ISCTurkey 2018

SONUÇ BİLDİRGESİ

Bilgi güvenliği ve siber güvenlik alanında, ulusal ve uluslararası boyutta bilimsel, teknik, sosyal ve kültürel çalışmalar yürüterek kişisel, kurumsal ve ulusal 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 düzenlemektedir. Bu konferansın onbirincisi, Gazi Üniversitesi, İstanbul Teknik Üniversitesi ve Ortadoğu Teknik Üniversitesi işbirliğiyle ve T.C. Ulaştırma ve Altyapı Bakanlığı ile Bilgi Teknolojileri ve İletişim Kurumu'nun destekleriyle 17-18 Ekim 2018 tarihlerinde BTK Konferans Merkezinde gerçekleştirilmiştir.

Uluslararası ISCTurkey Konferansı, düzenlendiği ilk yıldan beri Türkiye'nin bilgi güvenliği alanındaki bilimsel ve sektörel çalışmalarının paylaşıldığı, üniversite-kamu-endüstri işbirliğinin geliştirildiği, kamuoyunun bilgilendirildiği, konuya ilgi duyanların eğitildiği, ulusal ve uluslararası bilim insanları, araştırmacılar ve sektörel uygulayıcılar arasında bilgi alışverişinin sağlandığı, ülkemizin bu alandaki en önemli etkinliğidir. Bu etkinlik ile bilgi güvenliği alanında, toplumun her kesiminin farkındalığının arttırıldığı, politika koyucu ve karar vericilerin çalışmaları gözden geçirdiği, üniversite-kurum-sektör arasında işbirliği imkânlarının oluşturulması veya artırılması ve en önemlisi ülkemizin bu alandaki

akademik bilgi birikimini artırmayı hedeflenmiştir. ISCTurkey 2018 Konferansı, Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) tarafından da desteklenmekte ve Avrupa Birliği'nin her yılın Ekim ayı olarak belirlediği "Avrupa Siber Güvenlik Ayı" etkinlikleri kapsamında yer almaktadır.

Kripto paraların yaygınlaşması, uygulama ve teknolojilerin güvenliğinin sağlanmasına yönelik olarak yeni çözümlerin geliştirilmesine duyulan ihtiyaç göz önüne alındığında, araştırmacıların son yıllarda blokzinciri teknolojileri ve uygulamalarına önem verdiği, yeni çözümler geliştirmeye çalıştıkları, gerek sistemleri gerekse süreç ve uygulamaları daha güvenli hala getirmeye çalıştıkları görülmektedir. ISCTurkey 2018 konferansının bu yılki ana teması "Siber Güvenlik ve Blokzinciri Teknolojisi" olarak belirlenmiştir. Milli güvenliğin önemli bir parçası olan siber güvenlik konusunda zafiyet gösterilmemesi için hem nitelikli siber güvenlik uzmanları yetiştirilmesi hem de gerek donanım gerek yazılım alanında milli ve yerli çözümler üretilmesinin şart olduğu düşüncesinden hareketle ISCTurkey 2018 Konferans Programı oluşturulmuştur.

ISCTurkey 2018 konferansına; bu yıl 934 kişi elektronik kayıt yaptırmış ve konferansa 640 kişi katılmıştır. Konferans programında; 4 panel, 3 akademik oturum, 2 davetli konuşmacı, 1 eğitim programı ile 3 firma ve ürün tanıtım oturumu gerçekleştirilmiştir. 30'a yakın firma konferansımızda ürün tanıtıcı standlar açmışlardır.

Konferans açılış konuşmalarını; Bilgi Güvenliği Derneği Başkanı Sn. Ahmet Hamdi ATALAY, BTK Başkanı Sn. Ömer Abdullah KARAGÖZOĞLU ve UAB Bakan Yardımcısı Sn. Dr. Ömer Fatih SAYAN yapmışlardır.

Konferansımıza konuşmacı olarak davet edilen ve "Blokzincir Teknolojisi ve

Yaygınlaşması ile Önündeki Problemler" konusunda bir konuşma yapan Sn. Prof. Dr. Ali Aydın SELÇUK (TOBB ETU Siber Güvenlik ABD Başkanı); dünya literatüründe yapılan çalışmaları özetlemiş, düşüncelerinizi literatür ışığında katılımcılarla paylaşmış, dünyada blokzincir teknolojilerinin önemli adımlarını ve karşılaşılabilecek riskleri aktarmış ve sonuçta bu teknolojileri bazı alanlarda uygulamanın çok yerinde olacağı ama bazı alanlarda yapılan uygulamaların mevcut çözümlere göre üstünlüğü olmayacağını bildirmiştir.

Konferansta düzenlenen 4 panele; üniversitelerden, sektörden, kurumlardan ve ilgili bakanlıklardan panelistler katılmışlar, konuşmalar yapmışlar, görüşlerini kamuoyu ile paylaşmışlardır. Bu paneller hakkında kısa bilgiler aşağıda verilmiştir.

