T.C. Tarih : 02.02.2017

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU BAŞKANLIĞI Sayı : 17-009

Konu : VPN Engellemesi

İlgi : 21.11.2016 Tarih ve 16-029 sayılı yazımız

İlgi yazımızda özetle;

- Telkoder üyesi işletmecilerin Ulusal Güvenlik ile ilgili konuların öneminin bilincinde oldukları ve bu konudaki yükümlülüklerini her zaman hassasiyetle yerine getirmeye çalışmakta oldukları,
- Ancak VPN engellemesinin bazı üye şirketlerimizin mevcut sistemleri/altyapılarıyla gerçekleştirmelerinin teknik olarak mümkün olmadığı, bu üyelerimizin geçici çözümlerle yükümlülüklerini yerine getirmeye çalışmakta oldukları,
- VPN engellemesinin ekonomik ve ticari olarak son derece olumsuz sonuçlarının olabileceği konusunda endişelerimizin bulunduğunu

Belirterek, 5809 ve 5651 sayılı yasalar kapsamında işletmecilerin nasıl bir işlem yapması gerektiğine ve nasıl çözüm üretilmesi gerektiğine dair bir toplantı düzenlenmesinin ve Kurumunuz tarafından işletmecilere yol gösterilmesinin yararlı olacağını belirtmiştik.

Kurumunuz Yetkilendirme Dairesi ve ilgili diğer daire temsilcileri ile Telkoder üyelerinin katılımıyla 13 Ocak 2017 tarihinde yapılan toplantıda ve bu toplantıyı takip eden teknik toplantılarda görüşülen konular ve riskler aşağıda özetlenmiştir;

- VPN servislerine erişimi engellemek, zor, pahalı ve kaynak gerektiren bir işlemdir. Bu konuda çok sıkı düzenlemelerin yapıldığı Çin, Rusya ve İran gibi ülkelerde dahi bu tam olarak gerçekleştirilememektedir.
- Günümüzde, Internet üzerinde, başta yasal otoritelerin getirmiş oldukları içerik engelleme kararlarının, medya ve e-ticaret sitelerinin IP adresi bazında coğrafi engellemelerinin aşılmasını olanaklı kılan birçok VPN servisi bulunmaktadır.
- Bu servislerden birçoğu reklam karşılığından ücretsiz hizmet vermektedirler. Ancak üzerinden hizmet verdikleri alt yapı ve kullandıkları teknikler incelendiğinde bu tür servislerin kullanıcı erişimlerini profilleyerek, bu bilgileri kullanıcılarının iradesi dışında başka amaçlarla kullanarak, aslında mahremiyetini korumaya çalışan kullanıcıların mahremiyetlerini ihlal etmelerinin mümkün olabileceği değerlendirilmektedir.
- Bu servisleri sunan firmalar doğrudan veya dolaylı ticari çıkar sağladıklarından, servislerinin verilmesi önündeki engelleri aşmak için sürekli olarak kullandıkları teknikleri ve alt yapılarını geliştirmektedirler. Bu yüzden bu servislere erişimin engellenmesi sürekli bir çabayı gerektirmektedir. Bu servisleri sunan firmalar yazılım dağıtım kanalları üzerinden çok kısa bir sürede kullanıcı tarafındaki yazılımlarını güncelleme kabiliyetine sahiptirler.
- Başta batılı şirketler olmak üzere Internet'i günlük yaşantısının bir parçası haline getirmiş tüm şirketler şirket içi iletişimlerini gizli tutmaya önem vermektedirler. Özellikle ekonomik istihbaratın ön plana çıkması ile VPN kullanmaktan kaçınan veya kullanma imkanı bulamayan şirketlerimiz, bulundukları ülkelerde hedefli veya hedefsiz olarak ticari sırlarını başkalarına kaptırmak riski ile karşı karşıya kalmaktadırlar.
- Erişim engelleme kararları SSL kullanan sitelerde eğer tek bir URL'in engellenmesine olanak tanımıyorsa tüm domainin engellenmesi yoluna gidildiği için Türk siteleri SSL'den uzak durmaktadırlar. Oysa tüm gelişmiş dünyada sitelerin SSL'li hale getirilmesinde %100 oranının hedeflendiği bir dönemde yaşamaktayız.
- VPN servislerinin engellenmesi konusunda Kurum tarafından talep edilen işlemlerin yerine getirilmesi teknik olarak ciddi bir DPI (Deep Packet Inspection) yapısı gerektirmektedir. Bu da aşağıdaki sorunları beraberinde getirmektedir;

