Siber Güvenlik Konusunda Türkiye'nin 4 Yıl Sonra Hala Ödevlerini Yapmadığı Anlaşılıyor

Füsun Sarp Nebil - *turk-internet.com Yayın Yönetmeni*
fusun@nebil.com

1 ay önce Türkiye'deki internet altyapısına, Garanti Bankası'nı başrole koyan bir saldırı yapıldı[1]. 1 ay sonra siber güvenlik ile doğrudan ya da işi gereği uğraşan 8 farklı uzman ile durumu yeniden değerlendirdik. 2015 sonunda yani 4 yıl önce, TR sunucularına yapılan dDOS saldırı ile de karşılaştırarak bunu yeniden inceledik [2].

Bu saldırıyı analiz edelim. Ama önce Garanti Bankası saldırısından bir kaç gün sonra Ulusal Siber Olaylara Müdahale Merkezi (USOM) tarafından bankalarla yapılan toplantıdan bazı notlar aktaralım;

- Toplantı sonucunda tüm bankalardan, yurt dışı bağımlı servislerin (yani envanterin) çıkarılması istenmiş.
- Yurt dışı bağımlı servislerin mümkün olduğunca azaltılması gibi bir karar alınmış.
- Bankaların dDoS hizmeti için operatörlere bildirdiği IP aralıklarının eksik olduğu durumlar varmış. Sadece internete yayın yapan IP aralıkları değil, tüm IP subnetler bildirilsin ve bildirilenler gözden geçirilsin diye karar alınmış.
- Bankalarca yapılan dDOS testlerine, NTP, DNS, Mamcache, TCP Reflection senaryolarının katılması istenmiş.

Bunları USOM bankalara söylemiş.
Ama biz uzmanlardan aldığımız bilgilerle duruma daha yakından bakalım. Önce yurt içi altyapı ve yurt dışına bağlantılar (çıkışlar).

Yıllardır ihmal edilen Türkiye'nin internet-telekom şebekesi, hem eylül sonunda yaşadığımız deprem, hem de ekim sonunda yaşadığımız siber saldırı sırasında durumunu ortaya koydu. Fiber yatırım 15 yıldır her sene 200-250 bin km yapılmalıydı, oysa toplam 365 bin km.

Cumhurbaşkanı R.Tayyip Erdoğan, geçen hafta "fiber yatırımı engelleyen karşısında beni bulur"[3] dedi. Ama fiber şebekenin ihmal edilmesi tamamen AKP döneminde gerçekleşti. Bugün 3 ya da 4 milyon km düzeyinde olması gereken altyapı, maalesef serbestleşmenin ilan edildiği 2004 ve özelleştirmenin yapıldığı 2005 yıllarından bu yana gelişmedi. Duruyor. Oysa her bir yıl 200 ya da 250 bin km düzeyinde yapılmış olmalıydı.

Ama 2020 yılına ulaştığımız bugünlerde Türkiye'nin tüm yurt içi fiber şebekesi sadece 1,5 yılda yapılması gereken düzeyde yani 365 bin km kadar.

Bugünlerde Türk Telekom günde 100 km döşediğini iletiyor [4]. Ama bu da 1 yıl boyunca her iş günü yapılsa bile 1 yılda ancak 22 bin km eder. Yeter mi?

Yerli İçerik ve Veri Merkezi Sektörü Gelişemeyince Yurtdışı Bant Genişliği Dolu

Bu arada, USOM yetkilileri gayri resmi olarak yaptıkları konuşmalarda, "altyapı ile ilgisi yok, yurt dışından gelen saldırı yani yurt dışı çıkışlarla ilgili" dediğini biliyoruz ama bu ifade altyapının eksikliği yanında yurt dışı bant genişliğinin dolu olması sorununu da ortaya koyuyor.

Öncelikle bir şeyi vurgulayalım; sorunun altyapı ile ilgisi var. Şöyle ki; 365 bin km'lik altyapının küçüklüğü nedeniyle, bu tür bir dDOS saldırısında, oradan-oraya saçılan paketler şebekeyi tıkıyor. Bunun bir nedeni de, trafiği rahatlatacak olan IDN yani trafik değişim noktasının 20 yıldır hala olmayışı [5].

USOM'cuların söylediği noktaya gelirsek; yurt dışı bant genişliği nedense gizli. Neredeyse 10 yıldır yurt dışı bant genişliği açıklanmıyor, vatandaştan ya da sektörden gizleniyor. Bu rakam, BTK'nın her çeyrek yayınladığı raporlara girmiyor.

