Dünya Enerji Konseyi Türkiye

Makale Özetleri

Sayı 257: 17-23 Mayıs 2021

BORU HATTI SİBER SALDIRISI, ABD ALTYAPI GÜVENLİĞİNİN YENİDEN DEĞERLENDİRİLMESİNİ GEREKLİ KILIYOR *

Geçen Cuma, Houston'dan New York Limanı'na ve New Jersey'e 5.500 mil uzunluğundaki ve Doğu Kıyısı'nın yakıt ihtiyacının %45'ini karşılayan Alpharetta merkezli Colonial Pipeline'a bir siber saldırı düzenlendi. Fidye yazılımı saldırısının, 'Darkside' isimli bir hacker grubu tarafından gerçekleştirildiğine inanılıyor. Siber saldırı, operasyonel bilgisayar sistemlerinden ziyade işletmeyi hedef alsa da şirket tüm boru hattı işlemlerini çok sayıda ihtiyat nedeniyle durdurdu. Yakıt fiyatları yükseldi. Boru hattını çalıştıran sistemler tehlikeye atılırsa, boru hattı haftalarca hatta aylarca kapatılabilir. Biraz şansla, bu durum hafta sonuna kadar kaldırılabilir.

Ulaştırma Bakanlığı, yakıtların taşıtlarla taşınması için acil bir feragatname yayınladı, ancak bu uzun vadeli bir çözüm değil. Amerika Birleşik Devletleri ve altyapısı ister rakip ülkeler ister fırsatçı suçlular tarafından olsun, daha fazla siber saldırı ile karşı karşıya kalacak.

Bazı bilgisayar korsanları, sadece para almak için bu siber saldırıları gerçekleştirirler, ancak bu tip suçlar genellikle düşman bir güçten de kaynaklı olabilir. Suçlanan örgütün Rus bağları var, ancak bu bağlar henüz doğrulanmadı.

Bu özel saldırının Rusya, Çin veya başka bir hükümet tarafından emredilmiş olup olmadığı, ortaya çıkarmak için kapsamlı bir soruşturma gerekmektedir. Şu anda söylenebilecek şey, Amerika'nın savunmasızlığının rakipleri tarafından göz ardı edilmeyeceğidir. Şüphesiz uygulanabilir hedefler belirlenmekte ve bunlardan yararlanılmaktadır.

Geçen yılki SolarWinds saldırısı, belki de tarihte ABD'ye yapılan en büyük siber saldırıydı. Daha sonra aylarca tespit edilmeyen saldırı, faillerin (muhtemelen Rus kökenli) sadece özel şirketlerin değil, önemli devlet kurumlarının e-postalarına ve dosyalarına erişmesine izin verdi. Etkilenen kurumlar arasında Pentagon, Dışişleri Bakanlığı ve Ulusal Nükleer Güvenlik İdaresi çalışanları vardı. Özel şirketler arasında ise McDonalds MCD, AT&T ve Microsoft MSFT bulunuyordu.

Gelecekteki bir siber saldırı, sivil altyapıyı hedef alabilir, hastane sistemlerini veya ülkenin her gün güvendiği hava trafik kontrol frekanslarını bozabilir. Sistemler, SolarWinds'de olduğu gibi, kimsenin haberi olmadan aylarca tehlikeye atılabilirse koordineli bir saldırı aynı anda düzinelerce askeri ve sivil hedefi de vurabilir.

* "Pipeline Cyber Attack Demands Reevaluation Of U.S. Infrastructure Security", *Forbes*

Amerika Birleşik Devletleri'ne fiziksel bir saldırı hayal edin, güvenlik güçleri ülke çapındaki elektrik kesintileri ve yakıt kıtlıkları nedeniyle etkili bir şekilde yanıt veremiyor, yanlış bilgi alınıyor ve temel altyapı ciddi şekilde etkileniyor. Mükemmel şekilde düzenlenmiş bir siber saldırı, müdahaleyi ve kurtarmayı sakatlayarak fiziksel bir saldırıyı kolaylaştırabilir.

Siber savaş geleceğin savaşıdır ve Amerika saldırılara karşı hükümetin ve sanayicilerin farkına vardığından çok daha savunmasızdır. Bazı eleştirmenler, Başkan Biden'ın altyapı planında siber güvenlik finansmanı eksikliğine işaret etti. Bu sorun, yalnızca harcama yoluyla çözülebilecek bir sorun değil, Amerika'nın daha kötü saldırılarla karşılaşmamasını veya misilleme yapma yeteneğini kaybetmemesini sağlamak için ayrı ve iki taraflı bir yasa tasarısı gerekiyor.

Ulusal altyapı projeleri güvenlik düşünülerek geliştirilmeli, eskiyen donanım ve yazılımlar değiştirilmelidir. Amerika, Çinli veya Rus bilgisayar korsanlarının kritik ulusal altyapıyı tehlikeye atmasına izin vermemelidir. Bütün bunlar paraya mal olacak. Bazı harcamalar tartışmasız bir şekilde gereklidir. Savaş değişti ve Amerika'nın düşmanları bunu çok iyi anladı. Kongre de aynı şeyi yapmalı yoksa 21. yüzyıl kaybedilecektir.

* “Pipeline Cyber Attack Demands Reevaluation Of U.S. Infrastructure Security”, *Forbes*