ISCTURKEY 2015 KONFERANSI SONUÇ BİLDİRGESİ

Bilgi güvenliği alanında, ulusal ve uluslararası boyutta bilimsel, teknik, sosyal ve kültürel çalışmalar yürüterek birey ve kurumlarda farkındalığın oluşması ve ortak akıl ile çözüm önerilerinin geliştirilmesi amacı ile 2007 yılında kurulan Bilgi Güvenliği Derneği (BGD) her yıl Uluslararası Bilgi Güvenliği ve Kriptoloji (ISCTurkey) Konferansı'nı düzenlemektedir. Bu konferansın 8.si, Gazi Üniversitesi, İstanbul Teknik Üniversitesi ve Ortadoğu Teknik Üniversitesi işbirliğiyle ve T.C. Ulaştırma, Denizcilik ve Haberleş Bakanlığı ve Bilişim Teknolojileri ve İletişim Kurumu destekleriyle 30-31 Ekim 2015 tarihlerinde ODTÜ Kültür ve Kongre Merkezi'nde gerçekleştirilmiştir.

Son yıllarda siber saldırıların doğrudan ülkelerin önemli altyapılarını hedef alması ve bu saldırıların çok ciddi ekonomik kayıplara ve manevi zararlara yol açmasının önemi değerlendirilerek ISC Turkey 2015 Konferansının bu seneki ana teması "Siber Güvenlik ve Kritik Altyapılar" olarak belirlenmiştir.

Konferansta ele alınan konular aşağıda sunulan 4 ana başlık altında toplanmıştır.

1. Mevzuat ve Organizasyonel Yapı

1.1. Bütüncül bir bakış açısıyla Türkiye'nin Siber Güvenlik mevzuatı ele alınmalı, kamu ve özel sektör kurumlarının eş güdümlü bir şekilde siber mücadeleyi yürütmesi için Siber Güvenlik Kurulu uhdesinde gerekli operasyonel yapı kurulmalıdır.

1.2. 2015-2017 Dönemini kapsayan "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı"nı, revize edilerek 2016-2018 dönemini kapsayacak şekilde düzenlenmeli ve 2015 yılı sonuna kadar da yayımlanmalıdır.

1.3. Kişisel verilen korunması kanun tasarısının en kısa sürede TBMM gündemine alınması için girişimlerde bulunulmalıdır.

1.4. Milli güvenliğin önemli bir parçası olan siber güvenlik konusunda zafiyet gösterilmemesi için nitelikli personel yetiştirilmesine ihtiyaç olduğu gerçeğinden hareketle "Siber Güvenlik Uzmanı" (aynı İş Güvenliği Uzmanı gibi) meslek grubu **kanun ile** oluşturulmalı, "Siber Güvenlik Uzmanı" için gerekli eğitimler ve sınav şartları Siber Güvenlik Kurulu tarafından belirlenmeli, kritik altyapı barındıran kurumlarda Siber Güvenlik Uzmanı istihdamı **yine kanunla** zorunlu hale getirilmelidir.

1.5. Siber Güvenlik Kurulu tarafından ülkemize ait kritik sektörler; Enerji, Elektronik Haberleşme, Finans, Ulaşım, Su Yönetimi ve Kritik Kamu Hizmetleri olarak belirlenmiştir. Kritik altyapılara sahip tüm kurumların bilgi güvenliği standartlarına uygun hizmet vermesi yönünde hem belgelendirme hem de denetim çalışmaları yapılmalıdır.

1.6. Siber saldırıların kritik altyapıları hedef almak suretiyle doğrudan ülkelerin milli güvenliğini tehdit ettiği gerçeğinden hareketle kritik altyapılar olarak belirlenen sektörlerin her biri için "Kritik Altyapıların Korunmasına Yönelik Politika ve Strateji" dokümanları hazırlanmalıdır.

1.7. Mevcut SOME yapısının Endüstriyel Kontrol Sistemi (EKS) kullanan kurumlar için doğru bir model olmadığı görüşü ifade edilerek EKS-SOME kurulması önerisi (https://ics-cert.us-cert.gov) getirilmiştir. Öneri ilgili kurumlara aktarılmalı ve tartışılmalıdır.

1.8. Siber güvenliğin her yönüyle ilgili bilimsel çalışmalar yapan ve raporlar üreten Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) benzeri bir ajans (Türkiye Ağ ve Bilgi Güvenliği Ajansı (TABGA)) kurulması değerlendirilmelidir. Ya da mevcut bir yapının (TÜBİTAK BİLGEM gibi) böyle bir ajansa dönüştürülmesi düşünülmelidir.

2. Yerli çözümler

2.1. Siber güvenlik alanında kullanılan donanım ve yazılımların başka güvenlik sorunlarına yol açıp açmadığı ciddi bir endişe olarak karşımıza çıkmaktadır. Bu endişenin bertaraf edilebilmesi için gerek donanım gerek yazılım alanında milli çözümler üretilmesinin şart olduğu düşünülmektedir. Bu düşünceden hareketle UDHB'nin ARGE fonu, milli çözümlerin geliştirilmesi yönünde hızlı çalışan bir modelle kullanılmalı, milli çözümlerin kullanılması teşvik edilmelidir.

