12. ULAŞTIRMA VE HABERLEŞME ŞÛRASI

HABERLEŞME ÇALIŞMA GRUBU

SEKTÖR ÖNGÖRÜ RAPORU

-

GÖREV MATRİSİ BAŞLIKLARI

2.5.Siber Güvenlik

4.5.Siber Güvenlik

TELKODER Görüşleri

-

Koordinatör

Dinçer Dikici

2. TÜRKİYE'DE MEVCUT DURUM VE GELECEK ANALİZİ

2.5.Siber Güvenlik

Ülkemiz, haklı gerekçelerle, siber güvenliğini sağlamak için son yıllarda önemli adımlar atmıştır. Bunların başında, 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi gelmektedir. Bunun dışında atılan üç önemli adım daha vardır. Bunlardan birincisi, 2021 Yılı Cumhurbaşkanlığı Yıllık Programı 470.1 sayılı tedbir; İnternet Değişim Noktası (İDN) kurulmasına yönelik usul ve esasların belirlenmesi ve İDN kurulumunun gerçekleştirilmesi hedefi yer almaktadır. Bu tedbirle ilgili sorumlu kuruluşlar; Ulaştırma ve Altyapı Bakanlığı ve BTK'dır. Ayrıca BTK 2020 Yılı İş Planına göre, Türkiye İnternet Değişim Altyapısı Kurulmasına İlişkin Çalışmaların Aralık 2020 tarihinde tamamlanacağı belirtilmektedir.

İkincisi, 2021 Yılı Cumhurbaşkanlığı Yıllık Programı 470.2 sayılı tedbir; Veri merkezi sektörünün geliştirilmesini sağlayacak düzenleyici çerçeve ve teşvik mekanizması oluşturulması, Türkiye'nin yoğun ticaret yaptığı ülkelerle bulut hizmetlerinin sunulmasına yönelik işbirlikleri yapılması hedefi yer almaktadır. Bu tedbirle ilgili sorumlu kuruluşlar; Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ve Sanayi ve Teknoloji Bakanlığı'dır. Üçüncüsü ise, yakın zamanda yayımlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planları (2020-2023)'dır.

Bu adımlar ile birlikte, Bilgi Teknolojileri ve İletişim Kurumu tarafından, elektronik haberleşme hizmet vermek için yetkilendirilmiş işletmecilere, siber güvenliğin tesisi için zaman zaman çeşitli yükümlülükler getirilmektedir. Bu yükümlülükler; lisans, cihaz, depolama donanımları gibi çeşitli alanlarda yatırım yapılmasını gerektirmekte ve ciddi maliyetler oluşturmaktadır. Bu kapsamda ihtiyacı karşılayabilecek cihaz, lisans ve donanımlar için tedarikçiler ile görüşmelerin ve testlerin yapılması, aynı zamanda her bir işletmeci için uygun cihaz, lisans ve altyapı ihtiyacı ortaya çıkmaktadır. BTK tarafından istenilen yükümlülüklerin eksiksiz ve sorunsuz yerine getirilebilmesi, siber güvenliğin olması gerektiği gibi tesis edilebilmesi için BTK'nın yapılacak yatırımlar konusunda işletmecilere destek olması gerekmektedir.

4. TÜRKİYE VİZYONU

4.5.Siber Güvenlik

Küresel veri ve bulut hizmetleri pazarında rekabet, Amazon AWS, Microsoft Azure, Google Cloud ve Alibaba Cloud gibi büyük oyuncular arasında yaşanmaktadır. 2022 yılında 350 milyar doları geçmesi beklenen bulut pazarının, 2019 yılı büyüklüğü 250 milyar dolardır. Bu pazarın yaklaşık %63'ü bu 4 şirkete aittir (TELKODER 2020: 1). Yeni nesil bulut sistemleri dinamik yapılardır. Verilerimiz dün Türkiye'de durmuş, bugün Almanya'da duruyor, yarın da Yunanistan'da duracak olabilir. Ülke olarak hem fiber altyapımızı hem de yazılım yeteneklerimizi geliştirmek zorundayız. Ancak, verinin ne kadar önemli olduğunu bir benzetme ile örnek vermek gerekirse, gerçek anlamda bir millî arama motoru, en az *Altay Tankı* veya *Millî Muharip Uçak projesi* kadar önemli bir konudur.

