

DÜNYA - ABD'nin BM Büyükelçisi: Dünya, nükleer bir felaketi kıl payı atlattı

Ana Sayfa > GÜNDEM > Sıradaki tehlike Siber FETÖ

Sıradaki tehlike Siber FETÖ

13.08.2016 - 06:41 | Son Güncelleme: 13.08.2016 - 08:40



“Örgütün, Facebook, Twitter gibi sosyal medya şirketlerinde çalışan teknik elemanları var. FETÖ'nün emirlerine ayarlı beyinler o ne derse yapacak nitelikte”

ALİ ÇELİK

Sosyal Medya ve Bilgi Teknolojileri Dstrateji Derneği Başkanı **Abdullah Çiftçi** gazetemize önemli açıklamalarda bulundu.

Darbe girişimi sonrası yapılan operasyonlar buzdağının görünmeyen kısmından bize ipuçları vermeye başladı. Paralel yapıya yönelik operasyonlarda birçok isim gözaltına alındı. Hâlen bu temizlik sürüyor. Geriye dönüp baktığımızda bizi içten nasıl kuşattıklarını gördük. Netice itibarıyla ülke insanının kafasında bir takım sorular ve korkular başladı. Evet tankları uçakları savuşturduk ancak farkında olmadığımız tehlikelerle nasıl mücadele edeceğiz?

Şöyle ki; bu yapı devletin her kademesinde 40 yıl boyunca yapılmış. Kendilerine göre bir ağ kurmuşlar. Şimdi yapılan operasyonlar ve gözaltına alınan, meslekten ihraç edilen kişilere bakınca devletin en mahrem

VIDEO HABER



yerlerinde görev yaptıklarını görüyoruz. Örneğin Cumhurbaşkanlığı, Başbakanlık, MİT, Emniyet, TSK, Anayasa Mahkemesi, TİB, bakanlıklar, borsa, bankacılık sektörü gibi adını saymadığımız alanlarda bulunmuşlar. Üstelik imza yetkisi olan her türlü bilgiye ulaşabilmişler. Önümüzdeki süreçte bizi bekleyen muhtemel tehlikeleri Sosyal Medya ve Bilgi Teknolojileri Strateji Derneği Başkanı Abdullah Çiftçi'ye sorduk.

DİJİTAL SINIRLARIMIZI YABANCILAR BEKLİYOR

Vatandaşlar olarak tedirginiz. Artık her şeyin sanal olarak yapılabildiği, e-devlet gibi bir platformu milyonlarca insanın kullandığını dikkate alırsak nasıl bir tehlike ile karşı karşıyayız?

21. yüzyıl dijital dünyasında, devletler kendilerini "dijital dünyada" yeniden yapılandırıyor. Reel sınırlarımızı Mehmetçik bekler, ama dijital sınırlarımızı ise kendi yerli güvenlik yazılımlarımız olmadığı için yabancılar bekliyor.

Artık savaş yöntemleri değişti. Devletler direk orduları ile değil, dolaylı yoldan, vekalet savaşları ile birbirine saldırıyor. İspat edilemeyen, faili meçhul olacak şekilde, yeni savaş yöntemleri var. Finansal terör, istihbarat ifşası, itibar suikastleri, örgütler üzerinden vekalet savaşları, kitle kıskırtma ile iç isyan, kaos çıkartma ve siber savaş. Siber savaş, ucuz, hızlı sonuç alma ve faili meçhul kalabilecek en önemli saldırı şeklidir. NATO, kara, hava, deniz gücüne ilaveten siber gücü de oluşturma kararı aldı. Birçok ülke kendi siber ordusunu kurdu. Türkiye'nin dijital dünya yapılandırmasında FETÖ elamanları etkin oldu. TİB, BTK, Türk Telekom gibi kurumlarda FETÖ mensupları görev aldı.

29 ÜLKEYE KAYNAK YAPMIŞLAR

15 Temmuz darbesini milletin feraseti, cesareti ve hızlı müdahalesi engelledi. Milletin öz güveni çok yüksek. Bu nedenle siber saldırılar milletin öz güvenini yıkmaya, devlete karşı güvenini azaltmaya, fitne ve kaos çıkartmaya yönelik olur. FETÖ örgütü kurgulanması gereği toplumda fitne ve huzursuzluk çıkartmaya ayardır.