Ama öğrendiğimize göre yurt dışı çıkışımızın büyüklüğü 9'u Türk Telekom olmak üzere 16 TB düzeyinde. Bunun tamamı doluya yakın çalışıyor. Yedekli çalışması gere-

kirken, maalesef öyle değil. Saldırı sırasında ise doluluk nedeniyle başka yöne hareket etmek mümkün değil.

Yanlış (ya da olmayan) teknoloji politikaları sonucunda ve trafik değişim noktasının da olmaması nedeniyle yurt içinde internet erişimi ve veri merkezi hizmetleri sadece sınırlı (az) değil aynı zamanda pahalı. Bu da yerli içerik ya da yurt içinde yerleşik içerik hizmetlerinin gelişememesi anlamına geliyor.

Bu nedenle de, Türkiye'nin yurt dışından "download" için gereken bant genişliği doygun durumda (satüre). Çünkü internete giren herkes yurt dışından bir şeyler okuyor ya da yazıyor. Aslında yedekli çalışması gerekirken, dediğimiz gibi tamamen dolmuş durumda. Bu da siber saldırının etkili olmasına yardımcı olan bir durum.

Bunu da hatırlatalım.

Siber Saldırı Ne Gösterdi? 4 Yıl Öncekine Nazaran Gelişme Var mı?

Bu bölümde 2019 siber saldırısının bize ne gösterdiğini bir tablo ile analiz edelim. (Not: Kasım ayı sonunda Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin siber güvenlik konulu bir çalıştay düzenlediğini duyduk. Bu çalıştayla ilgili olarak henüz elimize bir bilgi ulaşmadı. Bu çalıştaya sadece devlette çalışan uzmanların çağrıldığı bilgisi var. Dolayısıyla bize uzmanların gösterdiği eksiklerin konuşulup, konuşulmadığı ya da bu konularda görüşme yapılıp, yapılmadığı şeklinde bilgimiz yok. Bilgi ulaşırsa onu da yayınlarız.)

Siber Saldırı Ne Gösterdi? 2015 dDOS Saldırısına Nazaran Güvenlik Konusunda Gelişme Var mı?

4 yıl sonraki bu siber saldırıdan günümüze kadar ki gelişmeleri incelerken 4 bölümde bakacağız.

- Devletin Görevleri
- Telekom Sektöründe Tekel Kalmanın Getirdiği Görevleri
- Üniversitelerin Görevleri
- Halkın ve Özel Sektörün Görevleri

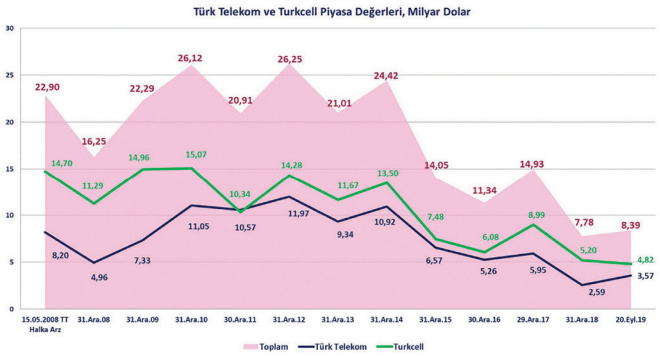
Şimdi sorunlara detaylı bakalım :

Devletin Görevleri

Toptan Bir Telekom Politikası - Stratejisi Yok

Olmamasının sonucunu, küçülen telekom operatörlerinden, dünyanın gerisine düşen internet hızlarından, fiber istediği halde alamayan vatandaşlardan ve veri merkezi ile Türkçe içerik sitelerinin kısır kalmasından görüyoruz.

Telekom sektöründeki düopol (mobilde Turkcell, sabitte Türk Telekom liderliği) hükümetin sandığının aksine sektörü küçültüyor . Aşağıdaki grafiğe dikkatle bakın. Borsaya açılan 2 firmamızın 12 yılda geldiği noktayı göreceksiniz.



4G lisansları ve diğer gelişmeler sonucunda telekom operatörlerinin borç yükünün çok yüksek olmasının da siber güvenlik açısından getirdiği soruna dikkat çekelim.