- Panel Başkanlığını İTÜ Bilişim Enstitüsü Müdürü ve Konferans Eş Başkanı Sn. **Prof. Dr. Ertuğrul KARAÇUHA**'nın yaptığı "**Siber Güvenlik ve Blokzincir Teknolojisi**" oturumuna Sn. **Dr. Öğretim Üyesi Pelin ANGIN** (ODTÜ Bilgisayar Mühendisliği Bölümü), Sn. **Gökhan SEÇKİN** (Kimlic Blockchain Yazılım Teknoloji Genel Müdürü), Sn. **S. Bilgehan ÜSTÜNDAĞ** (CHOMAR Antivirüs CEO), Sn. **İlker İMAMOĞLU** (FORTİNET Türkiye Teknik Müdürü), Sn. **Fatma Hacıoğlu DOĞAR** (NETAŞ Siber Güvenlik Servisleri Direktörü) katkı vermişlerdir. Bu oturumda;
  - ülkemizde blokzinciri teknolojileri konusunda belirsizlikler olsa da özellikle büyük çaplı uygulamalarda bu teknolojiye dayanan çözümler geliştirmenin yerinde olacağı,

- bu tür teknolojilerin kullanılabileceği ve hatta geliştirilmiş uygulamaların bulunduğu bu alana ilgi göstermek ve daha fazla akademik çalışma yapmanın, uygulama geliştirmenin ve bunları paylaşmanın yerinde olacağı ve
- bu alanın gelişmesi için elektronik imza mevzuatının güncellenmesi, Avrupa EIDAS ile uyumlu hale getirilmeleri, ve son olarak ta "bulut imza yasasını" çıkarmalarının yerinde olacağı belirtilmiştir.

- Panel Başkanlığını Konferans Eş Başkanı Sn. **Prof. Dr. Mustafa ALKAN**'ın yaptığı "Ulusal Güvenlik Açısından Siber Güvenlik" oturumuna Sn. **Ömer KORKUT** (STM Genel Müdür Yardımcısı), Sn. **Mahmut KÜÇÜK** (Siber Güvenlik Direktörü), Sn. **Mehmet Ali ORTAYATIRTMACI (**TÜRKSAT Kurumsal Bilgi ve Siber Güvenlik Yönetimi Direktörü), Sn. **Haydar Erdem YILMAZ** (VODAFONE Bilgi Teknolojileri Operasyon Direktörü), Sn. **M. Feridun AKTAŞ** (TURKCELL Teknoloji Yönetişimi ve Güvenlik Direktörü) katkı vermişlerdir. Bu oturumda; ülkemizde siber güvenlik alanında yapılan çalışmalar kapsamlı olarak değerlendirilmiş, ülke güvenliğine yönelik olarak tehditler ve fırsatlar üzerinde durulmuş, yerli ve milli üretime daha fazla destek olunması gerektiği vurgulanmıştır.

- Panel Başkanlığını SSB Siber Güvenlik ve Bilişim Sistemleri Grup Başkanı Sn. **Mustafa ÖZÇELİK**'in yaptığı **"Siber Güvenlik Sanayi ve Kümelenmesi"** oturumuna Sn. **Doç. Dr. İzzet Gökhan ÖZBİLGİN** (HAVELSAN Ar-Ge, Teknoloji ve Ürün Yönetimi Direktörü), Sn. **Burak KIRIMER** (TÜRKTRUST Ar-Ge Merkezi Müdürü), Sn. **Murat TORA** (Atar Labs Kurucu Ortağı), **Serdar YOKUŞ** (BİZNET

Bilişim Genel Müdürü), **Prof. Dr. Şeref SAĞIROĞLU** (Gazi Üniversitesi, MF Bilgisayar Mühendisliği Bölüm Başkanı) katılmışlardır. Bu oturumda;

- dünya siber kümelenme çalışmaları ile ülkemizdeki siber kümelenme çalışmaları özetlenmiş, bundan sonra yapılacak olan çalışmaların neler olması gerektiği üzerine görüş ve öneriler sunulmuş, SSB Siber Kümelenme çalışmasının ülke siber güvenliğine katkısının çok kısa sürede anlaşılması için sektör-üniversite-kurum birlikteliğinin çok önemli olduğu ve bunun güçlendirilmesi çalışmalarına devam edilmesi gerektiği,
- Yerli ve milli ürün çalışmalarına odaklanılması ve özellikle müşteri olarak kamunun sektörü cesaretlendirmesi ve ürün alımında önceliğe almasının yerinde olacağı,
- Nitelikli insan kaynağının çok önemli olduğu ve geliştirilmesine yönelik daha radikal kararlar alınması gerektiği,
- Ülkemizde bilgi birikimi düşük veya zayıf olan alanlarda bilgi birikimi ve yeteneklerin geliştirilmesi için ulusal ve uluslararası işbirliklerinin artırılması gerektiği,
- HAVELSAN'ın ürettiği "yerli siber güvenlik çözümlerini ilgilenen üniversitelere açma" niyetinde olması, siber güvenlik girişimcilerini destekleme kararı, üniversite laboratuvarlarını güçlendirme çabası, gibi hedeflerin ülke siber güvenliğinin daha hızlı gelişmesine büyük katkı sağlayabileceği, buna benzer örneklerin sayısının artırılmasına katkı sağlayacağı ve
- bu kümelenme kapsamında başarı örneklerinin ve hikayelerinin kamuoyu ile paylaşılmasının faydalı olacağı gibi hususlara bu toplantıda yer verilmiştir.