Küresel istihbaratçılar, FETÖ örgütünü "açık/gizli istihbarat teşkilatı" olarak görüp kullanıyor. Örgütün, Facebook, Twitter gibi sosyal medya şirketlerinde çalışan teknik elamanları var. Örgüt mensuplarının beyni "Mehdi" olarak bildiği FETÖ'nün emirlerine ayardır. FETÖ, yak, yık talimatını verirse gözünü kırpmadan her şeyi yapacak nitelikte. Seçim zamanlarında FETÖ örgütünün Twitter ve Facebook üzerinden organize bir şekilde Cumhurbaşkanı Erdoğan'a ve AK Parti'ye saldırdığını, "algı yönetimi" ile olumsuz hava yaydığını görmüştük.

Kayyum atanan Kaynak Holding'te 29 ülkeye VPN teknolojisi ile 200 megabitlik özel kriptolu hatların tespit edildiği server'larda, 300 bin terabaytlık depolama sistemi bulunmuştu. FETÖ siber çetesi son 15 günde Kaynak Holding'e sayısı belirsiz siber saldırı gerçekleştirdi. FETÖ'nün siber çetesi, küresel istihbaratçıların yönlendirmesi doğrultusunda Türkiye'ye de siber saldırı girişiminde bulunacaktır. 15 Temmuz darbe girişimi gecesi TRT'nin ve DigiTürk'ün yayını kesmek için FETÖ mensubu 5 bilişim uzmanının helikopterle Vodafone Arane'ya indirildiğinin görüntülerini gördük.

İNSAN KAYNAĞINA FORMAT ATILMALI

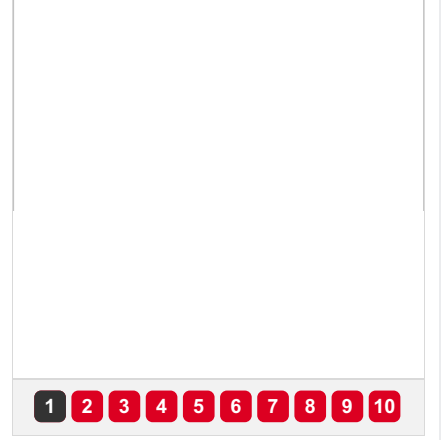
Okulda çocuğu olan herkes bilir. Haftada bir ya da birkaç kez özel eğitim kurumlarından arananlar var. Bu da bilgilerin bir havuzda toplandığını ve birilerine servis edildiğini gösteriyor. Ne amaçlanıyor?

Türkiye'de faili meçhul, montaj, şantaj işlerinin tamamını paralele bağlamak mümkün. Çünkü vekalet örgütleri üzerinden yürütülen savaşta, örgüte bu yöntemler küresel istihbarat kuruluşları tarafından öğretiliyor, eğitiliyor. Türkiye'nin bilgileri ellerinde ama Türkiye içinde güçleri kalmadığı ve devletin de olayın farkına vardığı için yapabilecekleri bir şey yok.

Üst akıl denen aslında şeytani akıl için dünyada "ekonomik sömürü"den çok ülkelerin "insan kaynağını sömürme, yönetme, formatlama" daha önemlidir. FETÖ örgütünün üyeleri, Türkiye'nin fakir ailelerin zeki çocuklarının beynine format atması ile oluştu. Anadolu'daki gariban anne-baba'nın hiçbir şeyden haberi yok. Oğlumuz dindar, namaz kılar diyorlar. Bu nedenle devlet, ekonomik kaynağından daha öncelikli insan kaynağını kontrol etmeye yönelmeli. FETÖ örgütünün muadili olarak dünyada Moon Tarikatı, Opis Dei, Falung Gong gibi, Hristiyan, Budist dünyasında kullandıkları tarikat, cemaatler var. Hepsinde aynı yöntem, yani ülkelerin insan kaynağını formatlayıp küresel sisteme entegre etmek.