Sadece birkaç işletmecinin içinde bulunduğu rekabet, gerek bölgesel gerekse küresel veri ve bulut hizmetleri pazarını şekillendirmekte, bilişim dünyasında köklü dönüşümlere neden olmaktadır. Her türlü verinin büyük bölümü 3-4 büyük işletmeciye ait devasa veri merkezlerinde toplanmakta ve bu işletmeciler, kendileri dışında herhangi boyutta bir oyuncunun var olmasına veya bir ekosistemin oluşmasına imkân vermemektedirler.

Yurttaşlarımız, üniversitelerimiz, kamu kurumlarımız ve şirketlerimiz, bu büyük işletmecilerin yurtdışında bulunan veri merkezlerine veri tabanlarını yükleyerek, sanal sunucu, e-posta, veri depolama gibi birçok hizmeti kullanmak durumunda kalmaktadırlar. 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ve 2021 Yılı Cumhurbaşkanlığı Yıllık Programında yer alan 470.1, 470.2 sayılı tedbirler de ülkemiz siber güvenliği açısından büyük önem taşımaktadır. Bu 3 hedefin gerçekleştirilebilmesi ve bazı uluslararası şirketlerin tekel davranışlarının önüne geçmek adına acilen *Ulusal Veri Stratejimizi* oluşturmamız gerekmektedir.

Bu noktada en önemli hususların başında gelen konu; Microsoft Azure, Amazon AWS, Google Cloud, Alibaba gibi büyük işletmeciler Türkiye'de bulunan veri merkezi işletmecileri ile işbirliği yapmalarıdır. Ancak bu sayede, kendi ekosistemimizi oluşturmuş, yurttaşlarımıza, üniversitelerimize, kamu kurumlarımıza ve şirketlerimize kendi topraklarımızda istedikleri hizmeti vermiş, vergisini devletimize ödeyen veri merkezi işletmecilerimizi büyütmüş ve en önemlisi de verilerimizi güven altına almış olabiliriz (TELKODER 2020: 2).

İnternet Değişim Noktaları

Tüm erişim sağlayıcılarının bağlanmadığı, birden fazla İnternet Değişim Noktası olmadan ülkemizin siber güvenliğini sağlamak mümkün değildir. Dolayısıyla, Siber Güvenlik Türkiye Vizyonu ile ilgili unutulmaması ve çok önemli olan bir diğer başlıkta İnternet Değişim Noktaları'dır. Ülkemizde, tüm erişim sağlayıcıların bağlandığı herhangi bir İDN bulunamamaktadır.

İnternet Değişim Noktaları, İnternet Servis Sağlayıcılarının (İSS'ler) ve İçerik Dağıtım Ağlarının (CDN'lerin) kendi ağları (Özerk Sistemler-AS) arasında internet trafiği alışverişinde bulunduğu fiziki bir altyapıdır. Bir işletmeci için bütün işletmecilerin bağlantılı olduğu bir noktaya bağlanmak, her işletmeciye ayrı ayrı bağlanmaktan çok daha avantajlıdır. Maliyetleri düşürür, gecikmeyi ve veri kaybını azaltır, iletişim kalitesini artırır. İDN'ler, İSS'lerin CDN'lere teslim etmesi gereken trafik miktarını düşürür. İDN üzerinden artan yolların sayısı, yönlendirme (routing) verimini arttırır ve veri iletiminde yaşanan hataların/kayıpların azalmasını sağlar.

Bir İDN'nin başlıca amacı, iki ya da daha fazla ağın kendi aralarında bağlantı kurmadan, bir santral aracılığı ile birbirleriyle iletişim kurmasını sağlamaktır. Ağların böyle bir santral aracılığıyla birbirleriyle direkt iletişiminin çok çeşitli avantajları vardır. Başlıca avantajları; maliyetlerin düşmesi, gecikme sürelerinin azalması ve bant genişliğinin artmasıdır.