Ülkemizde 1990'lardan itibaren telekomünikasyon sektöründe serbestleşme ve özelleştirme hedeflendi. Bu amaçla 2000 yılında sektöre bir düzenleyici kuruldu; BTK ve 2004 yılında serbestleşmenin adımı olarak lisanslar ilan edildi. 2005 yılında ise Türk Telekom özelleştirildi. Ama geldiğimiz noktada ne serbestlikten, ne de tekelin yok olduğundan veya rekabetin kurulduğundan bahsedebiliriz. Bunun pazara ve tüketiciye ticari anlamda ve kaybolan değerler (para ve hatta eleman) açısından zararları ayrı bir yazı konusu ama siber güvenliğe zararlarını aşağıda anlatıyoruz.

5G ve dijital dönüşümün motoru olan bilişim ve telekom sektörünün gelişmesinin sağlıklı olması açısından, toptan bir "Telekom Stratejisi" yapılmalıdır. Bunu yaparken de, özel sektör dışarıda bırakılmamalıdır. Bu stratejiyi özel sektörsüz hazırlamak, baştan topal ördek haline getirir.

Telekom stratejisi konusunda "ne olmalı" içeren bir yazı yayınlayacağız..

Siber Güvenlik Stratejisi ve Eylem Planının 2'ncisi 2019 sonunda bitiyor..

Önceki saldırıda da 2012-2014 arasını kapsayan siber güvenlik stratejisi ve eylem plânı süresi bitmişti. Şimdi de 2016-2019 arasını kapsayan siber güvenlik stratejisinin sonuna geldik. 2020 ve sonrasını kapsayan, "Siber Güvenlik Stratejisi ve Eylem Plânı" henüz ufukta görülmüyor.

2013 yılında 2 kere toplanan Siber Güvenlik Kurulu, 2014 ve 2015'de hiç toplanmadı[6][7]. Aynen 2017-2018 ve 2019'da da toplanmadı[8]. Yapılması kanunla konulan 4 toplantı pas geçildi. Ondan sonra da zaten toplantı moplantı kalmadı.

Bu arada bir konuya daha dikkat çekelim. Gerek 2012-

2014 ve gerekse 2016-2019 Siber Güvenlik Strateji ve Eylem Plânlarında yer alan maddelerin, sektörün uzmanları tarafından yetersiz bulunduğunu da iletelim. Hatta 2016 stratejisine giden yolda, turk-internet.com uyarısının da etken olduğunu ve "laf olmasın hemen tamamlayalım" cinsinden bir acilliyet ile yapıldığını düşünüyoruz.

Halkı-Kamuoyunu Bilgilendirme

Son siber saldırının başlangıç saatlerinde durum operatörlerce "rutin saldırı" gibi açıklandı. Evet sürekli siber saldırı oluyor hatta binlerce oluyor. Ama genel olarak erişim engellenmişse, bu rutin değil, büyük bir siber saldırı anlamına geliyor. Bunu saklamak günümüzde hem komik oluyor. Çünkü "connected" yani "bağlı" bir dünyadayız. Biz burada inkâr etsek bile dış dünyada neler olup bittiği tespit edilebiliyor.

Hem tam tersine açıklamak lazım ki elbirliği ile sorunu anlayalım, hasar almayı azaltalım ve belki de çözebilelim.Yani üstünü kapatmak yerine açıklıkla rapor vermek lazım çünkü bazen bu saldırılar arkada başka bir şeyleri saklıyor da olabilir.

Ayrıca saklama yolu seçildiğinde, bizim de kamuoyu olarak bu konuda "güvenimiz azalıyor". Gördüğümüz saldırıyı birilerinin inkâr ediyor olması sonucu değiştirmiyor.

dDOS saldırıların zor saldırılar olduğu da biliniyor. Bir kere başladığında suçlama yerine hep birlikte çözmek için çalışmak lazım. Üstü kapatılınca, demek ki "beceremiyorlar" diye düşünmeye başlıyoruz. En azından güven açısından bunların şeffaf raporlanması lazım.

Proaktif Yaklaşım

Daha önce yayınlanan 2 siber strateji ve eylem planı, pasif önlemleri içeriyor. Daha önceleri BTK tarafından, fiziksel siber tatbikatlar yapılırdı [8]. Sonra bu tatbikatlar fiziksel olmaktan çıkarıldı ve daha sonra da yok oldu. Onun yerine siber yıldızlar gibi yarışmalar gerçekleştirilmeye başlandı.

Bunun yerine fiziksel (haberli) tatbikatların yapılması gerekli. İlaveten yurt dışından gelen yazılım ve donanımın incelenmesi ve raporlanması da USOM tarafından yapılmalı.

