VI. ULUSLARARASI BİLGİ GÜVENLİĞİ VE KRİPTOLOJİ KONFERANSI (ISCTURKEY 2013)

SONUÇ BİLDİRGESİ

ISCTurkey 2013 Düzenleme Kurulu

21/09/2013

Bilgi Güvenliği Derneği tarafından Gazi Üniversitesi, Orta Doğu Teknik Üniversitesi, Bilgi Teknolojileri ve İletişim Kurumu işbirliği ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığı himayelerinde bu yıl altıncısı düzenlenen ISCTurkey 2013 etkinliği, 20-21 Eylül 2013 tarihleri arasında Ankara'da ODTÜ Kültür ve Kongre Merkezinde yapılmıştır. Kongre ile ilgili tüm bilgiler www.iscturkey.org adresinden erişilebilinir.

Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı düzenlendiği ilk yıldan beri Türkiye'nin bu alanlardaki bilimsel ve sektörel çalışmaların paylaşıldığı,üniversite-kamu-endüstri işbirliğinin geliştirildiği, kamunun bilgilendirildiği, eğitildiği, ulusal ve uluslararası tüm bilim insanları,araştırmacılar ve sektörel uygulayıcılar arasında bilgi alışverişinin sağlandığı, ülkemizdeki bu alandaki en önemli etkinlik olup bilgi güvenliği ve kriptoloji kavramlarının, toplumun bireyleri tarafından özümsenmesine yardımcı olmak, ülkemizde bu alanda bilimsel bilgi birikiminin arttırılmasına katkılar sağlamak, kurumlar ve sektör arasındaki işbirliğini arttırmak ve en önemlisi bunu uluslararası boyutta yaparak katılımcıların kazanım ve katkıları arttırmayı ve uluslararası işbirliğini arttırmayı hedeflemiştir.

Bilgi güvenliği ve kriptoloji alanlarında farkındalığı oluşturmak, ulusal ve uluslararası işbirliğini arttırmak ve siber tehdide yönelik riskler ve çözüm önerilerini geliştirmek amacıyla gerçekleştirilen bu etkinliğe 700'e yakın kişi kayıt yaptırmış olup, kamu, üniversite, özel sektörden ulusal ve uluslararası düzeyde 500'ün üzerinde ilgili kişiler katılmıştır. Konferansın bildiriler kitabında yayınlanması için akademisyenler ve uygulayıcılar tarafından eşbaşkanlara iletilen bildiriler, alanında uzman en az iki hakem tarafından değerlendirilmiştir. Hakem değerlendirilmesi sonucunda uygun bulunan bildiriler sözlü veya poster sunumu için seçilerek bildiriler kitabında basılmıştır. Toplam 108 bildiri başvurusundan 39 adedi oral (sözlü) sunum ve 26 adedi ise poster sunumu için kabul edilmiştir. Sözlü sunum için seçilen bildiriler konferansta iki gün içersinde sekiz ayrı salonda; poster sunumları ise, katılımcıların görebileceği fuaye'de yazarlar tarafından sunulmuştur. Kabul edilen bildiriler ve posterler, bulut bilişim güvenliği, siber güvenlik ve savunma stratejileri, yazılım güvenliği, steganografi, kriptografi, kriptoanaliz, protokol güvenliği, bilgi güvenliğini sağlama yöntemleri, saldırı tespit yöntemleri, saldırı tespit sistemleri, kaotik şifreleme ile akıllı kartlarda kullanılan kriptografik protokoller ve bunların uygulamalarına yönelik çalışmaları kapsamaktadır. Bu yıl yurt dışından gönderilen bildirilerin

çoğunluğu, bildirilerde karşılaşılan alıntı oranlarının yüksek olması ve alıntılara atıf yapılmadığı için kabul edilmemiştir.

Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı'nın hedefleri doğrultusunda, bu sene ana teması "Bulut Bilişim Güvenliği" olarak belirlenen etkinliğin, ülkelerin askeri, ekonomik, teknolojik ve kritik altyapılarına karşı son zamanlarda büyük artış gösteren siber saldırılara karşı koyabilecek ve/veya engel olabilecek çözüm önerileri diğer konularla beraber özellikle konferans çerçevesinde konunun uzmanları tarafından değerlendirilmiştir.

Bu yıl altıncısı yapılan bu uluslararası konferansın açılışını Bilgi Güvenliği Derneği II. Başkanı Prof. Dr. Mustafa ALKAN, ODTÜ Rektörü Prof. Dr. Ahmet ACAR ve Ulaştırma, Denizcilik ve Haberleşme Bakanı Sn. Binali YILDIRIM yapmıştır.

Bilgi Güvenliği Derneği II. Başkanı Prof. Dr. Mustafa Alkan, "uluslararası savaşların artık siber ortamda gerçekleştiğine dikkat çekerek, Türkiye'nin Dünyada siber saldırıya uğrayan ülkeler sıralamasında ilk sıralarda yer aldığına dikkat çekerek binlerce bilgisayarın köleleştirilip kontrol altına alındığını ve gerek ülke gerekse kişisel bilgilerin tehdit unsuru olarak karşımıza çıktığını, kişisel ve kurumsal bilgi güvenliği konusunda bilinç oluşturulması, yaşayan bir sistem olarak bilgi güvenliği olgusunun hayata geçirilmesi ve siber dünyada her türlü tedbiri almamız ve her türlü tehdit ve tehlikeye karşı hazır olmamız gerektiğini, ifade etmiştir.

Bilgi Güvenliği Derneği olarak ülkemizde bu alanın gelişmesi ve geliştirilmesi için 2006 yılından beri çalıştıklarını, Dernek olarak belirledikleri yol haritası ve çalışma planından bahseden alkan, bundan 6 yıl kadar önce Temel olarak 3 başlıkta hedeflerini belirlediklerini. Bunlardan birincisinin toplumun tüm kesimlerinde Bilgi Güvenliği konusunda farkındalık oluşturmak. İkincisinin Türkiye için strateji belgesi ve eylem planını hayata geçirmek üçüncüsünün de kurumsal ve yasal altyapıların tamamlanmasını sağlamak olduğunu, bu gün itibariyle bu hedeflerine büyük ölçüde erişildiğini ifade etmiştir. Bunlardan Siber Güvenlik Strateji Belgesi Taslağı'nın hazırlanarak UDH Bakanımız Sn. Binali Yıldırım'a dernek olarak sunduklarını belirterek, bunun sonucunda Bakanlıkça bu çalışmanın tamamlanarak yürürlüğe konulduğundan duyduğu mutluluğu ifade etmiştir. İkincisi Siber Güvenlik

Koordinasyon Kurulunun kurulmuş olmasının ülke için öneminden bahsederek bundan sonra da bu tür katkıları vermeye devam edeceklerini belirtmişlerdir.

Son olarak ta, konferansımıza başından beri destek veren UDH Bakanımız Sn. Binali YILDIRIM'a, BTK Başkanı Sn. Tayfun ACARER'e ve şimdiye kadar tüm Konferanslarımıza ev sahipliği yapan ODTÜ Rektörü Prof. Dr. Ahmet ACAR'a her zaman verdikleri destekten dolayı teşekkür etmiştir. Ayrıca etkinlik sponsorları TÜRKCELL, VODAFONE, AVEA, ASELSAN, HAVELSAN, STM ve NETAŞ'a ve katkı veren tüm kişi ve kurumlara teşekkür etmiş, konferansın ülkemize katkılar sağlamasını dileyerek konuşmasını bitirmiştir.