Telekomünikasyon pazarlarında serbestleşmeyi tam anlamıyla gerçekleştirebilmiş, rekabeti tesis edebilmiş ülkelerde, İDN herhangi bir düzenlemeye tabii değildir. İDN'lerin düzenlenmeye tabi olmasından ziyade daha çok İSS'ler arasında veri alışverişi, trafik değişimi (peering) üzerinden yürüyen ve tarafların menfaatine olacak şekilde düzenlenmiş çeşitli anlaşmalar ile sağlamaktadır. Çünkü karşılıklı bir yarar ve fayda söz konusudur.

İDN faaliyetleri hükümet denetimi olmaksızın tamamen işletmeciler arasında kendiliğinden gerçekleşmektedir. İDN'ler yalnızca trafik alışverişi, değişimi (peering) yapmak isteyen birçok sağlayıcının bulunduğu ülkelerde mevcuttur. Bu nedenle gelişmiş ülkelerde, İDN'lere kamu tarafından herhangi bir müdahale olmadığı görülmektedir. Bu ülkelerde İDN'lere bağlanma, ya ücretsiz ya da çok ucuzdur.

Gelişmekte olan birçok ülkede İDN'lerin eksikliğinin başlıca nedeni, pazarda belirli altyapı veya hakları kullanan tekel yetkisine sahip tek bir oyuncunun varlığıdır. Düşük rekabet seviyelerinin olduğu ülkelerde, İSS'lerin trafiklerini kendi aralarında değil de hâkim olan oyuncu aracılığıyla değiş tokuş etmekten başka çaresi bulunmamaktadır. Bu durumun önlenmesi için devletlerin müdahale ederek bu alanı, ülkenin ve sektörün yararına olacak şekilde düzenlemesi ve yeni piyasa katılımcılarının kısıtlamalarını azaltmak için yardım etmesi gerekmektedir.

Dolayısıyla, tüm erişim sağlayıcılarının katılımının zorunlu olacağı birden fazla İnternet Değişim Noktası kurulmalıdır. İDN'nin bir ülkenin güvenliği için çok önemlidir. Bu nedenle, mümkün mertebe yerli olanaklar ile hayata geçirilmelidir. Bu kapsamda, TNAP desteklenmelidir (http://tnap.net.tr/). Aynı zamanda başka yerli/yabancı girişimlerin oluşmasına imkân sağlayan ortam sağlanmalıdır.

Veri merkezleri için olmazsa olmaz bir ihtiyaç olan İDN'ler ile ilgili sorunların aşılamaması durumunda ülkemiz, birçok konuda dışa bağımlı hale gelecektir. Türkiye'de depolanması gereken verilerin yurt dışındaki veri merkezlerine kayması, Türkiye'nin üzerinden geçmekte olan internet trafiğinin artması yerine azalması hatta kaybedilmesi vb. gibi sayısız ekonomik ve teknik tehlikeler ile karşı karşıya olacağımızın bilinmesi ve farkına varılması gerekmektedir. Söz konusu risklere ilişkin farkındalığımızın arttırılması gerektiği düşünülmektedir.

Bu şartlar altında internet trafiği konusunda Türkiye'nin bölgesel bir merkez olması için tüm erişim sağlayıcıların katılımının zorunlu olacağı birden fazla İDN kurulması şarttır. Fiber altyapı yaygınlaştırılmalı, veri merkezleri güçlendirilmeli ve İnternet Değişim Noktaları kurulmalıdır. İnternet Değişim Noktaları sayesinde veriye çok daha hızlı ve ucuza erişilebilecektir. İDN tek başına düşünülmemesi gereken bir bütünün parçasıdır.

Kurulması planlanan İDN'lerin istenilen amaca hizmet edebilmesi için öncelikle atılması gereken adımlar bulunmaktadır. Aksi durumda kurulacak İDN'ler, hedeflenen amaçlara hizmet edemeyecektir. İnternet Değişim Noktasına bağlantı fiyatları düşük olmalıdır. İDN'ye bağlanma maliyetinin, internet kapasitesi almaktan daha az maliyetli olması gerekmektedir. Aksi durumda, İDN'ye bağlanmanın işletmeciler açısından rasyonel olması mümkün değildir.

