SİBER GÜVENLİK ve KAMU KURUMLARI için MİLLİ SERTİFİKASYON MEKANİZMASI

Mustafa AFYONLUOĞLU
afyonluoglu@gmail.com

21.01.2018

E-Devlet ve Siber Güvenlik

"Devletin, vermekte olduğu hizmetleri bilgi ve iletişim teknolojilerinden istifade etmek sureti ile daha hızlı, kolay, ekonomik şekilde her yerden ve her zaman vermesi" olarak hayatımıza giren "e-Devlet" kavramı, bu hizmetleri sağlarken temin ettiği ve hizmetler sonucunda oluşturduğu veriler bakımından "siber güvenliği" de beraberinde getirmiştir. Bu verileri genel çerçevede:

- Kişisel veriler
- Kamu verisi / kamu sırrı (Veri Gizlilik Seviyeleri)
- Ticari veriler / ticari sırlar
- Açık veri / anonim veri / istatistiki veri

olarak kategorize ettiğimizde, farklı güvenlik seviyelerinde korunması gereken bilgi kümelerinin olduğunu açıkça görürüz. Verinin güvenlik seviyesi yükseldikçe ona olan ilgi de artmakta ve siber saldırılara hedef olmaya başlamaktadır.

Özellikle kamu kurumlarında, e-Devlet çerçevesinde verilen hizmetlerin getirdiği entegrasyonlar sebebi ile siber güvenliği kurum bazında ele almak yeterli olmayıp bütüncül olarak yaklaşma zorunluluğu ortaya çıkmaktadır. Günümüzde olgunluk seviyeleri yüksek e-devlet projelerine sahip olan kurumlarımız, bir projede 10 ile 15 Bakanlık ve bazılarında 40'dan fazla kurumla entegrasyon yaparak hedeflediği hizmeti vermektedir. Böylesine yüksek sayıda ve karmaşık içerikte entegrasyonların yer aldığı projelerde, verilen hizmetin kalitesi ve sürekliliği kadar sistemin siber güvenliği de zincirin en zayıf halkasının güvenliği kadar olabilmektedir.

Siber Güvenlik ve Milli Güvenlik

MGK tarafından "Milli Güvenlik", "*Devletin milli varlığına, bekasına ve güvenliğine yönelik tehditlere karşı tedbirler almak için bölgesel ve küresel ortamın izlenerek tehdit ve fırsatların tespit edilmesi ile bu hususlara uygun siyasetin belirlenmesini ve en uygun politikaların uygulanmasını sağlayacak süreç ve unsurlar*" olarak tanımlanmaktadır[*1]. Bu çerçevede milli güvenliğin temel unsurları arasında yer alan askeri, siyasi, diplomatik ve ekonomik bileşenlerin yanına "**siber**" unsurlar da girmektedir. Nitekim, savunma sahası bakımından Temmuz 2017 tarihli NATO açıklamasında, kara, hava, deniz ve uzay'dan sonra **siber alan** 5. operasyonel alan olarak ilan edilmiş[*2], Aralık 2016'daki NATO toplantısında, uluslararası hukukun siber alanda da uygulanması gerektiği belirtilmiş ve 14 Aralık 2017 tarihinde, NATO'nun kolektif savunma çerçevesindeki çekirdek görevlerinden birisinin siber savunma olduğu vurgulanmıştır[*3].

Siber güvenliğin, milli güvenliğin bir parçası olduğu çağımızda, aşağıdaki tespitler dikkat çekicidir:

