SİBER GÜVENLİK HUKUKU ÇALIŞTAYI

SONUÇ BİLDİRGESİ

T.C Ulaştırma Denizcilik ve Haberleşme Bakanlığı, **Bilgi Güvenliği Derneği**, **Türkiye Barolar Birliği** işbirliği ile düzenlenen **Siber Güvenlik Hukuku Çalıştayı**, 25-26 Ocak 2012 tarihlerinde Ankara'da Türkiye Barolar Birliği Konferans Salonunda yapılmıştır. Konferans hakkındaki bilgilere www.iscturkey.org/calistay adresinden erişilebilinir.

Çalıştay açılışını T.C. *Ulaştırma, Denizcilik ve Haberleşme Bakanı* Sn. Binali YILDIRIM, Bilgi Teknolojileri ve İletişim Kurumu Başkanı Sn. Dr.Tayfun ACARER, Bilgi Güvenliği Derneği Başkanı Doç. Dr. Mustafa ALKAN, Ankara Üniversitesi Hukuk Fakültesi Dekanı Sn. Prof. Dr. Hüseyin ALTAŞ ve Türkiye Barolar Birliği Başkan Yardımcısı Sn. V. Ahsen ÇOŞAR yapmıştır.

Siber Güvenlik Hukuku Çalıştay'ının birinci gününde Prof. Dr. Hüseyin ALTAŞ başkanlığında, **"Temel Sorunlar " ve "Çözüm Önerileri" başlıklı iki oturum düzenlenmiş, ikinci gününde ise bir günlük ücretsiz "Siber Güvenlik Eğitimi" verilmiştir. Bilgi Güvenliği Derneği üyeleri tarafından verilen eğitimde "Kişisel Verilerin Güvenliği ve Savunma Teknikleri", "Web Ortamlarında Siber Güvenlik ve Koruma" ve "Sosyal Ağlarda Siber Güvenlik ve Korunma Yöntemleri" gibi konular işlenmiş ve bu eğitimler sırasıyla Sn. Prof. Dr. Şeref SAĞIROĞLU, Sn. Burak ÇİFTER ve Sn. Yük. Müh. Uraz YAVANOĞLU tarafından verilmiştir.**

Siber Güvenlik Hukuku Çalıştay'ına toplam 340 kişi katılmış olup, 176 kişiye de "Siber Güvenlik Eğitimi" verilmiş ve katılımcılar sertifikalandırılmıştır.

Çalıştay sonucunda elde edilen çıktılar ve ülkemiz için yapılması gereken hususlar ile ilgili öneriler aşağıda balıklar halinde verilmiştir.

1. Günümüzde kişi, kurum ve kuruluşlara ait bilgi varlıklarının hacminin ve çeşitliliğinin geçmişe oranla ciddi artışlar gösterdiği. Artık bilgi varlıklarımızın çok büyük ölçüde sayısallaştığı ve bu durumunun gerek kamu gerekse özel iş süreçlerini kolaylaştırdığı. Geçmişte mümkün olmayan yeni servisleri mümkün hale getirdiği. Ancak bütün bunların yanı sıra hayatımızın birçok yönünü ve evresini kapsayan siber uzay altyapısının güvenliğinin sağlanması konusunun ciddi bir problem olduğunun taraflarca kabul edildiği ve gerekli eylemlerin ivedilikle hayata geçirilmesi gerektiği.

2. Başta Kamu olmak üzere tüm kurum ve kuruluşların birçok hizmetlerini internet ortamında sunmaya başlamasıyla birlikte bu ortamda yaşanacak olumsuzlukların kişisel, sosyal ve ekonomik hayatımızı önemli ölçüde etkilediği. Etkili tedbirler alınmadığı takdirde gelecekte yaşanabilecek olumsuzlukların daha da artacağı. Oluşabilecek siber güvenlik vakalarının hem maddi hem de manevi zararlar verebileceği. Bu tür zararlarının büyük ölçüde engellenebilmesi için ilgili tüm taraflara görevler düştüğü.

3. Ülkemizde bilişim ve internet ortamında işlenen suçlar ile ilgili mevcut mevzuat değerlendirildiğinde, 5237 sayılı "Türk Ceza Kanunu", 5651 sayılı "İnternet

Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun", 5070 sayılı "Elektronik İmza Kanunu" gibi kanunlar ve ilgili yönetmeliklerle siber güvenlik hukuku altyapısının desteklendiği fakat sadece bu düzenlemelerle günümüz ihtiyaçlarının tümüyle karşılanmasının mümkün olmadığı.