Mevcut durumda, ülkemizde internet kapasite fiyatları çok yüksektir. Gecikme (Latency) süreleri düşürülmelidir. Türkiye'de gecikme süreleri 100-150 milisaniye iken bu rakam Avrupa'da 20-30 ms, hatta Londra gibi bazı finans merkezlerinin olduğu yerlerde ise 2-3 ms'ler seviyesindedir. Ülkemizde kurulacak olan İDN'ye, başta CDN'ler (Content Delivery Networks - İçerik Dağıtım Ağları) olmak üzere, işletmecilerin bağlanma tercihinde bulunabilmesi için söz konusu gecikme hızlarının düşmesi gerektiği değerlendirilmektedir (TELKODER 2017: 15-19).

Ulusal Kamu Entegre Veri Merkezi (UKEVM) ve Kamu Sanal Ağı (KamuNet)

Siber Güvenlik Türkiye Vizyonu ile ilgili diğer önemli iki husus ise, Ulusal Kamu Entegre Veri Merkezi (UKEVM) ve KamuNet (Kamu Sanal Ağı)'dır. UKEVM**,** Kamuya ait bilgi işleme kaynaklarının kontrol altında tutularak bir ortamda yönetilmesi, verilerin saklanması, işletilmesi ve tek bir noktadan sunulması için oluşturulması planlanan bir ekosistemdir (UABHGM 2021). Kamu Kurum ve Kuruluşlarını doğrudan ilgilendiren, veri merkezi işletmeciliği ve sundukları hizmetler profesyonel olarak ele alınması gerekmektedir. Kamuya ait verilerin, sektörü dışlayıcı bir şekilde, bütün veri merkezi işletmecileri göz ardı edilerek, sadece kamuya ait bir veri merkezinde bulunması; güvenlik, sürdürülebilirlik, veri merkezleri ile ilgili yetişmiş personelin konuya hâkimiyeti gibi açılardan doğru bir karar değildir. Kamunun Veri Merkezlerinden hizmet alım modeline geçmesi dünyada da gündemde olan bir konudur. Bir veri merkezi işletmecisinden hizmet alımı, toplam sahip olma maliyetine göre daha avantajlı olmaktadır (TELKODER 2017: 27).

Hizmet alımına ilişkin örneklerden bir tanesi Güney Kore'dir. Güney Kore Ulusal Bilgi Kaynakları Servisince verilen kararın sonucuna göre, daha önce kendi kaynaklarından yararlanılarak kullanılmaya çalışılan hizmetlerin, bulut hizmetleriyle dışarıdan alınmasıyla maliyetlerde %50'lik bir tasarruf elde edildiği belirtilmektedir (NIRS 2017: 4). Amerika Birleşik Devletleri'nde kamu bilgi işlem yöneticileri 2011 yılında FDCCI (Federal Data Center Consolidation Initiative) ismiyle bir girişim başlatmış ve bir kamu bulutu şeklinde yapılandırılan proje ile ABD, konuyla ilgili harcamalarında %25 tasarruf sağlanmıştır (CIO 2015: 8).

Birleşik Krallık ise "Government as a Platform" ismiyle bir projeyi başlatmıştır. Bu proje ile kamunun uygulamaları bir bulut mantığı ile tek bir platformdan verilmeye başlanmıştır. Şu ana kadar 250 ayrı iş kolunda 1.700 adet uygulama bu platforma taşınmıştır. Böylece Birleşik Krallık yılda 60 Milyon £ tasarruf sağlamıştır (UK 2011: 12). Dünyadaki bu örneklere bakıldığında, kamu bulutu çerçevesinde çalışmalar yapılmış, erişim, tasarım, işletme ve sürdürülebilirlik profesyonel bir çerçevede yürütülmüştür. Kamu Kurumlarımızın, kendi verilerini sınıflandırılması/derecelendirmesi ve saklanma önceliğine göre bu verileri kendi bünyesinde ve/veya veri merkezi işletmecilerinde barındırmasına olanak tanımalıdır. Böylelikle veriler, hem daha güvenli ve düşük maliyetli olarak saklanmış, hem de sektör oyuncuları dışarı itilmemiş ve sektörü büyütücü bir adım atılmış olacaktır (TELKODER 2017: 28).