- Panel Başkanlığını Konferans Eş Başkanı **Prof. Dr. Şeref SAĞIROĞLU'nun** yaptığı **"Siber Güvenlikte Eğitim ve İnsan Kaynağı Yetiştirme Politikaları"** oturumuna Sn. **Prof. Dr. Türksel KAYA BENSGHIR** (Ankara Hacı Bayram Veli Üniversitesi Öğretim Üyesi), **Doç. Dr. Sedat AKLEYLEK** (19 Mayıs Üniversitesi BMB Öğretim Üyesi, ISCTurkey Program Komitesi Başkanı), Sn. **Prof. Dr. Ferruh ÖZBUDAK** (ODTÜ UME Kriptografi ABD Başkanı, ISCTurkey Eş Başkanı), Sn. **Ali Kemal YURTSEVEN** (HAVELSAN Siber Güvenlik Grup Müdürü), Sn. **Zafer POLAT** (ARISTA Networks Ülke Müdürü) katkı vermişlerdir. Bu oturumda;
  - Prof. Dr. Ferruh ÖZBUDAK; Ortadoğu Teknik Üniversitesinde yapılan çalışmaları, ülkemize yapılan katkıları ve bundan sonraki süreçte odaklandıkları konular aktarmışlardır. Bundan sonraki süreçte katkılarının artması için ülkemizde ortak çalışmalar yapılmasını, ticari ve askeri uygulamalarda kullanılan algoritmaların mutlaka test edilmesi ve bundan sonraki süreçte Kuantum Kriptografik konularına ağırlık verilip yeni algoritmaların geliştirilmesi gerektiğini iletmiştir.
  - Prof. Dr. Şeref SAĞIROĞLU; nitelikli insan kaynağının ancak ve ancak nitelikli öğretim üyeleri, programlar, ders içerikleri, iyi altyapı ve laboratuvarlar ile yüksek bilgi birikimi ve araştırma kabiliyeti ile geliştirilebileceğini belirtmiştir. Ayrıca, Kalkınma Bakanlığının altyapı kurulmasına yönelik olarak teşvik desteği vermesi, TÜBİTAK'ın özel çağrılar açması, MEB ve YÖK'ün yurt dışına öğretim elemanı yetiştirilmesine yönelik öğrenci göndermesi, YÖK 100/2000 Burs Programı, Araştırma Üniversiteleri belirleme ve destekleme, Aselsan Akademi Lisansüstü Programı, kümelenme çalışmaları (siber güvenlik, 5G, vb.) bunları destekleyen burs programlarının nitelikli insan gücü yetiştirmek için iyi

örnekler ve önemli adımlar olduğunu bildirmiş, buna benzer desteklerin artırılarak devam ettirilmesinin önemini vurgulamıştır.

- Prof. Dr. Türksel KAYA BENSGHIR, her ne yapılırsa yapılsın iyi bir planlamanın ancak ve ancak strateji ve politikalar ile belirlenmesi gerektiğini, ülkemizde açılan programların, içeriklerin, çıktıların ise bu kapsamda değerlendirilmesi gerektiğini belirtmiştir.
- Doç. Dr. Sedat AKLEYLEK; YÖK Siber Güvenlik Çalışma Grubunun yaptığı çalışmaları özetlemiş; siber güvenlik alanında eğitim, öğretim ve araştırma yapan üniversite ve laboratuvarların altyapı, cihaz ve insan kaynaklarını daha verimli kullanabilmesi için "açık laboratuvar" ve "akademik siber güvenlik kümelenmesi" kavramları ve bunların etkin olarak işleyebilmesi ve sürdürülebilmesi için gerekebilecek teknik, idari ve mali düzenlemeler hakkında yapılan çalışmaları detaylı olarak aktarmış; "kamu kaynaklarına erişim kolaylığı" ve "bilgi paylaştıkça çoğalır" olduğunu vurgulamış; "T.C. Cumhurbaşkanlığı Bütçe ve Strateji Başkanlığı" 2018 yılı araştırma altyapıları çağrısında öncelikli alan olarak yer alan siber güvenlik için birçok üniversitenin başvuruda bulunduğu ve açık laboratuvar fikrine uygun olarak tüm paydaşların yeterli ölçüde faydalanabildiği/kullanabildiği, uzaktan erişim imkanına sahip, gerektiğinde fiziksel erişime açılabilen bir yapının gerekliliğini ifade etmiş; eğitim ve araştırma için destekleyici/yardımcı materyallerin geliştirilmesi ve bunların aktif kullanım için çalışma grubunun yaptıklarını sunmuş; siber güvenlik alanında nitelikli insan gücü yetiştirmek için yapılan çalışmalar hakkında hem üniversiteler hem de siber güvenlik kümelenmesi ve Yükseköğretim Kurumları Siber Güvenlik Genelgesinin neleri içermesi