Ayrıca USOM ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekipleri (SOME) yapılanması sadece bilgilendirme düzeyinde ve pasif çalışma içeriyor. Gerek "siber istihbarat", gerekse proaktif çalışmalar (Honey-pot gibi) yapılmıyor. Bunların da yeniden düşünülmesi ve plânlanması gerekli.

Örneğin, son saldırıda da "Komuta Kontrol Sunucuları Tespit Edilebilmeliydi". dDOS saldırıları, dağıtık gelir ama aslında bir veya bir kaç merkezden emir alır. Siber mücadele ise, saldırının etkisini azaltmak kadar, bu zinciri kırmak ve hatta kumanda merkezlerini tespit edip, indirmek için çalışılır. Bu da "honey pot" denilen sistemler gibi sistemler kurularak yapılır. Bunu yapacak olan ulusal yapıdır yani USOM bunu yapabilmeliydi, ama böyle olmadı [10][11].

Kritik Varlık Envanteri Çıkarılmalı

Acaba bu ülkenin siber güvenlik açısından en önemli varlıkları nelerdir? Bunu da 2015 saldırısında yazmışız ve bugün hala bu envanter çıkarılmış değil. Günümüzde bazı devletlerin siber orduları var. Bunların ise saldırı yapmaları durumunda en önce elektrik-su gibi endüstriyel tesisleri hedefleyecekleri kolayca tahmin edilebilir.

Bu nedenle, bunların korunması için öncelikle bir envanterin oluşturulması lazım. Garanti Bankası saldırısı sonrasında USOM, yurt dışı için böyle bir envanter istedi. Ama bunun kritik tesisler için de belirlenmesi gerekli [12].

Uluslararası Güvenlik Firma ve Kurumları İle İşbirliği

Güvenlik artık tek başına yapılabilecek bir fonksiyon değil. Bu fonksiyonu koordineli ve işbirliği içinde, yani dünyada olan şeylerden haberdar olarak yürütmek gereklidir.

3 Büyük Operatör ve Devlet Dışındaki Yerel Uzmanlardan Yararlanmak

Devletin zaten az sayıda olan uzmanları kullanmadığını görüyoruz. Daha ziyade, devlette çalışanlarla bir çalışma götürülüyor. Ama sektörde büyük firmalarda çalışmayan yerel uzmanlar da var. Bazıları da kıymetli. Bunların da değerlendirilmesi iyi olurdu. Ama bu yönde

bir çaba görülmüyor. Özel sektör işin içine çekilmez ise, siber güvenliğin yönetimi eksik kalır.

Yerel Yazılım ya da Donanım Firmalarına Özel Teşvik Vermek ve Desteklemek

Yerel firmaların bazıları donanım ve yazılım geliştiriyor ancak hepsinden duyduğumuz şey şu; devlet bu firmaları desteklemek yönünde özel bir çaba göstermiyor. Hatta kamu ihalelerinde, Gartner Listesi gibi taraflı listelerin kullanıldığı görülüyor.

Bir yandan da yurt dışından alınan donanım ve ekipman için bir değerlendirme yapılmıyor olması sorun. Bunun için USOM içinde bir teknik birim kullanılarak, yurtiçine gelen makina ve yazılımlarla ilgili çalışılmalı.

İnsan Kaynakları Yaratmak ve Korumak için Plân Yapmak

Üniversitelerimizde yeterli eğitim olmasa da bu konuya yönelen insanlar görüyoruz. Bu kişilerin teşvik edilmesi ve yurt dışına kaptırılmaması gerekli. Devletin insan kaynağı için "yüksek maaş" dışında önlemler plânlaması şart. Ayrıca operatör, banka ve diğer firmalarda çalışacak siber güvenlik uzmanları için de bazı teşvikler verilebilir. Hem yetişmeleri açısından, hem de ülkede kalmalarını sağlamak açısından [13].

İnsan kaynağı yaratmada, ne idüğü belirsiz yarışmalar değil, bilinçli bir plânlama gerekir.

Telekom Sektörünün Görevleri

Altyapının Güçlendirilmesi

Bunu 10 yıldır defalarca yazdık. 2010 itibariyle yavaşlayan bir strateji var. Sonuçta da bugün ancak 1,5 yılda tamamlanacak düzeyde yani 365.000 km fiber altyapıya sahibiz. Bu da olması gerekenin 10'da biri. Bu kimin ayıbı?

