinin bahanesi olamaz. Gerekli teknolojik yatırımla ve düzgün planlama ile bu tür saldırılar engellenebilir.

300Gbps'lik dev saldırı

18 Mart 2013'te Türkiye'ye yapılan saldırının çok daha büyük ölçeklisi Spamhaus'a karşı yapılmıştı. Saldırının boyutu 85Gbps seviyelerindeyken, Spamhaus, DDOS önleme konusunda dünyanın en iyi firmalarından birisi olan Cloudflare'e başvurmuştu. Cloudflare, duruma el koyduğunda saldırının boyutu 300 Gbps seviyelerine ulaşmıştı. İnternetin ana omurgaları bile böyle bir saldırıyı taşıyacak güçte değildi ve dünya interneti çökme noktasına gelmişti. Cloudflare, trafiği dünya genelindeki farklı veri merkezlerine taşıyan Anycast teknolojisi ile bu saldırıyı bertaraf etti. Spamhaus çökmedi. Dünya interneti ayakta kaldı. 18 Mart 2013, tarihe en büyük DDOS saldırısı olarak geçti. Cloudflare firması da bu saldırıyı bertaraf eden firma olarak adını altın harflerle tarihe yazdırdı.

Eğer Nic.TR de Anycast benzeri bir teknolojiye sahip olsaydı veya bu teknolojiyi kullanan bir firma ile çalışıyor olsaydı Türk interneti çökmeyecekti. Hükümetin bu saldırıyı fırsat bilip, siyasi nedenlerle, Nic.TR yönetimini ODTÜ'den alıp Bilgi Teknolojileri ve İletişim Kurumu'na (BTK) vermek istemesini doğru bulmuyorum. Nic.TR bu saldırıdan ders alıp, gerekli teknolojik yatırımları yapabilir ve bir sonraki saldırıyı engelleyebilir. Burada değişmesi gereken kurumlar değil, zihniyettir. "Bize bir şey olmaz" zihniyeti Türkiye'nin genel zihniyetidir. Yılbaşı akşamı Milli Piyango'nun sitesinin çökmesi, sınav sonuçları açıklandığı gün ÖSYM'nin sitesinin açılmaması, olağan karşılanmaktadır. Oysa bunlar olağan değildir. İnternet siteleri gerekli teknolojiler kullanılarak, ne kadar büyük trafik gelirse gelsin ayakta tutulabilir. DDOS saldırıları karşısında diz çökmek kader değildir. Bize yapılandan daha büyük ölçekteki DDOS saldırıları engellenebilmiştir.

Bu daha başlangıç

Türkiye olarak bölgesel bir lider olmak istiyorsak, savunma sanayimize ve askeri gücümüze ne kadar önem veriyorsak, internet altyapılarımıza da o kadar önem vermeliyiz. Geleceğin savaşları topla tüfekle değil, siber saldırılarla olacaktır. DDOS, siber saldırı türlerinin en basit ve en kolay yöntemidir. Bu savaşın daha başlangıcıdır. Eğer gerekli önlemleri almaz ve siber güvenlik konusunda genel stratejimizi belirlemezsek, daha başımız çok ağrır.

Sağlık, sevgi, barış, mutluluk dolu ve siber saldırısız bir 2016 dileğiyle...