Kamudaki bilgileri ifşa edebilirler

Hatırlayacağınız gibi Nisan ayında 50 milyon kişinin kimlik bilgilerinin çalındığı tespit edilmişti. Bu bilgilerin YSK'dan sızdırıldığı da konuşulmuştu. Sızdıktan sonra nereden alındığının bir önemi



Piyasalar	Fark %
USD	14.2478 % 0.84
EUR	15.5892 % -0.59
BIST 100	1990.75 % -1.41
ALTIN	895.516 % 1.83
GBP	18.8825 % -0.18

FOTO HABER



olmasa da neticede bu bilgiler birilerinin elinde. Bu ve benzer durumlara karşı önümüzdeki süreçte ne gibi sorunlarla karşılaşabiliriz?

FETÖ terör örgütü Türkiye’de tüm vatandaşlara aynı anda zarar verebilecek eylemler peşinde. Bu nedenle, vatandaşın kamudaki bilgilerini yayımlamaya yönelik siber saldırı yapabilirler. Tapu kayıtları, UYAP verileri, Banka bilgileri, seçmen kütük bilgileri, adres bilgileri, kredi kart bilgilerini ele geçirip ifşa etme girişiminde bulunabilirler.

Türkiye finans sektörünün güvenlik altyapısı sağlamdır. Banka, kredi kartı bilgilerini ele geçirmeleri zor. Vatandaşın kimlik bilgileri ile yapabilecekleri fazla bir şey yok. Ancak, küçük dolandırıcılık çeteleri bilgilerden sahte kimlik oluşturup, kredi müracaatı vs deneyebilirler. FETÖ bireysel değil toplum eylemi peşinde. Vatandaşın kimlik, adres bilgilerinin internette yayınlanması düşmanı olanlar için ciddi risk taşıyor. Sonuçta toplumda bir huzursuzluk, güvensizlik oluşturur.

Sağlık Bakanlığı’nın bir süredir uyguladığı avuç içi tarama sistemi, emniyetin parmak izi uygulaması, biyometrik fotoğraf... hepsi normal işleyiş içerisinde vatandaştan alındı.

Dahası hastanelerde her türlü kan tahlilimiz dahi var. Bunlar nerelerde kullanılabilir?

Mayıs ayında Anonymous Hacker grubu bazı hastanelere ait yaklaşık bir milyon kişinin sağlık verilerini yayınlamıştı. Bunlar arasında HIV’li 50 kişinin de listesi yayımlandı! Türkiye’de tüm hasta kayıtları Sağlık Bakanlığı’nda var. Bakanlığın bilgi işleminde geçmişte FETÖ elamanları vardı. Verileri bir şekilde yedeklemişler ise veya bilgi serverini hack edebilirler ise bu verileri Anonymous veya başka bir grup adına internette yayımlayabilirler. Bu durum da hastalar için ciddi problem teşkil edebilir. Parmak izi, biyometrik kimlik bilgilerini ve kan gruplarını ciddi bir yerde kullanamazlar. Ancak bu bilgilere sahip olan dolandırıcılık çetelerinin girişimi sonucu münferit dolandırıcılık olayları gündeme gelebilir.

VEKALETLER İPTAL EDİLMELİ

Bu yapı sadece devlette değil özel sektörde de faaliyette. Farkında olmadan muhatap olduğumuz kurumların taleplerine göre birçok yere kimlik, adres ve banka bilgilerimizi veriyoruz. Hatta vekalet verdiklerimiz bile var. Bunların kötüye kullanıma ihtimaline karşı nasıl bir yol izlemeliyiz?

Vekalet verme ve yetki devri FETÖ mensuplarının elinde ise kötüye kullanma ihtimali olabilir. Bu nedenle bundan önce işbirliğinde olunan şirketler arasında FETÖ’cü şirketler var ise, geçmişte verilen tüm vekaletler iptal edilmelidir. FETÖ örgütü mensupları şu anda can derdinde, saklanma, kaçma peşinde. Çok fazla bir şey yapamazlar.

Bir de sosyal medya hesaplarımız var. Bunların ele geçirilmesi ve olumsuz bir bilgi paylaşımı durumunda yasa önünde suçlu duruma düşebiliriz. Örneğin terör paylaşımları, devlet büyüklerine hakaret gibi. Bu ihtimallere karşılık nasıl bir tedbir alabiliriz?