Yurt Dışı Bağlantılar Satüre Durumda ve Yedekli Güzergah Yok

Türkiye'nin kullandığı internet içeriği yurt dışında. Çünkü hem içerik gelişemedi. Hem de içeriği barındıran veri merkezleri sorunlu (aşağıya bakın). Bunun sonucunda yurt dışı bağlantılar doygun (satüre) durumda. Türk Telekom'un 9 TB ve tamamının 16 TB düzeyinde yurtdışı bağlantısı olduğunu duyuyoruz (bu konu nedense açıklanmıyor).

Burada bir sorun da yurt dışına çıkışta yedekli olarak ele alınan çıkışların aynı yerden geçiyor olması. Tabi bunu bir kaç şekilde de yani "çünkü trafik değişim noktası yok" diye de tanımlayabiliriz. Dünyada operatör sayısına bağlı olarak, özellikle kurumların yedekli yani birden fazla operatörden hizmet alma alışkanlığı var. Bu da saldırının bir yerden gelmesi ya da başka bir arıza durumunda, diğer yandan devam edebilmeyi sağlar. Ama ülkemizde tekel var. Hatta şu anda mevcut olan, topallayarak ya da küçük kalarak da olsa hayatta kalan küçük firmalar da yok edilmeye çalışılıyor. Oysa mesela bankalar bir büyük telekom firmasında, bir de küçük firmadan hat alabilirler. Ama telekom stratejimizde sorun var. Bunu yapmıyoruz. Dolayısıyla saldırı geliyor ama biz başka tarafa dönemiyoruz. Saldırıyı atlatamıyoruz. Sistemi kapatıyoruz.

Yurt Dışı Bağlantılar Parçalı, Bütün Değil

Bağlantılar eskiden bu yana gelen bağlantılar. Bu nedenle de eski moda yani 100 Gbps yerine 10 x 10 şeklinde. Bu da bir saldırının kolayca yolları tıkaması anlamına geliyor.

Bugün dünyada 1,3 TB'lere ulaşmış saldırılar var. Belki eski alışkanlık, belki yatırımdan kaçmak için 10 GBps x 10 adet şeklinde kullandığımız bir yapımız var ise, bunun anlamı, 10Gbps lik sadece 1 adet linkin dolması ile 100 Gbps'lik yapının hepsinin birden çökmesi, yani siber saldırıya daha çabuk yenilmektir. Bunların durumunun da yayınlanması lazım ki, bilelim.

Yurt Dışından Gelen Trafik İçin Yönetim Yapılmıyor

Yurtdışı trafiği yönetmede zayıf kalıyoruz. Çünkü kısıtlı bilgi birikimi ile karşı karşıyayız. Son siber saldırıda olduğu gibi, bir nedenle yurt dışı trafiği kapatılması gerektiği durumlarda -ülke içi hizmet alanlara sadece bir açıp/kapatma anahtarı verilmesi nedeniyle- Türkiye'den erişim tüm dünyaya aynı anda kesiliyor. Halbu ki dünyada bunun karşılığı olarak bölgesel, kıtasal olarak erişim kısıtlamak ve saldırı trafiğini yönetmek mümkün olabiliyor.

Bu tür saldırıların yurt dışında karşılanması ve temizlenmesi gerekirdi. Sonunda bu yola gidildi. Ama baştan da yapılabilirdi.

dDOS Temizleme (ve de Botnet temizleme) Yetersiz

Türk Telekom 2-3 yıldır İstanbul ve Ankara'dan dDOS temizleme servisi veriyor. Çeşitli sektör uzmanından bu servisin yetersiz olduğu bilgisini alıyorduk. Saldırı sırasında yetersiz olduğu görüldü. Garanti Bankası yurtdışından bu hizmeti almak zorunda kaldı.

Zaten yedek ekipmanı müşteri alıyor. Geçmişe göre gelişme var ama yeterli değil.

Diğer yandan botnet konusunda USOM'un çalıştığı görülüyor ama dediğimiz gibi bunun da bilgi vermek düzeyinden, önceden tespit düzeyine yani proaktif düzeye çıkması lazım. Çünkü asıl risk sızma ile ilgili.