konusunda yapılan çalışmalar hakkında bilgi vermiş, siber güvenlik lisansüstü program içeriklerinin ulusal ve uluslararası hedeflere uygun olarak oluşturulabilmesi için yapılan çalışmaları belirtmiş; siber güvenlik ve kriptoloji alanında ürün geliştirme sürecinde güvenilir ve kaliteli yazılım geliştirme ve test süreçlerinin öneminden ve bu kapsamda Yazılım Sektörü Stratejisi ve Eylem Planında yapılanları açıklamış; "Siber Güvenlik ve Kriptoloji Köyü" fikrinin üniversite-kamu-sanayi üçlüsünün buluşması ve hep birlikte eğitim, bilgi paylaşımı, ürün geliştirme adına kullanılabilecek bir Ar-Ge platformu olabileceğini ifade etmiştir.

- Siber güvenlik ekosisteminin oluşturulması için sektör, üniversite ve kamunun ortak çalışmalar yapması, sektör dinamiklerinin iyi anlaşılması, nitelikli öğrenci yetiştirilmesine önem verilmesi, ortak projeler üretilmesine önem verilmesi, bitirme projelerinde güvenlik çalışmalarına ağırlık verilmesi, girişimci gençlere ihtiyaç duyulduğu, üniversitelerde siber güvenlik bilincinin artırılmasına yönelik çalışmalar yapılması gibi hususlara da önem verilmesi gerektiği, diğer panelistler tarafından önerilmiştir.

Her yıl olduğu gibi bu yıl da konferansta düzenlenen eğitimlere yoğun ilgi olmuştur. Eğitimlere, 312 kişi kayıt yaptırmış olup 219 kişi ise eğitimlere katılmış ve katılım sertifikası almıştır. HAVELSAN'ın sponsorluğunda yapılan eğitimlerde aşağıdaki konulara yer verilmiştir;

- **Dr. Emre YÜCE** ve **Duygu ÖZDEN** "Blokzincir Teknolojileri"
- **Artur MEHMET** ve **Ali Orhun AKKIRMAN** "Pardus İşletim Sistemi ve Kamuda Kullanımı"

Bu yıl yapılan konferansta, **SİBER GÜVENLİK ÜSTÜN HİZMET ÖDÜLÜ TÖRENİ** ilk kez yapılmıştır. Bu ödülün amacı; ülkemizde bilgi güvenliği ve siber güvenlik alanının gelişimine katkı veren kişilere ve kurumlara şükranlarımızı sunmak, bundan sonrada bu alana hizmet verenleri takdir etmek ve gençleri özendirmektir. Bundan sonraki etkinliklerde bu ödüller verilmeye devam edilecektir. Ödüller, kurum, sektör ve üniversite olmak üzere üç kategoride verilmiştir. Bu yıl verilen ödüller, ödül alan kişi ve gerekçeleri aşağıda verilmiştir.

- **Prof. Dr. Ersan AKYILDIZ, Emekli Öğretim Üyesi (ODTÜ)**

  Ülkemizde kriptoloji biliminin geliştirilmesine verdiği katkılar, bilimsel kongre düzenlemesine verdiği hizmetler, yaptığı yayınlar, ODTÜ Kriptografik Test Laboratuvarının Kurulması ile ülkemizde kriptografik algoritmaların güvenlik testlerinin yapılmasını sağlaması ve STK'lara gerek başkan ve gerekse üye olarak verdiği katkılardan dolayı bu ödüle layık görülmüştür.
- **Dr. Ömer Fatih SAYAN (UAB, Bakan Yardımcısı)**

  BTK Başkanı olduğu süre içerisinde USOM'un kurulması, BTK'nın konferans salonlarının üniversitelere ve sektöre açılması, gençlerin siber güvenliğe ilgisinin artmasına yönelik yapılan yarışmalar, ulusal ve uluslararası düzenlenen etkinliklere verdiği çok önemli desteklerden dolayı bu ödüle layık görülmüştür.
- **TÜRKTRUST**

  Ülkemizde, yerli ve milli ürün geliştirilmesine yönelik olarak TSK Güçlendirme Vakfı bünyesinde kurulan ve ülkemizde e-imza teknolojilerini yerli ve milli olarak üretip bu alanda Elektronik Sertifika Hizmet Sağlayıcısı olarak verdiği hizmetlerden, bilgi güvenliği alanında yaptığı projelerden, kamuya, sektöre ve üniversitelere verdiği destekten dolayı bu ödüle layık görülmüştür.