- Internet dünyasındaki yöntemlerin çokluğu sebebiyle bir kısım VPN servisleri engellense bile, farklı yöntemlerle bu engellerin kolayca aşılabileceği açıktır. İşletmecilere VPN servislerini engelleme görevi yüklenmesiyle, işletmeciler VPN hizmet sağlayıcılarla mücadele ederken diğer taraftan hiç bitmeyecek bir risk ve yükümlülük altında yaşamak zorunda kalmaktadırlar.
- VPN servisleri yabancı istihbarat kurumları tarafından bulunmaz bir nimettir. Bir ülkenin özellikle bu servisleri kullanabilen nispeten daha eğitimli kısmı blok halinde birkaç VPN servisine yönlendirilmekte ve kolayca kitlesel dinleme yapılabilmektedir. Özellikle İran'daki erişim engellemelerinden sonra İsrail istihbaratının kendine yakın VPN servislerinin pazarlamasını bu ülkede yaptığı haberleri Internet'te birkaç arama yapılarak kolayca bulunabilir.
- DPI teknolojisini içeriğe müdahale amaçlı olarak işletmeci şebekelerinde bulundurmak işletmecilere olağanüstü maliyetlere katlanmaları zorunluluğu getirmektedir. Diğer yandan, 15 Temmuz sürecinde özellikle büyük işletmecilerde yaşanmış olan sızmaların ülke içi riskler oluşturduğu ve bu risklerin uluslararası "Üst Akıl" tarafından kullanıldığı görülmüştür.
- VPN engelleme konusundan daha önemli olarak, bu sızmaların belki de işletmecilere ait abone kütük bilgilerinin, IP bilgilerinin, İşletmecilerin teknik birimlerdeki personellerinin bilgilerinin başka ellere aktarılmış olduklarını düşünmek, irdelemek ve önlem almak zorunluluğu olduğuna dikkat çekmek istiyoruz. Ayrıca, Kurumun işletmecilere ilettiği mesajları anonim mailler üzerinden göndermesini doğru bulmadığımızı da belirtmek isteriz. Özellikle bu hassas dönemde işletmecilere basit maillerle ve anonim adreslerden gönderilen maillerle bilgilendirme yapılmasının kötü niyetli eller tarafından yanlış yönlendirme yapılmasına çok açık olduğunu ve toplumsal riskler taşıdığına da dikkat çekmek isteriz.

- Sıradan bir Internet hizmetine yapılan bağlantı ile bu tür servise yapılan bağlantıyı ayırt edebilmek ve engelleyebilmek için Deep Packet Inspection (DPI) teknikleri / sistemleri yanı sıra davranışsal analiz yapabilen sistemlere de gereksinim duyulmaktadır. Zira çoğu durumda bir Internet hizmetine yapılan SSL bağlantısı ile bu tür servise yapılan bağlantıyı sadece paket içeriği analizi yaparak ayırt etmek mümkün değildir. Tipik olarak SSL bağlantılarında Client Hello mesajındaki Server

Name Indicator sahası bağlantının nereye yapıldığına ilişkin bir fikir verir ancak, VPN servislerine yapılan bağlantılarda kullanılan yazılımlar bu veriyi pakete eklemedikleri gibi, sahte adresler de belirtebilmektedirler. Bu yüzden kısa bir zaman periyodu içinde aynı IP adresinden şüpheli bir bağlantı yapılıp yapılmadığı kontrol edilerek bir engelleme işleminin yapılması gereklidir. Öte yandan bir NAT geçidi arkasında aynı IP adresi üzerinden VPN bağlantısı yapan ve yapmayan kullanıcılar olabileceğinden, yasaklama kararı için hem kaynak ve hem de hedef IP adresi için geriye dönük bir skor sistemi kullanılması zorunludur. VPN servisi veren firmalar bulut hizmeti veren firmalardan alt yapı hizmeti aldıklarından ötürü, uygulanacak yasaklama kararlarının, diğer Internet servislerine erişimi de aksatabileceği göz önünde bulundurulmalıdır.