Uluslararası Taşıyıcılar Ülkemizde Servis Veremiyor

Google, Microsoft vs gibi büyük firmalar neden gelip sunucularını ülkemize kurmuyor diye merak ediyoruz. Bunun bir nedeni, altyapının düzgün olmaması, diğer nedeni düzenleyici/hukuk altyapısındaki sorunlar ise, üçüncü neden bu taşıyıcıların ülkemize gelmesinin yani

rekabetin bizzat engellenmesidir. Komşumuz Bulgaristan ve Romanya'da ve hatta Dubai'de 100'den fazla taşıyıcının kendi fiberlerini getirip taşıdığı "hub"lar var. Bizde yok. Bunun anlamı ise şudur; siber saldırıya uğradığımızda, bu tür taşıyıcılar olsaydı, ayakta kalabilirdik.

Trafik Değişim Noktası HÂLÂ YOK

Türk Telekom lehine olmak üzere yıllardır (en az 20 yıl) Türkiye'de trafik değişim noktası kurulamıyor. Oysa, Balkanlar, Kafkaslar ve Ortadoğu (hatta Afrika ve Uzak Doğu) arasında bir köprü görevi görecek olan böyle bir değişim noktası ülkeye para kazandırabilir, güvenlik açısından da avantaj olur. Ama bunu zaten çoktan kaybettik bile[10].

Üstelik bu hareket korunulmaya çalışılan firmanın ne zarar etmesini engelledi, ne de borcunun gittikçe ölçülemez düzeyde yükselmesini.

Knowhow ve İnsan Kaynakları Gelişimi

Az sayıda firmayla verilen servis, ülkemizde bilgi birikimini engelliyor. Farklı teknolojileri denemek, öğrenmek, tecrübe ve bilgi birikimi yapmak mümkün olmuyor. Zaten telekom firması sayısı az olunca, telekom teknolojisi bilen uzman sayısı da az oluyor. Bugün siber saldırı olduğunu bile hemen farkedemeyişimizin başında bu sorun geliyor. Üstelik elimizdeki az sayıda insanı da hızla yabancı ülkelere kaybediyoruz (Ör: Aselsan'dan Hollanda'ya giden mühendisler [9])

Üniversitelerin Görevleri

Marka Bağımlı Eğitime Son Verilmeli

Özellikle teknik üniversitelerin siber güvenlik alanında kendilerine özel -bir marka ile işbirliği olmayan- siber güvenlik programları geliştirmesi lazım. Cisco, Microsoft öğreterek siber güvenlik olmaz.

Üniversiteler Devlete Strateji Geliştirmeliler

Yukarıdan aşağıya bahsettiğim, telekom politikası ya da insan kaynakları ya da USOM-SOME nasıl şekillenmeli konularında, devlet talep etmemiş olsa bile, üniversitelerin çalışma yapması, yayın yaratması, özgün makale, özgün kitap, özgün siber güvenlik bilimi geliştirmesi gerekmez mi?

İnsan Kaynağının Güçlendirilmesi

Üniversitelerin esas görevi olan bu konuda, lisans öğrencileri kadar, lisans sonrası programlar için çalışılmalı

Vatandaşın ve Özel Sektörün Görevleri

Siber Güvenlik Konusunda Bilincin Yükselmesi

Vatandaş ya da şirketler (bireysel ve kurumsal kullanıcılar) heyecanla yeni uygulamalar, yeni yazılımlar, yeni donanımlar kullanıyorlar. Ama bunları kullanırken, kendilerinin ya da kendilerinin bilgisizliği sonucunda firmalarının/diğer kişilerin maruz kalabilecekleri tehlike ve riskleri inceliyorlar mı? Pek değil.

Ayrıca bu konuda sadece halkın değil, devletin de bilinçlendirme çalışmaları yapması, belki kamu spotları yayınlaması gerekmez mi?

Telekom Hizmetleri Kullanım Bilincinin Yükselmesi

Kullandığınız bant genişliği, boyut x fiyatını seçerek satın aldığınız pakete uyuyor mu? Yoksa kandırılıyor musunuz? 16 MB'a kadar dedikleri hat sadece 2 MB mı veriyor? Bu da altyapı konusunda neden gelişemediğimizin bir göstergesi.

Ne aldığınızı dikkatle inceleyin. Doğru değilse, talep edin. Gerekirse tüketici hakları, BTK ya da mahkemeler yoluyla hakkınızı arayın. 1 kişinin araması ile belki işler düzelmez ama çok kişinin hakkını araması konuyla ilgili soruna bilinci yükseltir.

Özel sektördeki firmaların da telekom hizmetlerini nereden alacakları konusunda kendilerini geliştirmeleri lazım. Bankaların ve diğer kurumların kendi veri merkezlerini kurmaları, yazılım yapmaları, data centercılık yapmaları anlamlı mı? Bunu tartmak lazım.