KamuNet, Kamu kurum ve kuruluşları tarafından içerik güvenliği sağlanan veri iletişiminin, kurumlar arası internete kapalı olan daha güvenli sanal bir ağ üzerinden yapılarak siber güvenlik risklerinin minimize edilmesi, mevcut ve kurulacak olan güvenli kapalı devre çözümlere standart sağlanması, ortak uygulamalar için uygun alt yapının tesis edilmesi ve oluşturulması, planlanan ortak veri merkezi/merkezlerinin dâhil edilmesi amacıyla oluşturulmuştur (UAB 2021).

KamuNet'in kurulmasına ilişkin KamuNet İşbirliği Protokolü UAB Haberleşme Genel Müdürlüğü ile Türk Telekomünikasyon A.Ş. arasında imzalanmıştır. İmzalanan protokol çerçevesinde yürütülecek çalışmalarda ihtiyaç duyulacak her türlü destek ve yardımın bütün kamu kurum ve kuruluşlarınca titizlikle sağlanması ve ulusal siber güvenliğin sağlanması adına önem verilen bu projenin en kısa süre içerisinde tamamlanması amacıyla kamu kurum ve kuruluşları tarafından gerekli hassasiyetin gösterilerek KamuNet ağına dâhil olunması ile İlgili 2016/28 Sayılı Başbakanlık Genelgesi 3 Aralık 2016 tarihli Resmi Gazetede yayımlanmıştır (TELKODER 2017: 29).

Özetlemek gerekirse, KamuNet (veri merkezlerini de ilgilendiren) bir VPN hizmetidir. Pek tabii ki, yukarıda istenen bu hizmetleri, diğer telekomünikasyon işletmecileri de sunabilir. Bu haliyle KamuNet, korunması istenen yazışmaları/verileri gerçekten koruyabilecek midir? "Kırmızı ve Mavi" Kuvvetler yöntemine uygun olarak tesis edilirse korunacağı yönündedir. Bunun için öncelikle, KamuNet'le ilgili Başbakanlık Genelgesinin güncellenmesi ve buna göre yeni bir güvenli altyapı kurulması sağlanmalıdır. Yeni güvenli altyapı şöyle kurulabilir;

- Tüm işletmecilere açık bir ihale yapılır.
- İhale, "Kırmızı ve Mavi" Kuvvetleri temsil edecek iki işletmeciyi belirlemek içindir. Birincisi mevcut yapıyı alıp kendince en güvenli hale getirmeye, diğeri ise sistemi delmeye çalışacaktır. Güvenlik delindiğinde, yer değiştireceklerdir. Ancak bu yöntem ile KamuNet için istenen güvenlik ve hizmet kalitesi sağlanmış olacaktır. Aksi halde diğer işletmeciler dışarıda bırakılıp sadece bir işletmeciye bu işin devredilmesi, istenmeyen birçok durumun yaşanmasına yol açabilecektir (TELKODER 2017: 29).

KAYNAKÇA

- CIO (2015). Federal Chief Information Officer of the United States, Data Center Consolidation and Optimization
- NIRS (2017). *Ministry of the Interior and Safety, National Information Resources Service, Achievements, G-Cloud*
- UK (2011). *UK Government Cloud Strategy*
- UAB (2021). *KamuNet* - https://www.uab.gov.tr/uploads/pages/siber-guvenlik/kamunetweb.pdf

- UABHGM (2021). *Kamu Entegre Veri Merkezi Projesi* - https://hgm.uab.gov.tr/kamu-entegre-veri-merkezi-projesi
- TELKODER (2020). *Ulusal Veri Stratejisinin Oluşturulmasına Yönelik Önerilerimiz* - https://telkoder.org.tr/wp-content/uploads/2020/11/20-051.pdf
- TELKODER (2017). *Veri Merkezi İşletmeciliği - Önemi Anlaşılabildi mi?* https://telkoder.org.tr/wp-content/uploads/2017/12/TELKODER-Veri-Merkezi-Raporu-Aralık2017.pdf