15 Temmuz başarısız darbe girişimi sonrasında şu ana kadar sosyal medya hesapları yoğun saldırı altında. Kişilere Facebook veya Twitter’den geliyormuş gibi göstererek mailler geliyor, “bilgileriniz çalındı lütfen şifrenizi değiştirin” şeklinde. Bu maile cevap verilip şifre girilirse, şifrenizi çalmış oluyorlar ve anında hesabın kontrolünü ele geçiriyorlar. Hesap ele geçmesinden sonra hesap adına atılan mesajlar ile önceki mesajlar zaten uymaz. Bu nedenle bir problem teşkil etmez. Ama, özel mesajlar, ekleme, çıkarma ve montaj yapılarak yine sosyal medyada “itibar suikastleri” olabilir. Bunu engellemek için de gelen mesajlara şifre girmemek ve hesabı mutlaka telefon onaylı yapmak gerekir.

ESKİSİ GİBİ DİNLEMİYORLAR

Parelel yapının en mahrem yerlerde dahi görüntü alıp, ses kaydı yaptığını biliyoruz. En yaygın olarak kullanılan böcek ve benzeri aygıtlara ya da sizin gibi uzmanların bildiği yöntemlerin kullanımına karşı bir öneriniz var mı?

ABD’de özel bir eğitim şeklidir bu, “Olmayan suç nasıl oluşturulur”. 2006 yılında Türk Emniyetinden ABD’ye eğitime giden FETÖ’cü polisler bu şekilde bir eğitim verilmişti. 17-25 Aralık sürecinde, Baykal kaseti, MHP kasetlerinin çekilmesinde bu yöntem uygulandı. Vatandaşlarımız için artık bu şekilde suçlayıcı, montaj, şantajlar bir anlam ifade etmez. Çünkü sosyal medya kullanıcıları bu konuda bilgi sahibi. Kamuda önemli görevlerde bulunanlara şantaj yapmak, dinlemek, kaydetmek için gizli kamera, böcek vs yerleştirmek mümkün. Kamuda çalışan FETÖ’cülere yoğun operasyon var, kısa sürede ciddi temizlik yapıldı. Bu nedenle eskisi gibi rahat yapamazlar.

KAMUDA ŞİFRELER DEĞİŞTİRİLMELİ

Füze sistemlerimiz, savaş planlarımız, savaş uçaklarımızın, tanklarımızın, hassas silahlarımızın her türlü bilgilerini ellerinde bulundurmuyorlar. Aselsan gibi gözde bir kurumumuzda faili meçhul

cinayetler bile işlenmiş. Muhtemelen bu bilgileri klonlamışlardır. Kanaatimce belki ferdi olarak değil ama toplum olarak ciddi bir sorunla karşı karşıyayız. Bu fikre katılır mısınız?

Bu fikre katılıyorum. FETÖ örgütü planlı bir şekilde Türkiye'nin elektronik/dijital bilgilerini çalmak üzere bir el tarafından kamuya yerleştirildi. Savunma sanayi alanında da faaliyet yapmışlardır. Hızlıca, kamudaki şifrelerin değiştirilmesi ve güvenlik yazılımlarının güncellenmesi gerek. Siber saldırıda başarı eğer içeriden bir destek varsa daha yüksektir. Türkiye'nin bu alandaki şanssızlığı FETÖ mensuplarının kaydetme, bilgi çalma amaçlı eğitimleri ve bunu uzun süredir yapıyor olmaları. Avrupa ülkeleri ve ABD'de dijital devlet yapılması 1990'dan sonra bir plan, proje dahilinde yapıldı. Buna rağmen sürekli siber saldırı altında. ABD'de FBI çalışanlarının neredeyse tamamının kimlik ve adres bilgileri çalınmıştı. Aselsan'ın aydınlatılmayan teknik elamanlarının sır ölümleri FETÖ örgütünün bugünkü hali çerçevesinde dosyaları yeniden açılmalıdır.



Türkiye'de Bugün

Anasayfa
Gündem
Politika
Ekonomi
Dünya
Spor
Teknoloji
Sağlık

Türkiye'de Bugün

Sondakika
Yazarlar
Eğitim
Emlak
Mağazın
Kültür-Sanat
Editörün Seçtikleri
TGRT Haber

Kurumsal

İhlas Gazetecilik
Kurumsal
Künye
İletişim
Reklam
Kişisel Verilerin
Korunması
Gizlilik İlkeleri
Kullanım Şartları
Privacy Policy

Sosyal Medya

Facebook
Twitter
LinkedIn
RSS
E Gazete
Foto Galeri
Türkiye İnternet Tv