- **BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU**

  Ülkemizde bilgi güvenliği ve siber güvenlik alanlarında yapılan düzenlemeler, yönergeler, yönetmeliklere ilave olarak; sektörün gelişmesi için sektörü BTK içerisine alan ve onlara ofisler veren, ürün tanıtım alanları sunan, konferans salonlarını sektöre açan, üniversiteler ile yakın çalışan, destekleyen, siber güvenliğin yayılması ve yaygınlaştırılmasına verdiği desteklerden ve en önemlisi bunu sürekli ve tüm paydaşlarla beraber yapan kurum olmasından dolayı layık görülmüştür.

Konferansın 2. günü akşamında ise "**BGD Ulusal Siber Güvenlik Bilim Kurulu**" gündemde olan konular ile ilgili olarak bir toplantı yapılmıştır. Ülkemizde ve dünyada karşılaşılan siber riskler, bilgi ve siber güvenlik alanında yapılan çalışmalar, karşılaşılan problemler masaya yatırılmış, gelecekte karşılaşılabilecek olumsuzluklar ve olası önlemler üzerinde değerlendirmeler yapılmış, yeni nesil problemlerin çözümüne yönelik ortak öneriler geliştirilmiştir. Gelecek yıl yapılacak olan konferansa yönelik olarak görüş alışverişinde bulunulmuştur.

ISCTurkey 2018 konferansında ele alınan konular 5 ana başlık altında gruplandırılarak değerlendirilmiş ve öneriler başlıklar altında sunulmuştur.

1. MEVZUAT VE ORGANİZASYONEL YAPI

1.1. Dağınık olan siber güvenlik mevzuatı, bütüncül bir bakış açısıyla ve tüm paydaşların katılımıyla ele alınmalı ve müstakil bir "Siber Güvenlik Kanunu" çıkartılmalıdır.

1.2. "Siber Güvenlik Uzmanlığı" mesleğinin gerekleri "Siber Güvenlik Kanunu" ile oluşturulmalı ve kritik altyapı barındıran kurumlar ile SOME'lerde Siber Güvenlik Uzmanı istihdamı yine kanunla zorunlu hale getirilmelidir.

1.3. UAB HGM'ye bağlı olan Siber Güvenlik Dairesinin sorumluluğunda olan Siber Güvenlik Stratejisinin takibi daha etkin yapılmalıdır. 2016-2019 "Ulusal Siber Güvenlik Stratejisi ve Eylem Planının" etkin olarak uygulanıp uygulanmadığını kamuoyu adına takip için bir "Kamuoyu İzleme Komisyonu" kurulmalıdır. BGD, bunu koordine etmek veya komisyon üyesi olmak için gönüllüdür.

1.4. BGD'nin Kişisel Verileri Koruma konusunda her etkinliğinde gündem yaptığı, tartıştığı ve önerilerde bulunduğu 6698 sayılı Kişisel Verilen Korunması Kanunu yürürlüğe girmiştir. Bu ülkemiz için çok önemli bir adımdır. Kurumun çalışmaya başlaması, kişisel verileri koruma konusunda etkin çalışmalar yürütmeye başlaması sevindiricidir. Bu kurumumuzun, özellikle gelecekte büyük tehlike oluşturacağı değerlendirilen sosyal medya hizmetlerinin, kişisel verilerin ihlal edilmesi kadar ulusal mahremiyeti (vatandaşlarının mahremiyetini) ihlal edebilecek seviyede tehdit edecek ihlaller oluşturabileceği dikkate alınarak çalışmalar yapılmalı ve kamuoyu ile paylaşılmalıdır. Ayrıca; üniversitelerin araştırma yapmasında çok önemli olan veriler bu Kanun bahane gösterilerek üniversiteler ile paylaşılmamakta ve üniversitelerde de nitelikli ve ülkeye katkı sağlayacak araştırmalar yapılamamaktadır. Kanunda bu durum için istisna olsa da bu konunun önemi dikkate alınarak, ilgili kurumun Kamuoyu açıklaması yapması yerinde olacaktır.