1. Türkiye'de kamu kurumlarında kullanılan siber güvenlik ürünlerinin temininde, hiç birisi için şart koşulan bir **güvenlik sertifikasyonu / güvenlik onayı** ve **kontrol listesi mekanizması** yoktur.
2. Türkiye'de kamu kurumlarında kullanılan siber güvenlik ürünlerinin **%97'si yabancı** menşeili olup sadece %3'ü yerli ve/veya milli üründür[*5].
3. Geçmişte yabancı menşeili birçok ürünün, kriz dönemlerinde kamu kurumları ve özel sektördeki ürünlere uzaktan müdahale ettiği veya bu ürünlerin hatalı karar vermesini sağladıkları görülmektedir. Örneğin **İsrail** menşeili Checkpoint marka güvenlik duvarı yazılımı, Mavi Marmara ile ilgili haber yapan sitelerin tamamını "hacker" veya "porno" kategorisine alarak erişimin engellenmesini sağlamıştır. Benzer şekilde **ABD** menşeili anti-virus programı, "Free Gazze", "Filistin" adı altında yapılan aramaları "terör" kategorisine sokarak erişimi engellemiştir[*4].
4. Günümüzde en etkin ve yaygın hedef odaklı siber saldırı gruplarının tamamı devlet desteklidir. Bu grupların temel motivasyonu **casusluk** ve kritik altyapılara **sabotaj**dır[*6].

Saldırı Grubu	Kısa Adı	Ülke	Kuruluş Yılı	Motivasyonu	Hedef Kategoriler
Sandworm	Quedagh, BE2 APT	Rusya	2014	**Casusluk**, **Sabotaj**	**Hükümetler**, **Uluslararası Organizasyonlar**, **Avrupa**, **Amerika**, **Enerji Sektörü**
Fritillary	Cozy Bear, APT29, Office Monkeys	Rusya	2010	**Casusluk**, Hükümet Devirme, Yıkma	**Hükümetler**, Düşünce Örgütleri, Medya, **Avrupa**, **Amerika**
Swallowtail	Fancy Bear, APT28, Sednit	Rusya	2007	**Casusluk**, Hükümet Devirme, Yıkma	**Hükümetler**, **Avrupa**, **Amerika**
Cadelle	-	İran	2012	**Casusluk**	**Havayolları**, **İletişim**, **İran Vatandaşları**, **Hükümetler**, STK'lar
Appleworm	Lazarus	Kuzey Kore	2012	**Casusluk**, **Sabotaj**, Hükümet Devirme, Yıkma	**Finans Sektörü**, **Askeriye**, **Hükümetler**, Eğlence sektörü, Elektronik Cihazlar
Housefly	Equation	ABD	2001	**Casusluk**	Ülke saldırganlarına yönelik hedefler
Strider	Remsec	Batı	2011	**Casusluk**	**Büyükelçilikler**, **Havayolları**, **Rusya**, **Çin**, **İsveç**, **Belçika**
Suckfly	-	Çin	2014	**Casusluk**	**e-Ticaret**, **Hükümetler**, Teknoloji, **Sağlık Sektörü**, **Finans Sektörü**, **Gemicilik Sektörü**
Buckeye	APT3, UPS, Gothic Panda	Çin	2009	**Casusluk**	**Askeri Alanlar**, **Savunma Endüstrisi**, Medya, Eğitim Sektörü, **ABD**, **İngiltere**, **Hong Kong**
Tick	-	Çin	2006	**Casusluk**	**Teknoloji**, Yayıncılık, **Japonya**, Su Mühendisliği

Yüksek etkiye sahip saldırılar yapan ve hedef odaklı saldırı gruplarının hepsi, ülkeler tarafından desteklenmektedir.

5. 06 Nisan 2017 tarihli NATO'nun Varşova Zirvesi'ndeki açıklamasında, Denver Üniversitesi'ne yaptırdığı araştırmada, 2030 yılında Siber Güvensizlik hacminin **90 trilyon dolar** olduğu öngörülmüştür.
6. Ülkelerin siber güvenlik bütçeleri gün geçtikçe savunma bütçeleri ile yarışacak seviyede artmakta olup Fransa'nın bu alandaki 2014 bütçesi 1 milyar €, İngiltere'nin 2016 yılı siber güvenlik bütçesi ise **2.5 milyar €**'dur.
7. 2017'de Türkiye'deki siber güvenlik pazarının hacmi yaklaşık **1.5 milyar dolar** olarak ölçülmüştür.
8. Siber güvenlik dünyasında oluşturulan ürün ve hizmetler, bu ciddi pazardan pay almak üzere önemli bir alan olarak gündeme gelirken, ayrıca **siber istihbarat, siber casusluk, siber saldırı** gibi alanlar için de olası bir araç olarak karşımıza çıkma potansiyeli barındırmaktadırlar.

