Türkiye'ye büyük siber saldırı

ODTÜ Rektörü Prof. Dr. Ahmet Acar, 14 Aralık Pazartesi günü başlayan siber saldırılara ilişkin, "Uluslararası literatüre geçecek düzeyde bir siber saldırı yaşandı. Şunu çok rahatlıkla söyleyebilirim. Alan Adı Yönetimi sistemi, saldırı öncesinde ve saldırı sırasında uluslararası güvenlik standartları ne gerektiriyorsa, gerekli önlem ve işlemlerin hepsini fazlasıyla yerine getirdi" dedi.

24 Aralık 2015, Cumhuriyet web sitesi

Acar, yaptığı açıklamada, ".tr" üst düzey alan adı ve onun altında yer alan ikinci seviye alan adlarının yönetimi ve koordinasyonunun 1992 yılından beri ODTÜ tarafından sürdürüldüğünü hatırlattı.

".tr" uzantılı Alan Adları Yönetimi'nde yetki paylaşımı ve denetim sağlamak adına, 2000'de Ulaştırma Bakanlığı İnternet Kuruluna bağlı olarak çalışan, sektör temsilcilerinin yer aldığı "DNS Çalışma Grubu"nun oluşturulduğunu ifade eden Acar, bu bağlamda 2000'den bu yana politika ve kuralları belirleme işlevini DNS Çalışma Grubunun, tahsis işlevini ise ODTÜ'nün yerine getirdiğini anlattı.

Prof. Dr. Acar, ODTÜ'nün ".tr" uzantılı internet adreslerinin tahsisinde yetkili olmasına ilişkin şunları söyledi:

"Bizim 15 yıl önce önemini vurgulayarak altyapısını oluşturduğumuz 'güçler ayrılığı' ve 'çok paydaşlı yönetim' modelinin ne denli önemli olduğu, uluslararası çevrelerde son 4-5 yıldır konuşulur oldu. ODTÜ, '.tr' uzantılı internet adreslerinin tahsisine ilişkin yetkisini, uluslararası anlaşma kapsamında kullanıyor. İnternet tahsisi üzerine çalışan ICANN ve IANA adlı kuruluşların verdiği ve denetlediği yetki bu. Bu hizmeti veren bir kurumun altyapısında veya işleyişinde bir aksama olması halinde ICANN ve IANA zaten otomatik olarak devreye giriyor. Güvenlik konusunda da uluslararası standartlar ne gerektiriyorsa onun üzerindeyiz."

"Dünya üzerinde yaşanmış en yoğun saldırı"

Dünya üzerinde yaşanmış en yoğun saldırılardan birinin, 14 Aralık'ta gerçekleştiğini

belirten Acar, yurt içinde ve dışında 5 ayrı noktada konuşlanan 6 adet ".tr" alan adı sunucusuna doğru gelen Dağıtık Servis Kesintisi Saldırısının (DDoS) yaşandığı bilgisini verdi.

Acar, bunun sonucunda tüm ülkede, internet bant genişliğinde çok ciddi yoğunlukların yaşandığını, saldırının temel olarak "DNS yükseltme saldırısı" olarak başladığını aktardı. Acar, saldırının ".tr" alan adlarından ilgili IP adreslerine ulaşılmasını engellemek amacıyla yapay ağ trafiği üretmek de dahil, DNS sunuculara doğru yoğun ağ trafiği yollanması şeklinde, ülke dışındaki kaynaklar tarafından organize olarak gerçekleştirildiğini dile getirdi.

Acar, "Bu toplu saldırı, bugüne kadar dünya üzerinde yaşanmış en yoğun saldırılardan biri. Uluslararası literatüre geçecek düzeyde bir siber saldırı yaşandı" ifadesini kullandı.