2.2. Ülkemizde bilgi güvenliği alanında çalışan/çalışmak isteyen çok sayıda kişi ve kurumların olduğu görülmüştür. Bu girişimlerin desteklenmesi ve etkinliğinin arttırılabilmesi için tüm bu çalışmaların "Siber Güvenlik Ekosistemi" içerisinde bütüncül bir bakış açısıyla ele alınması gereklidir. Bunun için BGD'nin yürüttüğü envanter çalışması önemli bir zemin olarak görülmektedir.

2.3. Yerli ve güvenilir teknoloji kullanımı için açık kaynak modelinin büyük bir fırsat olduğu düşünülmektedir. Bir "Açık Kaynak Ekosistemi" oluşturulabilmesi için kamu alımları başta olmak üzere BT kaynaklarının bu alana yönlendirilmesi gerekmektedir. Aksi halde gerçek anlamda bir açık kaynak ekosistemi oluşamayacak ve markalı ithal ürünleri satmaya ve kullandırmaya yönelik sektör dinamiği aynen devam edecektir. Bu noktada her zaman en iyisini değil, ama asgari ihtiyacı gören, iyileştirilebilir, yerli ve güvenilir olanın da tercih edilebileceği, bu tercihi yapanların riske girmeyeceği, bir modelin üzerinde çalışılması bununla birlikte istismarın engellenmesi içinde gereken standartların aynı zamanda çalışılması sağlanmalıdır.

2.4. Bilgi Güvenliği konusunda geliştirilen ürünlerin kapsamlı olarak test edilebilmesi için "Bilgi Güvenliği Veri ve Test Merkezi" kurulmalıdır.

2.5. Havelsan A.Ş. Genel Müdürü Konferansta yaptığı konuşmada; yerli ve milli çözümleri olan tüm girişimcilerle birlikte çalışabileceklerini belirtmiş ve açık bir davette bulunmuştur. Siber güvenlik alanında çalışan/çalışmak isteyenler bu daveti değerlendirmelidir.

3. Kapasitenin arttırılması ve farkındalık

3.1. İlköğretimden itibaren bilgi güvenliği konusu müfredata dahil edilmeli, her yıl farklı seviyelerde konunun ele alınması ve gündemde kalması sağlanmalıdır. Böylece hayatımızın nerdeyse tamamının üzerine inşa edildiği bilgi dünyasında siber güvenliğin farkında olan nesiller yetiştirilmelidir.

3.2. Açık Bilgilendirme Platformları, farkındalık sağlayan projeler ve araştırmalar gibi sosyal projeler de UDHB AR-GE fonu kapsamında desteklenmelidir.

3.3. Sürdürülebilir bir siber mücadele için toplumun tüm kesimlerinin siber güvenlik farkındalığını arttıracak başta kamu spotu olmak üzere farklı halkla ilişkiler yöntemleri kullanılmalıdır.

3.4. ENISA tarafından her yılın EKİM ayının "Avrupa Siber Güvenlik Ayı (ECSM)" olarak belirlenmesi ve yoğun etkinlik takvimiyle siber güvenliğin her yönünün ele alınmasına zemin hazırladığı düşünülmektedir. Avrupa'da olduğu gibi ülkemizde de EKİM ayının "Türkiye Siber Güvenlik Ayı (TUSGA)" olarak ilan edilmesi ve TUSGA Platformunun Siber Güvenlik Kurulu hamiliğinde, ülke çapında etkinlikler düzenlenmesine destek olarak siber güvenliğin her yerde ve mecrada gündeme getirilmesini sağlamalıdır.

3.5. Gerek tüketiciler gerekse de kurumlar hem kişisel hem de işleri ile ilgili bilgileri yabancı menşeli ürünler (google, facebook, msn, whatsapp, twitter, ofis uygulamaları, smallpdf,

wetransfer, storage hizmetleri vb.) kullanarak depolamakta, aktarmakta ya da çevrim içi hizmetler almaktadır. Kritik altyapılara ilişkin bilgiler de çoğu zaman aynı uygulamaları kullanarak işlem görmektedir. Bu durum çok ciddi bir güvenlik tehdidi oluşturmaktadır. Tüketicilerin bilinçlendirilmesi ile birlikte daha önemlisi tüketiciye bu hizmetleri alabileceği yerli çözümler sunulması gerekmektedir. Bu konuda ilgili kamu kurumlarının inisiyatif alması gerektiği düşünülmektedir.

3.6. USOM, Sektörel ve Kurumsal SOME'lerin faaliyetleri her yıl sonunda USOM tarafından raporlanmalıdır.

4. Uluslararası İşbirliği

4.1. Siber güvenlik alanının en temel unsurlarından biri olan uluslararası işbirliğinin arttırılması yönünde ENISA ve benzeri organizasyonlarla ilişkilerimiz, muhtelif seviyelerde sağlanmalı ve sürekli kılınmalıdır.

4.2. Uluslararası kuruluşlarda, STK'larda ve muhtelif platformlarda çok ciddi çalışmalar yapılmakta ve çıktılar üretilmektedir. Bu çıktıların kullanılmasının yanı sıra üretiminde de yer alınması çok önemlidir. Kamu ve özel sektör kuruluşları bu kurumlarla ilişkili olmalı, BGD başta olmak üzere benzeri STK'lar da uygun buldukları uluslararası kuruluşlarla irtibata geçerek yapılan çalışmalara müdahil olmalıdır.

Kamuoyuna saygıyla duyurulur. 07.11.2015

ISCTurkey 2015 Konferansı Yürütme Kurulu