1.5. Ülkemizde bilgi güvenliği ve siber güvenlik alanlarında karşılaşılan tehditler, açıklıklar, tehlikeler, saldırılar vb. istatistiklerin dış kaynaklardan, ticari kuruluşların web sitelerinden veya her yıl yayımladıkları raporlardan öğrenilmektedir. Bu

istatistiklere göre çözümler geliştirilmeye çalışılmaktadır. Ülkemiz siber güvenlik istatistiklerinin ulusal olarak yayımlanması, ülkemize karşı yapılan saldırıların, oluşan tehdit ve tehlikelerin doğru anlaşılması ve gerçekçi analiz ve çözümler geliştirilmesini sağlayacaktır.

1.6. Ülkemizin 2012 yılında AB çerçevesinde imzaladığı ve 2013'de Başbakanlık Genelgesi olarak Kamu Kurumlarına bildirdiği "Açık Veri Politikaları" kapsamında; ülkemizde siber güvenlik alanında nitelikli araştırmalar yapılabilmesi için kurumlar bünyesinde veya belirlenen bir kurum bünyesinde, açık veri veya araştırma verileri veri tabanları oluşturulmalı ve bu veriler üniversitelerin kullanımına açılmalı, veri setleri üzerinde kapsamlı ve nitelikli çalışmalar yapılması ve ülkeye değer kazandırılmasının önü açılmalıdır. Amerika, Almanya, Japonya, İngiltere, Kanada, Fransa gibi pek çok ülke ulusal kazanımları arttırmak ve araştırma faaliyetlerini desteklemek için verilerini gerektiğinde anonimleştirip yayımlamaktadır. "data.gov", "opendata.gov", "opendata.gov.de" ve "opendata.uk" buna örnek olarak verilebilir. Bu gibi hizmetlerin ülkemizde kullanıma açılması ve üniversitelere sunulmasıyla; ülkemizde karşılaşılan problemlere gerçekçi çözümler geliştirilebileceği, kayıpların azaltılabileceği, yeni ve farklı çözümlerin geliştirilmesi, çözümlerinin iyileştirilmesi, kalitesinin artırılmasına daha fazla katkı sağlanabilecektir.

1.7. İhtiyaç duyulan uzman açığını kapatmaya yönelik olarak **2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı** kapsamında bazı öneriler yapıldığı, hedefler belirlendiği, bu hedeflerin gerçekleştirildiği belirtilse de bu alanda hala yeteri kadar nitelikli personelin bulunmadığı, mevcutlarının da yurtdışına gitme eğiliminde olduğu hatta bazılarının yurt dışına gittiği (bugün için Almanya'da 200 ve İngiltere'de 80'in üzerinde güvenlik uzmanı bulunmaktadır.), yabancı ülkelerin ise güvenlik

uzmanlarını ülkelerine çekebilmek için uzmanlara cazip tekliflerde bulunduğu, şirket açmalarına izin verdikleri, vatandaşlık sağladıkları bilinmektedir. Buna yönelik olarak; mutlaka yeni çözümler geliştirilmeli, yurtdışından yabancı uzmanların ülkemize gelmesi için yeni adımlara ihtiyaç olduğu, ülkemizde de konu cazip hale getirilmelidir.

2. TEKNİK ALTYAPI VE YERLİ ÇÖZÜMLER

2.1. Ülkemizde bilgi güvenliği alanında çalışan/çalışmak isteyen çok sayıda kişi ve kurumun olduğu görülmüştür. Bu girişimlerin desteklenmesi ve etkinliğinin arttırılabilmesi için tüm bu çalışmaların "Siber Güvenlik Ekosistemi" içerisinde bütüncül bir bakış açısıyla ele alınması ve paydaşların yer alması gereklidir. SSB'nın oluşturduğu Siber Güvenlik Kümelenmesi, son yıllarda yapılan ve gerek sektörü gerekse üniversiteleri yakınen ilgilendiren ve memnuniyet uyandıran siber güvenlik kümelenmesi çalışmaları çok yerindedir. Bu kümelenmede, 3 yıl içerisinde ülkemiz için kritik olan 10 yerli ürünün geliştirilmesinin teşvik edilmesi gibi hedeflerin belirlenmesi ve bu hedeflerin yerine getirilmesi yerinde olacaktır.

2.2. Siber güvenliğin sağlanması için nitelikli çalışmaların yapılması ve insan kaynağı yetiştirilmesi için ülkemize büyük görevler düşmektedir. Ülkemiz üniversiteleri, dünya güvenlik bilimine yaklaşık 1/1000 oranında katkı sağlamaktadır. Ülkemizde bu alana katkı sağlayan ABD programlarının, bu oranları dikkate alarak bu alana daha çok katkı sağlamanın yollarını aramalı, mevcut programların buna önem vermeleri, laboratuvarlarını güçlendirmeleri, yetenek ve kabiliyetlerini geliştirerek yetkinliklerini artırmaları, ülkenin ihtiyaç duyduğu alanlara odaklanmaları, yeni

politika, strateji, ürün, algoritma, teori, uygulama ve çözümler geliştirmeye çalışmalıdırlar.