Siber Güvenlikte Sertifikasyon ve Akreditasyon

Siber güvenliğin ülke güvenliğinde bu kadar önemli konuma oturduğu günümüzde, bunu sağlayan cihazların (ve yazılımların) güvenliği ve güvenilirliği önemli bir problem olarak önümüze gelmektedir. Bu aşamada sertifikasyon, ürün ve servislerin güvenliği ile güvenilirliğini arttırmak ve istenilen çizginin üzerinde tutmak için kritik rol oynayan bileşendir. Gerek yabancı menşeili, gerek yerli gerekse milli ürünlerin hem uygun güvenlik ve güvenilirlik seviyelerine ulaşması, ayrıca milli ürünlerin küresel ekonomide daha çok kabul görmesi için, sertifikasyon şarttır. Nitekim bu konuda özellikle Avrupa Birliği'nde birçok sertifikasyon yapıları mevcuttur. Ayrıca AB, geçerli sertifikasyonlar için, Birliğe üye ülkelerde bütünlük sağlanması ve pazarda doğru kriterlere göre rekabet edilebilmesi için bir "**Siber Güvenlik Sertifikasyon Çerçevesi**" oluşturmak ve ayrıca ENISA bünyesinde **Siber Güvenlik Ajansı** kurmak üzere 13 Eylül 2017'de bir düzenleme önerisi yayınlamıştır[*7].

Sertifikasyon mekanizmasının talebi karşılayabilmesi ve sürdürülebilir olması bakımından, bu hizmette görevlendirilecek kamu kurumları ve bu hizmete talip olacak özel sektör için akreditasyon mekanizması çalıştırılmalıdır.

Öneriler

Tüm bu hususlar ele alındığında, siber güvenlik alanında hem yerli ve milli yatırımcıyı daha verimli olarak sahada konumlandıracak, hem de kamudaki siber güvenliği güçlü ve disiplinli hale getirecek öneriler aşağıda sıralanmıştır:

1. Siber güvenlik alanında başta kamu kurumları ve **kritik altyapılar** olmak üzere veri üreten tüm yerlerde konumlandırılacak yazılım ve donanım ürünlerinin yerli ve hatta **milli çözüm** olması gerekliliği konusunda bir şüphe bulunmamaktadır.
2. Siber alan çok geniş olduğu için, bu alana yatırım yapacak ve yapmakta olan sektör için, **önceliklendirilmiş siber güvenlik alanları** belirlenerek **ulusal siber politika** şeklinde ortaya konulmalı ve başta teşvik mekanizmaları olmak üzere tüm yatırımlar ve uygulamalar bu politika çerçevesinde ele alınmalıdır. Rekabet ve sürdürülebilirlik açısından her alanda **en az iki çözüm**ün sektörde oluşmasına ilişkin teşvikler gündeme alınmalıdır.
3. Siber güvenlik ile ilgili olan tüm yazılım ve donanım çözümleri, kamu kurumlarında konumlandırılmadan (ihale aşamasından) önce, her ürün segmenti için belirlenmiş olan **sertifikasyon** ve kontrol sürecinden geçirilmeli, bu süreci başarı ile geçen ürünler "**beyaz liste**" olarak ilan edilmelidir. **Kontrol süreci**nde, ürünlere, (bu konuda yetkilendirilecek ilgili kamu kurumu tarafından oluşturulacak olan) milli penetrasyon test aşamaları da uygulanarak herhangi bir arka kapı veya açık olmadığı da ortaya konulmalıdır. Kamu alımlarında siber güvenlik çözümlerinin **beyaz liste yer alması ön şart** olmalıdır.
4. Kurumlarda konumlandırılan ürünlere ilişkin tüm **yeni çözüm ilaveleri ve güncellemeleri**, bir üst maddede belirtilen kontrol süreçlerinden geçip onaylandıktan sonra uygulanmalıdır.
5. Belirtilen kontrol süreçlerine ilişkin hizmeti yeterli kapasitede ve kalitede ortaya koyabilmek için, bu konuda hizmet verecek kamu ve özel sektöre **akreditasyon** mekanizması işletilmelidir.
6. Siber güvenlik ürünlerinde, içerisinde kullanılan teknoloji kadar, sahadan toplandığı veri çerçevesinde oluşturulan olgunluk da çok kıymetlidir. Bu da ancak ürünlerin geniş bir sahada konumlandırılarak gerçek veriler ile karşı karşıya kalması ve buna ilişkin algortimaların olgunlaştırılması ile mümkün olur. Doğal olarak bir ülkede bu anlamda en geniş veri sahası