ODTÜ Rektörü Prof. Dr. Ahmet ACAR açılış konuşmasında, Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı düzenlendiği ilk yıldan beri ODTÜ olarak ülkemiz için çok önemli olan bu etkinliklerde yer almak ve her yıl ev sahipliği yapmaktan büyük bir memnuniyet duyduklarını, ODTÜ Uygulamalı Matematik Enstitüsü bünyesindeki Kriptografi Bölümü'nün kriptoloji alanında edindiği deneyim ve bilgi birikiminin ülkemizin bilgi toplumu olma yolundaki çabalarına önemli bir katkıda bulunduğunu, Uygulamalı Matematik Enstitüsü bünyesindeki Kriptoloji Laboratuvarı'nda gerçekleştirilen projeler ile ülkemizin bilgi güvenliği ve kriptoloji alanındaki ihtiyacını karşılayabilecek kapasitede olduğunu, E-devlet uygulamalarında kullanılan kriptografik algoritma ve modüllerin tasarımını, testlerini ve çeşitli platformlarda uygulamalarını yapabilmenin yanında, ülkemizde son yıllarda iyice artan elektronik imzaların ve akıllı kartlar ve özellikle e-kimlik üzerindeki uygulamalarının yazılımsal ve donanımsal güvenilirliğini test edebilme ve elektronik tebligat (Kayıtlı Elektronik Posta) sistemlerinde kullanılan kriptografik protokol geliştirme ve test edebilme kabiliyetine sahip olduğu belirtmiştir. Son olarak, UDH Bakanlığı'na, Gazi Üniversitesi'ne ve BTK'ya işbirlikleri ile emeği geçenlere ve konferansa katkı sağlayan sponsorlara teşekkür etmiştir.

Konferansımıza her zaman olduğu gibi destek veren ve bu yılkı açılışta da bizleri katılımlarıyla onurlandıran UDH Bakanımız Sn. Binali YILDIRIM ise video konferans ile katıldığı konferansımızda yaptığı açılış konuşmasında, UDH Bakanlığı olarak ülkemizde bilgi güvenliği konusuna çok önem verdikleri, ülke strateji belgesini

yayımladıklarını ve eylem planını hayata geçirdiklerini bu konuda çalışmalara hız kesmeden devam ettiklerini belirtmişlerdir.

UDH Bakanımız Sn. Binali YILDIRIM konuşmalarında; 2002 yılında genişbant abone sayısı 20 binin altında iken bugün 20,5 milyon genişbant abonesi olduğunu, mobil abone sayısının 68,02 Milyona, 3G Mobil abone sayısı 45,3 milyona, cep telefonu konuşma süresinde ve SMS kullanımında Avrupa'nın birincisi olduğumuzu, bilişim sektörü cirosu bugün 45 milyar dolarla dayandığını, günlük hayatta yaptığımız pek çok işlemin sanal dünyada da artık yapılır hale geldiği, hürriyet, demokrasi, hukuk ve adalet gibi kavramların yalan dünyada olduğu gibi sanal dünyada da geçerli olduğunun farkında olunması gerektiğinin bilinmesi, bu alanı kullananların dikkatli olması ve kimsenin bu alanı sorumsuzca kullanmaması gerektiğini, ülkemizde sanal dünya ve sosyal medya ile ilgili bir takım yasal düzenlemeler yapıldığını ve yenilerini de yapmaya devam edeceklerini belirtmiştir.

Sosyal medyanın özgürlük alanına kimsenin müdahale etmesinin, kullanımına karşı çıkmasının ve engellemesinin doğru bir şey olmadığını ama ne gerçek hayatta ne de sanal dünyada insanları mağdur edecek faaliyetlerden kaçınılması gerektiğini vurgulamışlardır. Sosyal paylaşım alanını da, interneti de temiz kullanmak için bir kampanya başlatılması gerektiğini, öncülüğünüde sivil toplum örgütleri, eğitim kurumları, üniversitelerin yapmaları gerektiğini, gelişen bu mecranın etik değerlerini de toplumsal düzeyde yazılı olmayan bir anlayışa göre oluşturması gerektiğini de konuşmalarında belirtmişlerdir.