Sahte Haber de Bir Siber Saldırı Cinsidir, Farkında Mısınız?

Son olarak, önümüzdeki dönemde yükselecek bir dalga olarak "sahte haber" konusuna dikkatinizi çekelim. Bu konuya özel ilgi gösterin ve lütfen, kendinize haberleri test etmek için bazı çıpalar belirleyin. Aksi takdirde önümüzdeki günlerde dalgalanmak mümkün, çünkü basın kaynaklarının çeşitlenmesi ile arka planda çeşitli konsoloslukların yer aldığı bir yapı göze çarpıyor.

Deep Fake gibi teknolojilerin de artık kullanıma girdiğini de yükseldiğini unutmayın. Nasıl 6-7 Eylül olaylarının arka planında Atatürk'ün Selanik'teki evinin yakıldığına dair sahte bir haber varsa, bugün de internet üzerinden bu tür haberler yayılacaktır.

Bu nedenle her habere hemen inanmayın. Paylaşım yaparken de, dikkatli olun. Gerçek olduğunu doğruladığınız haberleri paylaşın.

SONUÇ

- Devletin hem "Siber Güvenlik" hem de "Telekom'da Tekel" Stratejilerini Gözden Geçirmesi Lazım.. ACİL!
- Acilen fiber yatırımların önü açılmalı ve bu alanda rekabet sağlanmalıdır.
- USOM ve SOME mekanizması güçlendirilmeli, siber tatbikatlar fiziksel olarak gerçekleştirilmelidir.
- Bu stratejiyi sadece devlette masa başında oturan ve gerçek müşteri ile uğraşmayan, saldırılarda eli yanmayan kişilerle oluşturursanız, yanılırsınız. Oluşan strateji sadece teorik olur. Ayrı bir sivil yapı

içinde değil, aynı yapının bir parçası olarak değerlendirilmesi şart.

- Siber saldırılar konusunda "şeffaflık" mekanizmaları oluşturmak gerekir. Çünkü bir saldırı, bir başkasına taban sağlıyor da olabilir.
- Siber saldırılar sadece dDOS değildir. Veri de çalabilir. Nasıl Pasifik'teki 2004 Tsunami'si sonrasında uyarı mekanizması kurulduysa bizim de uyarı mekanizmaları oluşturmamız lazım.
- Üniversitelerin siber güvenlik konusunda özgün eğitim vermeleri sağlanmalıdır
- Halk, medya ve özel sektörde farkındalık arttırılmalıdır. Bunun 2. Dünya Savaşı ya da Kıbrıs Harekatı sırasında verilen eğitimlerden farkı yok.

Bu yazı, 8 farklı uzmanın ortak görüşleri ile oluşturuldu. Uzmanlar bazen bir şeyleri kendi isimleri ile söylemeye de çekiniyorlar ama birilerinin bunları söylemesi lâzım. Bu konu devleti ya da belli sayıda uzmanı değil, finans kurumları, ticari kurumlar ve halkı da etkiliyor.

Sırası gelmişken de vurgulayalım; telekomünikasyon stratejik bir sektördü. Telekomünikasyon altyapıları da, Türkiye'ye ve Türk halkına aittir (başka ülkelerde de o ülkelere aittir). Sanıldığının aksine bir firmaya ait değildir. Sadece "kullanım imtiyazı" verilir. Türkiye'de bu imtiyaz tüm firmalara 2026 yılına kadar diye verilmiştir. Bunu alan firmanın para kazanma hakkı ne kadar varsa, o kadar da yatırım yapma mecburiyeti vardır ve ama bu mecburiyeti devlet nedense zorlamadı. Devletin bu hakkı zorlamaması da halkın hakkının kaybı anlamına gelmektedir. Bunun tam olarak farkında olalım.

KAYNAKLAR:

[1] 27 Ekim 2019 Siber Saldırısı

[2] DDOS Siber Saldırısı Türkiye'ye Ne Gösteriyor? Ne Öğretiyor?