2.3. Yerli ve güvenilir teknoloji kullanımı için açık kaynak modelinin büyük bir fırsat olduğu düşünülmektedir. Bir "açık kaynak ekosistemi" oluşturulmalı ve yaygınlaştırılmalıdır. 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 çalışılmadır. Ulusal stratejide belirtildiği gibi PARDUS işletim sistemine gereken önemi vermeleri, Açık Ofis yazılımlarına geçiş yapmaları, PostgreSQL açık kaynak veritabanını tercih etmeleri, vb. bunlara verilebilecek güzel örneklerdir.

2.4. Bilgi güvenliği konusunda geliştirilen çalışmaların, uygulamaların, ürünlerin, çözümlerin, teknolojilerin, prototiplerin veya girişimlerin kapsamlı olarak test edilebilmesi için "Ulusal Siber Güvenlik ve Test Merkezi" kurulmalıdır.

2.5. Üniversitelerde bilgi güvenliği ve siber güvenlik alanında çalışma yapan bölüm ve programların etkinliğinin arttırılması ve yeteneklerin geliştirilmesi için ortak ar-ge laboratuvarları kurulmalı ve ortak kullanıma açılmalıdır.

3. KAPASİTENİN ARTTIRILMASI VE FARKINDALIK

3.1. Ülkemizde, farkındalık seviyesinin her geçen gün arttığı görülmektedir. Farkındalığı farklı seviyelerde (öğrenci, veli, çalışan, yönetici, üst yönetici, kritik personel, vb.) değerlendirilerek çalışmalara devam edilmesi gereklidir. Farkındalık çalışmaları konunun alışkanlık haline getirilmesine kadar sürdürülmeli veya bunun için önlemler alınmalıdır.

3.2. Nitelikli insan yetiştirmeye yönelik olarak, ülkemizde bu alanda eğitim veren üniversite programlarının sayısı arttırılmalı, mevcutların içerikleri ise gözden geçirilmeli, programlarda bilgi güvenliği alanında farklı alt alanlara uzmanlaşmaya önem verilmeli, ihtiyaç duyulan alanlarda yeni öğretim elemanlarının bu programlara kazandırılması için üniversitelere kadro desteği arttırılmalıdır. YÖK'ün 100/2000 Doktora Burs Programının ülkede iyi bilinmediği, programlara yüksek müracaat olmadığı görülmüştür. Ülkemizin 100 kritik alanında doktoralı eleman yetiştirmeye odaklanan bu çok önemli programın çok iyi bir şekilde duyurulması, bu programa üniversitelerin, araştırma merkezlerinin, enstitülerin sahip çıkmaları gereklidir.

3.3. AB ve ABD'de olduğu gibi ülkemizde de belirlenen bir ayın "Siber Güvenlik Farkındalığını İzleme ve Değerlendirme Ayı" olarak belirlenmesi faydalı olacaktır.

3.5. Kriptografik algoritmaların, uygulamalarda test yapılmadan kullanıldığı ve bunların da büyük tehdit oluşturacak güvenlik zaafiyetine sebebiyet verdiği belirlenmiştir. Bu tür algoritmaların test edilmeden kullanılmaması ve test etmek için test birimleri veya merkezlerin kurulması, mevcutlarının da desteklenmesi gerekmektedir.

3.6. Sadece siber güvenlik ve bilgi güvenliği konuları değil, bu alanı destekleyecek yeni konularda da (veri bilimi, büyük veri analitiği, nesnelerin interneti, yazılım tanımlı ağlar, kriptografik testler, post-quantum kriptografi, yapay zeka, derin öğrenme, kriptoanaliz, bulut ve sis güvenliği, Endüstri 4.0, adli ve karşı adli bilişim gibi) milli ve yerli teknolojik çözümlerin geliştirilmesi, son dönemde artmış olsa da (KOSGEB, TÜBİTAK, vb.) daha çok teşvik edilmelidir.

3.7. Etkinlik sırasında; üst düzey yöneticilerin gençleri siber güvenlik alanında çalışmaları konusunda cesaretlendirdiği, onlara iş garanti vermeleri çok önemli bir adımdır. Bu gibi açıklamaların sayısının artması, zeki ve yetenekli gençlerin bu alana çekilmesi,

yeteneklerinin geliştirilmesi ve desteklenmesini önemsiyoruz. Yöneticilerimizi bu gibi açıklamaları daha çok yapmaya davet ediyoruz.

3.9. ITU Global "Siber Güvenlik Endeksi" sıralamasında, ülkemizin olgunluk seviyesi yüksek ülkelerden birisi (43. sırada) olduğu raporlanmıştır. Bu sıralama, dünya geneline göre iyi olsa da bunun iyileştirilmesi için; araştırma yetenekleri artırılmalı, laboratuvar ve altyapılar iyileştirilmeli ve sayıları artırılmalı, programlar çeşitlendirilmeli ve kalitesi arttırılmalı, sektör ve kurum deneyim ve yeteneklerinden faydalanılmalıdır.