Sanal alemin diğer bir önemli sorununun da kuşkusuz güvenlik olduğunu, artık tüm resmi işlemlerimiz dahil olmak üzere bankacılık işlemlerimize kadar her şeyi internet üzerinden gerçekleştirdiğimizi, devletlerin uluslararası ilişkilerinden iç güvenlik politikalarına kadar bütün iş ve işlemler bilgisayarlar üzerinden hazırlandığını, siber güvenlik de bu nedenlerden dolayı hayati öneme sahip olduğunu, ABD siber güvenlik için yıllık 15 Milyar dolar civarında bir harcama yaptığını, UDH Bakanlığının bu alanda bir takım çalışmaları yürütüğünü, siber güvenlik kurulu kurulduğunu, koordinasyon ve sekreterya görevini de UDH Bakanlığını yürüttüğünü, siber güvenlik kurulu toplantıları yaptıklarını, bir yol haritası belirlendiğini, bu doğrultuda çalışmaları sürdürdüklerini belirtmiştir.

Avrupa Konseyi Siber Suçlar Sözleşmesine taraf olunduğunu, 48 ülke buna taraf, yani 48 ülkeyle adli yardımlaşma anlaşması yapıldığını, 7 gün 24 saat her ülke bu işlerle birbiriyle muhatap olup ona göre tedbirler alınacağını, Kamunun güvenliğine çok önem verdikleri ve karşılaşılan tehditleri azaltmak için ülkemizde kamu kurum ve kuruluşlarının güvenliğinin sağlanması için "Güvenli Kamu Ağı" kuracaklarını belirtmiştir.

Son olarak ta; bugüne kadar ülkemizde bilgi güvenliği alanında farkındalığın arttırılmasına ve bu konuda gerek bilimsel gerekse sektörün gelişime büyük katkılar sağlayan Bilgi Güvenliği Derneği, ODTÜ ve Gazi Üniversitesine bu etkinliği sürekli ve başarılı bir şekilde yaptıklarından dolayı teşekkür etmiş, bu etkinliği destekleyen kuruluşlara teşekkür etmiş ve başarılı bir konferans geçmesini dileyerek konuşmasını sonlandırmıştır.

Konferans süresince ana tema “Bulut Bilişim Güvenliği” konusu çerçevesinde sözlü sunumların yanında panellere davetli konuşmalara, eğitimlere ve sektör sunumlarına yer verilmiştir.

- Panel başkanlığını Prof. Dr. Şeref SAĞIROĞLU’nun yaptığı TÜRKİYE'NİN SİBER GÜVENLİK STRATEJİ BELGESİ VE EYLEM PLANI paneline, Dr. Hayretdin BAHŞİ (TÜBİTAK BİLGEM Siber Güvenlik Enstitü Müdürü), Gündüz ŞENGÜL (UDHB Daire Başkanı), K. Sacid SARIKAYA (BTK Daire Başkanı), Ali YAZICI (ASELSAN Bilgi Güvenliği Müdürü, BGD YK Üyesi) konuşmacı olarak katılmışlardır. Panelde 2012-2014 Strateji Eylem Planı tartışılmıştır. Siber güvenlik strateji belgesine sahip ülkelerin gelişmiş ülkeler olduğu ve ülkemizin için böyle bir strateji belgesinin ve eylem planının bulunmasının önemi üzerinde durulmuştur. Bu strateji belgesine ve eylem planlarına sahip ülkeler değerlendirildiğinde, eylem planlarının sürekli geliştirildiği, mevcut eylem planlarının uygulanmasında karşılaşılan güçlükler ile gelişen ve değişen teknolojiler ve altyapılar, yapılan saldırılar ile saldırı araçlarındaki hızlı değişim sebebinin bunda çok etkili olduğu görülmüştür. Ülkemizdeki mevcut strateji belgesinin de doğal olarak güncellenmesi gerektiği ve bu güncellemede aşağıdaki hususların dikkate alınarak revize edilmesinin yerinde olacağı değerlendirilmektedir. Bunlar;