"Artan ihtiyaca cevap verilebiliyor"

Saldırı başlayınca Bilgi Teknolojileri ve İletişim Kurumuna (BTK) gerekli bilgileri verdiklerini ve BTK'nın USOM koordinasyon merkeziyle süreci birlikte yürüttüklerini ve Telekom operatörleri ile çok etkili çalışmalar yaptıklarını belirten Acar, şu bilgileri verdi:

"Bu saldırı, sadece Alan Adı Yönetimi altyapısına yapılmadı, bunu söylememiz lazım. Hemen hemen tüm internet sağlayıcılarının altyapılarında sıkıntı yaşandı. Saldırı başlamaz başlamaz ODTÜ'nün sunucularını sistemden ayırdık. ODTÜ'deki 12 bilgisayar mühendisi, devamlı olarak sisteme destek veriyor. ODTÜ'nün Bilgi İşlem Dairesi'nde 56 kişi çalışıyor. Onların da desteği alındı. Bunlara ilaveten Enformatik Enstitüsü ve Bilgisayar Mühendisliği öğretim üyeleri devreye girdi. Enformatik Enstitümüz şu anda birçok ülkenin uzmanlarına siber güvenlik eğitimleri veriyor. Ülkemizde bu kadar yoğun uzmanlık ve tecrübe ODTÜ'de var. Bugüne kadar Alan Adı Yönetimini geliştirmek için hiçbir yatırımdan kaçmadık. Bu teknolojiyi ve servisi ülkemize, ODTÜ getirdi ve 1992'den beri bu sistemi aksatmadan çalıştırıyor ve geliştiriyor. Bugüne kadar da Alan Adı Yönetim servisini sorunsuz olarak sunuyor. Artan ihtiyaca sürekli olarak cevap verilebiliyor."

"Güvenlik tedbirleri fazlasıyla alındı"

Siber saldırılara karşı önlemlerin yoğun şekilde alındığını vurgulayan Acar, şöyle dedi:

"Saldırı sırasında 3'ü yurt dışında olmak üzere toplam 11 alan adı sunucusu ile hizmet verildi. Yurt dışındaki sunucularda uygulanan ANYCAST adlı sanal sunucu teknolojisi nedeniyle 11 sunucu ile pratikte 20'den fazla sunucu olarak hizmet sağlandı. Saldırı öncesinde ve sırasında alınan önlemler, bizim icat ettiğimiz bir şey değil, bunlar uluslararası düzeyde geliştirilen ve paylaşılan sistemler ve işlemler. Şunu çok rahat söyleyebilirim, bu tür servisleri veren kurumların, yurt dışında uyguladığı güvenlik tedbirleri fazlasıyla alındı. Önlemlerden bir tanesi sunucuları dağıtmak. Normal bir zamanda bize lazım olan bir veya iki sunucu. İşte böyle bir duruma cevap verebilmek için zaten üç tane yedeğimiz vardı. Saldırı öncesinde sunucuların bir tanesi Hollanda'daydı ve öyle bir saldırı oldu ki, Hollanda'daki sunucu

çok donanımlı olmasına rağmen, orası da bloke oldu. Saldırı başlayınca da en gelişmiş teknolojiyi kullanarak gerekli tedbirleri aldık ve bu çerçevede sunucu sayısını hızla 11'e çıkardık."

"Saldırılar siyasi ve ticari tehdit haline geldi"

Rektör Prof. Dr. Acar, bu tür saldırıların, geçmişte ABD'de, Avrupa'da, bir dönem Baltık ülkelerinde ve Ukrayna'da da yaşandığını anlatarak, "Bu tür saldırılar, siyasi ve ticari bir tehdit aracı haline geldi ve bu alanda bir sektör de oluştu" değerlendirmesinde bulundu.

Virüs kullanan korsanların bilgisayarlara habersizce girerek, arka kapı yarattıklarını ve kontrol ettikleri on binlerce bilgisayarı kiraladıklarını aktaran Acar, "Bu yolla bilgisayarlar, arka kapısından girip mesaj gönderebilir hale geliyor. Dolayısıyla bir anda on binlerce yerden mesaj gönderilebiliyor. Ama bilgisayar sahiplerinin ne olduğundan haberi yok. Korsan kuruluş, örneğin, diyor ki, 'ben sana saat 14.00-18.00 arasında 15 bin bilgisayar veriyorum, ücreti de bu.' Bu kapasiteyi kendisi de bir tehdit olarak kullanabiliyor. Düşünün, e-ticaret yapan bir şirkete 'şu kadar para vermezsen bloke ederim seni' diyor. Bu yolla sitesini 12 saat kullanılamaz hale getirebiliyor" ifadelerine yer verdi.