3.10. Siber güvenlik okuryazarlığı arttırılmalıdır. Sürdürülebilir yapılar kurulabilmesi için toplumun tüm kesimlerinin farklı seviyelerde farkındalığı artırılmalıdır.

3.11. Kişisel Verilerin Korunması Kanununun yayımlanması çok önemlidir. Panelistlerin açıklamalarından ve sunulan istatistiklerden, ülkemizde veri mahremiyeti üzerine yapılan çalışmaların az olduğu ve veri mahremiyeti farkındalığının düşük olduğu görülmüştür. Bunun arttırılmasına yönelikte çözümler geliştirilmelidir. Ayrıca, kamuda veri mahremiyetine her zamankinden daha fazla dikkat edilmesi, konuya gerekli önemin verilmesi gereklidir.

3.12. Kamu çalışanlarının devlet işlerini yürütürken, yaparken veya yerine getirirken ücretsiz elektronik posta (e-posta), ücretsiz depolama alan hizmetlerini kullandıkları ve bunun sayısının da hiç az olmadığı görülmektedir. Kamu bilgi varlıklarının korunması ve mahremiyetinin sağlanması için ilgili kurumların bünyelerinde sürdürülebilir kurumsal altyapılar kurulmalı ve işletilmelidir. Bazı üniversitelerimizin uluslararası e-posta hizmetlerini bünyelerinde kullandıkları, ücretsiz olarak verilen bu hizmetlerden faydalandıkları bilinmektedir. Bu üniversitelerimizin, konuya

gereken önemi vermeleri, 6698 Kişisel Verileri Koruma Kanunu gereği bunun bir zorunluluk olduğu unutulmamalıdır.

4. ULUSLARARASI İŞBİRLİĞİ

4.1. Siber güvenlik ve savunma konusu, uluslararası bir konudur. Bu konuda işbirliklerinin arttırılması, ortak faaliyetler düzenlenmesi, tehdit ve tehlikelere karşı topyekün mücadele edilebilmesi için elde edilen uluslararası deneyimlerden mutlaka faydalanılmalıdır.

4.2. Uluslararası yapılan çalışmalara bakıldığında; kurumların, kuruluşların, STK'ların, organizasyonların, enstitülerin, üniversitelerin çok ciddi çalışmalar yaptıkları, bunları yayımladıkları, önemli ve güncel çıktılar ürettikleri ve bunları kamuoyu ile paylaştıkları ve güncel hayatta kullanılabilir hale getirdikleri ve en önemlisi ticarileştirdikleri görülmektedir. Ülkemizde bu konularda çalışanların, dünyada olduğu gibi benzer konularda ciddi çalışmalar yapmaları, çalışmalarını ticarileştirmeleri, ülke siber güvenlik ekonomisi oluşturulmasına katkılar sağlamaları gerekmektedir. Alınan kararlarda bu hususlara özellikle ağırlık verilmelidir.

4.3. Yerli fikirlerin geliştirilmesi, üretilmesi, teknolojilerin tasarlanması, test edilmesi ve hayata geçirilmesi için açık kaynak proje geliştirme ortamlarının veya platformlarının sayısı arttırılmalı, uluslararası açık kaynaklardan faydalanıldığı kadar bu ortamların gelişimine de katkı sağlayacak yapılan oluşturulmalıdır.

5. DİĞER KONULAR

5.1. Siber güvenlik alanında yapılan çalışmaları desteklemek, bu alanda açık arşiv oluşturmak çok önemlidir. BGD, her konferansta olduğu gibi bu konferansta da

üretilen tüm dokümanları kamuoyu ile paylaşmaktadır. Bu dokümanlar (sunumlar, bildiriler kitabı, fotoğraflar, videolar, vb.) konferans resmi web sitesi www.iscturkey.org adresinden yayımlanmaktadır.

5.2. Ülkemizin siber güvenlik alanında en büyük açık kaynak arşivini oluşturma çalışmaları başlamıştır. Bunun için ilk olarak, siber güvenliğin boyutunu iyi ifade etmek, tehlikeyi veya fırsatları iyi görmek için yaklaşık 80 farklı konuyu içeren SİBER GÜVENLİK VE SAVUNMA KİTABI SERİSİ çalışmalarına başlanmıştır. Bu kitap serisinin ilki tamamlanmak üzeredir. Bu kitap çalışması, bir ay içerisinde kamuoyu ile ücretsiz olarak paylaşılacaktır.

Kamuoyuna saygıyla duyurulur.

ISCTurkey 2018 Düzenleme Kurulu