kamu kurumlarında bulunmaktadır. Dolayısıyla özellikle milli ürünler için bu sahada yer almak ve saha tecrübesi ile olgunlaşarak rekabette daha güçlü konuma ulaşmak son derce önemlidir.

7. Kamu kurumlarında konumlandırılacak siber güvenlik çözümleri bakımından yerli ve akabinde **sadece milli çözümler**in konumlandırılmasına ilişkin **kademeli geçiş planı** hazırlanmalıdır:
    a. Yerli ve akabinde sadece milli çözümlerin (*eğer kontrol sürecinde, yetkinlik ve yeterliliklerini kanıtlamış olgunluğa erişmedikleri ortaya konulmuş ise*) kurumda, ilk aşamada mevcut çözümlere ilaveten ikincil eşdeğer çözüm olarak konumlandırılması önerilmektedir.
    b. Kontrol süreçlerinde ve saha uygulamalarında yetkinlik ve yeterliliğini kanıtlayarak belirli olgunluk testini geçen ürünler, kurumlarda birincil konuma taşınmalıdır.
    c. Birincil konumdaki çözümlerin önce **bölgesel** sonra da **küresel açılım**larına ilişkin sektöre devlet tarafından mali teşvikin yanısıra (*başta Güney Kore olmak üzere İngiltere, Fransa gibi ülkelerde uygulanmakta olan devlet politikalarında olduğu gibi*) diğer ülkelerde bu çözümlerin konumlandırılmasına ilişkin idari ve hukuki destek de sağlanmalıdır.
8. Üniversitelerde bu alanda AR-GE çalışmalarının **önceliklendirilme**sine ilişkin modeller hayata geçirilmeli, 4691 sayılı **Teknoloji Geliştirme Kanunu**'na, siber güvenlikte AR-GE odaklı başvurulara ilişkin **ayrıcalıklar ve öncelikler** ilave edilmelidir.
9. Siber güvenlikle ilgili verilen tüm teşviklerde, ortaya konulan fikirden başarılı bir **AR-GE** ürünü oluşturulması yeterli görülmemeli, neticenin bir **ürün/çözüm** haline gelip ekonomiye kazandırılması süreci şart koşulmalı ve destekler de bu sürece kadar kademeli ve kontrollü olarak devam etmelidir.

Referans Kaynaklar:

1. Milli Güvenlik Kurulu Genel Sekreterliği Web Sitesi, http://www.mgk.gov.tr/index.php/milli-guvenlik-kurulu/genel-bilgi
2. NATO – Siber Savunma, 14.12.2017: http://www.nato.int/cps/en/natohq/topics_78170.htm
3. NATO http://www.nato.int/docu/review/2017/Also-in-2017/nato-priority-spending-success-cyber-defence/EN/index.htm
4. Mavi Marmara sabıkalı yazılım ne kadar güvenli?, 19.09.2017: http://www.turkiyegazetesi.com.tr/teknoloji/504287.aspx
5. Siber Güvenlik pazarının %97'si yabancılarda, 23.01.2017: http://www.iha.com.tr/haber-siber-guvenlik-pazarinin-yuzde-97si-yabancilarda-619115/
6. 27 Nisan 2017 Symantec Corp. Internet Security Thread Report, Vol: 22
7. The EU Cybersecurity Framework, 19.09.2017: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework
8. COM(2017)477 - Proposal for Regulation: EU Cybersecurity Agency and ICT Cybersecurity Certification (Cybersecurity Act), https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en