- Siber Güvenlik Strateji Belgesinin ve Eylem Planının hayata geçirilmesinin ülkemiz için çok yerinde bir adım olduğu,
- Mevcut eylem planlarının başarıyla hayata geçirilmeye çalışıldığı,
- Dünya eylem planları incelendiğinde her eylem planının belirli araklıklarla güncellendiği ve günün şartlarına göre revize edildiği,
- Mevcut ülke eylem planı değerlendirildiğinde, bu planın siber tehditler dikkate alınarak hazırlandığı, yeni eylem planın da tehditlerin yanında fırsatlara da yer verilmesi gerektiği,
- ülkemizde bu alanın sağlıklı olarak gelişmesi için kurum-üniversite-sektörün işbirliği yapması ve bunun sürdürülür olabilmesi için ekosistem modellerinin geliştirilmesi hususlarına ağırlık verilmesi,
- Yeni planda uluslararası işbirliğine daha çok ağırlık verilmesi gerektiği,
- Kritik kurumların bilgi güvenliği standartlarına özellikle ISO 27001 ve ISO 27032 standartlarına uygun yapılar oluşturması konusunda yaptırımlar uygulanmasının gerekli olduğu,
- Siber güvenliğin ve savunmanın sağlanması için proaktif bir yaklaşımın belirlenmesi ve
- Yeni hazırlanacak belgede Sivil Toplum Kuruluşları ile Sektör Temsilcilerinin de kurullarda yer almaları

uygun olacaktır.

- Panel başkanlığını Prof. Dr. Turhan MENTEŞ (TBD)'nun yaptığı BULUT BİLİŞİM GÜVENLİĞİ PANELİ paneline, Ş. Selçuk ŞAHİN (TÜRKSAT), Bünyamin KARADENİZ (HAVELSAN), Cenk TAŞTAN (TURKCELL Bilgi Güvenliği Müdürü), Ömer KÖKER (VODAFONE), Cem AKOYMAK (AVEA), Necmi ÖN (NETAŞ) tan katılmışlardır. Panelde yapılan sunumlardan, ülkemizde sektörün bulut bilişim alanında hizmet veren yapıları kurguladığı, bu konuya gerekli hassasiyeti gösterdikleri fakat sektörün gelişmesi ve ortamın daha güvenli ve verimli hale getirecek projelerin hayata geçirilmesinin gerekli olduğu belirlenmiştir.

- Panel başkanlığını Prof. Dr. Nazife BAYKAL (ODTÜ Enformatik Enstitüsü Müdürü)'nun yaptığı SOSYAL MEDYA konulu 3. panele, Osman Nihat ŞEN (BTK TİB Başkan V.), Serhat ÖZEREN (UDHB Internet Gel. Kur. Başkanı), Burak ÇİFTER (Bilgi Güvenliği Derneği) ve Doç. Dr. Ferah ONAT (Yaşar Üniversitesi)