4. Siber güvenlik hukuku mevzuat çalışmalarında, hukukçu, teknik kişi, sosyolog-psikolog gibi sosyal bilimci vb. farklı disiplinlerinden oluşan mesleki uzmanların katkı vermesinin hukuki ve teknik altyapı uyumluluğunun sağlanması noktasında önem arz ettiği.

5. Bireyleri ve toplumu siber güvenlik vakalarının muhtemel olumsuzluklarından korumak için, mevzuat, standart, eğitim ve denetleme unsurlarının tümünü içerecek kapsamlı bir altyapının ilgili taraflarının katkı ve katılımıyla oluşturulması gerektiği.

6. Siber güvenliğin sağlanması ve vatandaşlarının her türlü veri ve bilgilerinin korunmasının yasal güvence altına alınabilmesi için hukuk bütünlüğü içinde ilgili yasa ve yönetmelikleri içeren mevzuatın siber alandaki günümüz ihtiyaçlarını kapsayacak biçimde hazırlanması gerektiği.

7. Siber varlıkların sınırlarının ve bu varlıklar arasındaki iletişimin ulusal sınırları aştığı. Siber ortamda saldırgan ve mağdurların çoğu durumda farklı ülkelerde yer alabildiği. dolayısıyla siber güvenlik alanında, uluslararası birlikte çalışılabilirlik mekanizmalarının ve sözleşmelerin önem kazandığı. Önümüzdeki günlerde uluslararası işbirliklerinin daha da arttırılmasına ihtiyaç olduğu.

8. Türkiye'nin Avrupa Konseyi Üyesi 47 ülke tarafından imzalanan "Siber Suçlar Sözleşmesini" imzaladığı ve yürürlüğe girmesi için T.B.M.M onayını beklediği. Bu sözleşmenin Meclis tarafından onaylanmasına müteakip iç hukuka uyarlanması gerektiği. Bu sözleşme kapsamınca özellikle vatandaşların kişisel verilerinin diğer ülkelerle paylaşımı hususundaki düzenlemelerin dikkatlice irdelenmesi gerektirdiği.

9. Yasalaşmayı bekleyen "Kişisel Verilerin Korunması Yasa Tasarısının" farklı görüşlerin, yaklaşım ve kaygılarını da dikkate alarak kapsamlı şekilde değerlendirmesi gerektiği, bu konudaki yasal boşluğun bir an önce giderilmesine ihtiyaç olduğu.

10. Kişisel verilerinin korunmasıyla ilgili yasal düzenlemelerde, vatandaşlarının gizli kalması gereken kişisel veri ve bilgisine erişimde, istisnai durumlar olarak tanımlanan ve tanımlanacak olan hususların açık kriterlere bağlanmasına ihtiyaç olduğu. Bu yasal düzenlemelerde ülkemizde vatandaşların en önemli kişisel verilerinden olan genetik ve DNA bilgilerin gizliliğinin sağlanması konularının göz önünde bulundurulması gerektiği.

11. Siber güvenlik ve kişisel verilerin korunması hususundaki yasal mevzuat çalışmalarında katılımcılık ve şeffaflık ilkelerinin gözetilmesi gerektiği ve bu düzenlemelerinin hem idarenin hem de halkın talep ve menfaatlerini azami ölçüde gözetmesinin beklendiği.

12. Kamu kurumları ile bankacılık, telekomünikasyon vb. hizmet sunucu özel kuruluşlarının kullandıkları bilişim altyapılarının, önceden belirlenmiş ve yasal düzenlemelerdeki ihtiyaçlara cevap veren standartlara sahip olması gerektiği. Bu bağlamda öncelikli olarak uluslararası güvenlik standartlarından da faydalanılarak ulusal siber altyapı güvenliği standartlarının belirlenmesine ve uygulanmasına ihtiyaç olduğu.

13. Mevzuatta tarifi yapılmayan ve/veya içtihada bağlanmayan siber suçlarının, adli süreçlerde sorumluluğunun belirlenmesi ve dağıtılması hususlarının zorlaştırdığı; mevcut Türk Ceza Kanununda tarifi yapılmayan suç ve taraf tanımlarının yapılarak bu konudaki eksikliklerin giderilmesinin adli süreçlerin hızlı ve sağlıklı ilerlemesi açısından önem arz ettiği.