- VPN servislerini erişimi, hizmet verdikleri IP adreslerini tespit ederek engellemeye çalışmak, istisnasız tümünün bulut altyapıları üzerinden hizmet vermesinden ötürü, diğer Internet servislerine erişimi aksatacağı aşikardır. Öte yandan bu servisleri veren firmalar çok kısa sürede hizmet verdikleri IP adreslerini değiştirebilmektedirler.
- Engelleme için kullanılabilecek sistemler hem pahalı ve hem de işletilmesi zordur. Bu sistemlerin en iyi verimle çalışması için sürekli olarak yapılandırmalarının güncellenmesi gerekmektedir.
- Bazı yerli yazılım şirketleri asgari donanım kaynakları ve yapılandırma gereksinimine duyan, Türkiye'de geliştirilmiş, ekonomik, özgün bir içerik denetleme / engelleme sistemlerini üretme çabası içindedirler. Bu ürünler URL engelleme amacı ile de kullanılmaktadır. Bu ürünler internet trafiğini izlemekte ve engelleme için ağa paket enjeksiyonu yapmaktadır. Tüm trafiği üzerinden geçirmediği için daha az sistem kaynağına ihtiyaç duymaktadır. Eş zamanlı olarak birden fazla sistem çalıştırılarak yedeklilik sağlanabilmekte, yine üzerinden trafik geçirilmediği operatör firmalar açısından bir “Single Point of Failure” teşkil etmemektedir.
- Yerli firmalar tarafından sunulan çözüm şu anda engellenmesi istenen tüm VPN servislerini tespit edebilmektedir. False Positive tespitlerin en aza indirilmesi ve engelleme performansının artırılması için çalışmaları devam etmektedir. Bazı VPN servisleri arda arda birçok yöntemi denedikten sonra önden tanımlı bir grup IP

adresi içinden seçilen bir sunucunun standart olmayan bir portuna bağlantı yapabilmektedir. Bu IP adresleri ve portlarını da büyük ölçüde tespit etmişledir. Ancak bunları güncel tutmak için sürekli bir çaba gerekmektedir. Yapılan çalışmalarda VPN kullanıcı yazılımlarının, engelleme politikalarının uygulandığı ve uygulanmadığı ortamlarda farklı şekillerde, farklı protokol ve teknikleri kullanarak, bağlantı yapabildikleri de tespit edilmiştir.

- Yerli ürün geliştiricileri elde ettikleri bilgilerin tespiti için kullandıkları teknikleri Kurum ile paylaşabileceklerini belirtmektedirler. Kurumun da kendi denetimlerinde elde ettiği bulguları ve IP adreslerini işletmeciler ile paylaşmasının, etkin bir engelleme yapılabilmesi için oldukça faydalı olacağı düşünülmektedir.
- Yerli ürün geliştiricilerinin elinde uygulanabilecek ekonomik bir çözüm vardır. Bu ürünler VPN erişimlerinin tamamını tespit edebilmekte ancak diğer Internet servislerini aksatmadan azami verimle erişim engellemesi yapmak için çalışmaları devam etmektedir.

Sonuç olarak tespit ve taleplerimiz şöyledir;

- Erişim engelleme ve özellikle VPN engelleme konusu işletmecilere bırakılamayacak kadar ciddi iştir. Kurum ve devletin diğer birimlerinin mutlaka bu işin içinde olması gerekmektedir.
- Engelleme çalışmalarında devletin uzman ve mali destek sağlaması için Kurumun desteği gereklidir.
- Yapılan çalışmalar sonucunda yüzde yüz bir engelleme yapılamayacağının ve bunun bir süreç olduğunun kabulü ile işletmecilerin üzerinde baskı unsuru yaratmadan kamu yararı kapsamında yapılacak çalışmalarda çaba gösterilmesi ile sınırlı tutulması gerekmektedir.
- Kurum sürecin içinde aktif olarak yer almalı, denetimlerinde elde ettiği bulguları işletmeciler ve yerli ürün geliştiricileri ile paylaşmalı, kamuoyunu VPN kullanımının riskleri hakkında bilgilendirmelidir.
- Yerli ürün geliştirilmesi konusu desteklenmelidir.

Yukarıda belirtilen taleplerimizin olumlu karşılanarak gerekli işlemlerin yapılmasını ve yapılan işlemler hakkında tarafımıza bilgi verilmesini arz ederiz.

Saygılarımızla,

Rıdvan UĞURLU	Yusuf Ata ARIAK
Genel Sekreter	Yönetim Kurulu Başkanı

TELKODER

Serbest Telekomünikasyon İşletmecileri Derneği