[3] TELKODER: "Sayın Cumhurbaşkanı İle Aynı Görüşte Olmak Bizi Mutlu Etti"

[4] Portların % 33'ü Boş Her Gün 100 Km Döşüyoruz

[5] James Cowie ; İran ve Irak, Ermenistan Üzerinden Sofya'ya ve Avrupa'ya Bağlanıyor, Türkiye Oyun Dışı Kalıyor

[6] BAKANLAR KURULU KARARI

[7] Siber Güvenlik Kurulu 2.Defa Toplandı

[8] Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı Resmi Gazetede Yayınlandı

[9] Yarın Uluslararası Siber Kalkan Tatbikatı Yapılacak

[10] Breaking the DDoS Attack Chain

[11] US and Taiwan hold first joint cyber-war exercise

[12] Taner Yıldız : Frekans Düştü Ama Bunu Tetikleyen Sebebin Ne Olduğu, Müdahele mi, Teknik mi, Manipülasyon mu, Söyleyemiyoruz..

[13] Aselsan Yönetim Kurulu Başkanı Görgün Ayrılmaları Doğruladı ama % 2 Dedi

[14] AB Siber Saldırıların Açıklanmasını Mecbur Kılacak Kanun Hazırladı

ATECH FUARI'NDA "AKILLI BİNALARDA ENERJİ VE ELEKTRONİK SİSTEM YÖNETİMİ" PANELİ DÜZENLENDİ

21-23 Kasım 2019 tarihlerinde Ankara'da gerçekleştirilen "Akıllı Bina Teknolojileri Elektrik Sistemleri Fuarı"nda Elektrik Mühendisleri Odası Ankara Şubesi tarafından "Akıllı Binalarda Enerji ve Elektronik Sistem Yönetimi" paneli 22 Kasım 2019 Cuma günü düzenlendi. Panelin yöneticiliğini EMO Ankara Şubesi Yönetim Kurulu Sayman Üyesi Tufan Teziş yaptı.

Panelde ilk olarak söz alan Arif Künar "Kamu Binalarında Enerji Yönetimi"ni anlattı. Künar sunumuna "Enerji verimliliği eşittir en temiz enerji kaynağı, enerji verimliliği eşittir yenilenebilir enerji, enerji verimliliği eşittir en ucuz enerji kaynağı, enerji verimliliği eşittir en hızlı enerji kaynağı" diyerek başladı. Yılda 10 milyar dolarlık bir tasarruf sağlanabileceğinin altını çizen Arif Künar şunları söyledi; "Çok ciddi bir yan sanayi ve ar-ge yatırımı gerçekleşebilir. EVD firmaları, SÜPER ESCO-ESCO ve Türk mühendislik, danışmanlık, müteahhitlik firmaları gelişir, dışa açılır.İstihdam artışı sağlanır, Ülke çapında zincirleme bir yeşil "ekonomik kalkınma-iyileşme-gelişme-büyüme-sürdürülebilirlik" sağlanır. Enerji arz güvenliği, finansal kriz, dışa bağımlılık, iklim değişikliği, karbon yaptırımları, yeni enerji yatırımı, uluslararası rekabet vb. sorunların çözüme katkı sağlar." dedi.

Akıllı Binalarda Teknolojik Sistemler İş Ve Ev Yaşantımızı Kolaylaştırmaktadır

Arif Künar'ın ardından söz alan Ali Yiğit "Akıllı Binalar ve Entegrasyon" konusunu anlattı. "Gerek teknolojik gelişmeler gerekse bu gelişmelerin binalara uygulanması hem bu binalarda yaşayan insanların işlerini ve yaşamlarını kolaylaştırmakta hem de zaman ve kaynak tasarrufuna olumlu katkı sağlamaktadır." diyerek sunumuna başlayan Ali Yiğit sözlerini şöyle sürdürdü, "Teknolojik gelişmelerin binalara uygulanması, birden fazla sistemin belli bir senaryo çerçevesinde birlikte çalışmasını gerektirmektedir. Geçmiş dönemlerde kullanılan cihazlar arasında belli bağlantılar sağlayarak ve/veya role vb cihazlarla oluşturulmaya çalışılan senaryolar artık sistemlerin haberleşmesi şeklinde gelişmektedir. İnsanlar yaşamlarının büyük bir kısmını gerek ev gerekse iş yaşamı olarak binalarda geçirmektedir. Binaların temelinden başlayıp bir yaşam alanına dönüşmesine kadar; hem can ve mal güvenliğini sağlamak hem de insan ve iş yaşamını kolaylaştırmak için bir dizi elektronik sistem yapı üretim sürecinde yer almaya başlamıştır. Yapılardaki tüm elektronik sistemler tekil olarak düşünüldüğünde belirli bir işlevi yerine getirmek için geliştirilmiş olan sistemlerdir."

Panel haberinin tam metni için başlığa tıklayınız.