14. Fikri ve Sınaî Haklar Yasasında, yazılımların eser olarak tanımlandığı ve aynı yasanın 16. Maddesinde yazılımlarının değiştirilmesi hakkının manevi haklar kapsamında değerlendirildiği ve bu durumun özellikle kullanılan yazılımlarının güvenlik amaçlı olarak değiştirilmesi önünde engellere sebebiyet verdiği. Bu problemin özellikle yabacı menşeli savunma sınaî yazılımları için çok ciddi bir problem olarak ortada durduğu ve çözüm beklediği.

15. Başta A.B.D ve batı Avrupa ülkeleri olmak üzere siber suçlarla mücadele için çok ciddi mali kaynaklarının ayrıldığı, siber güvenlik politika ve strateji belgeleri oluşturulduğu; Ülkemizde bu yönde eksiklikler olduğu ve bu eksikliklerin ivedilikle giderilmesine ihtiyaç olduğu.

16. Kamu kurum ve kuruluşlarının siber güvenlik alanında bilgi, beceri ve imkanları arasında ciddi farklılıklar olduğu; kurumlar arası bu alandaki bilgi ve tecrübelerinin paylaşılması ve giderilmesi gerektiği.

17. Başta bankalar olmak üzere, ticaret ve hizmet hayatının önemli kuruluşların, şeffaflığı sağlamak ve hizmet alıcıları bilgilendirmek için yaşanan bilgi güvenliği açıklarını hesap sahipleri ile veya kamuoyu ile paylaşmaları gerektiği.

18. Ülkemizde siber güvenlik hukuku konusunda daha fazla uzman yetiştirilmesine ihtiyaç olduğu ve bu konuda üniversitelerin ve kurumların gerekli eğitim, sertifikasyon ve tez çalışmaları yapılmasına imkan sağlamasının daha çok faydalar getireceği ve sürecin sağlılık olarak yönetilmesine büyük katkılar sağlayacağı.

19. Ülke ekonomisi, kamu refahı ve güvenliği için çok önem arz eden su, elektrik, gaz, telekomünikasyon ve finans gibi sektörlerin kullandığı bilişim ve otomasyon altyapılarının AB Ülkelerinde ve A.B.D'de "Kritik Altyapılar" olarak nitelendirildiği. Bu tür altyapıların sürekli ve güvenli hizmet verebilmesi için ulusal güvenlik, risk değerlendirme ve denetleme standartlarının belirlenmesine ihtiyaç olduğu. Kamu, özel ayrımı yapmadan ülke Kritik Altyapının korunması için hukuki ve teknik düzenlemelerin ayrıca ve ivedilikle ele alınması gerektiği; bu konuda yürütülecek bilimsel çalışmaların desteklenmesinin faydalar getireceği.

20. Ulusal siber güvenliğin en önemli hukuki altyapısını oluşturacak olan "Ulusal Siber Güvenlik Yasa Tasarısının" ivedilikle gündeme alınması ve yasalaştırılmasının son derece önemli olduğu.

21. Bütün bunların yanı sıra; Ulusal Bilgi Güvenliği konusunda politika belirlemek, strateji geliştirmek, Siber Güvenlik alanında her türlü koordinasyonu sağlamak, planlanma ve uygulamaları gerçekleştirmek, Siber savunma gücünü oluşturmak, Ulusal anlamda bütün kritik altyapı ve ülke varlıklarını savunmak, gerektiğinde müdahale etmek ve toplu saldırılar karşısında gerekli koordinasyonu sağlamak amacıyla BOME, C-SIRT gibi birimleri de içerisine alan bir "Siber Güvenlik Ulusal Koordinasyon Kurulunun" ivedilikle hayata geçirilmesi ve

22. Yapılan bu ve bundan önceki etkinliklerin ülkemizde siber güvenlik farkındalığının artmasına katkılar sağladığı gibi 17-19 Mayıs 2012'de yapılacak olan "V. Uluslararası Bilgi Güvenliği ve Kriptoloji" konferansının da (www.iscturkey.org) ana temasının "Siber Güvenlik" olarak seçilmesinin ülkemizde bu sürecin daha hızlı olarak gelişmesi ve yönetilmesine büyük katkılar sağlayacağı

değerlendirilmektedir.

Kamuoyuna saygıyla duyurulur.

Siber Güvenlik Hukuku Çalıştayı 2012 Düzenleme Kurulu