konuşmacı olarak katılmışlardır. Panel de konuşmacılar, sosyal medyanın ülkemizde yoğun şekilde kullanıldığı, 40 Milyona yaklaşan kullanıcı sayısının gelecek yıllarda daha da artacağı, bu ortamları kullananların bilgi güvenliği farkındalığının düşük olduğu, etik kullanım konusunda bilinç seviyesinin düşük olduğu, her şeyi devletten beklememek gerektiği bu ortamları kullanan kişilerin de sorumluluklarının farkında olarak, bu ortamları kullanmaları gerektiği, bu ortamları bilinçsiz, dikkatsiz ve etik kurallara uymadan kullanmanın olumsuzluklarla karşılaşılabileceğinin farkında olunması gereklidir. Gençlerimizin bu alandaki farkındalığını arttırmak için eğitimlere ağırlık verilmesi gerektiği, her alanda olduğu gibi bu alanda da etik kurallara uyulması gerektiği, bu alanda karşılaşılabilecek tehdit ve tehlikelerin farkında olunması gerekmektedir. Elektronik ortamda uygun, etik ve doğruluğundan emin olunmayan paylaşımların yapılmaması gerektiği, bunun yapılması durumunda da hukuki süreçlerle karşılaşılabileceğinin farkında olunması gereklidir. Elektronik ortamların manipülasyonlara açık olduğu, emin olunmayan veya güvenilmeyen kişilerle iletişime geçilmemesi ve paylaşımlar yapılmamasının önemli hususlar olduğu değerlendirilmektedir. Sosyal ortamları bilinçli kullanımın ailede başlaması gerektiği, okullarda da bu eğitimin geliştirilmesi gerekmektedir.

- Koordinatörlüğünü Bilgi Güvenliği Uzmanı Uraz YAVANOĞLU'nun yaptığı SİBER GÜVENLİK VE SAVUNMA EĞİTİMİ SERTİFİKA PROGRAMINA 450 kişi kayıt yaptırmış ve 350'nin üzerinde katılımcı kapsamlı bir eğitim almışlardır. Bu eğitim programında eğitimciler Siber Güvenlik ve Savunma, Bilgi Güvenliği ve Kriptoloji Uygulamaları, Bilgi Güvenliği, Güvenli Yazılım Geliştirme, Casus ve Kötücül Yazılım, Adli Bilişim, Sosyal Ağlarda Adli Takip, Bulut ve Web Güvenliği, Mobil Güvenlik, Endüstriyel Güvenlik ve Kurumsal Bilgi Güvenliği Standartları konularına ağırlık verilmiştir. Bir önceki yılda 176 katılımcıya “Siber Güvenlik Eğitimi” verildiği ve katılımcıların sertifikalandırıldığı göz önüne alındığında bu yıl katılımcı sayısındaki artış sevindiricidir.

- Sektör temsilcilerimiz STM "Savunma Sanayinde Proje Geliştirme Ortamlarında Tek Noktadan Farklı Güvenlik Seviyeli Etki Alanlarına Güvenli Erişim" ve Türk Telekom "Bulut" ve "DDoS Atak Önleme ve Türk Telekom Kurumsal Güvenlik Hizmetleri" konularında bilgilendirme sunumları yapmışlardır.

Bunun yanında konferansta konuşulan diğer hususlar aşağıda belirtilmiştir.

1. Ülkemizde bilgi güvenliği farkındalığının artmaya devam ettiği, kurumlarında farkındalığı arttırmaya devam ettikleri olumlu olarak değerlendirilmekte ise de kamu bilgi işlem çalışanları ile kritik altyapılarda çalışan tüm personelin bilgi güvenliği sertifikası olmadan çalışmamalarının artık bir gereklilik olduğu değerlendirilmektedir.
2. Bulut bilişim konusunda kurumlardaki çalışmaların arttırılması, bu konudaki soru işaretlerinin giderilmesi için bilgilendirme ve eğitim faaliyetlerinin arttırılması, yeni teknolojilerin yakından takip edilmesi, anlaşılması ve uygulanması faydalı olacaktır.
3. Bulut bilişim teknolojilerinin ülkemizde hayata geçirilmeye başlandığı, bu konuda hizmet verilmeye başlandığı ama bu ortamlara olan güvensizliğin hala devam ettiği kurumların bu konuda daha dikkatli olmaları gereklidir.
4. Konferansa sunulan bildirilerden ve sunumu yapılan akademik çalışmalardan görüldüğü kadarıyla ise ülkemizde bulut bilişim güvenliği konusunda bilimsel çalışmaların beklenen düzeyde olmadığı, bu alanda akademik çalışmalara ağırlık verilmesinin kaçınılmaz olduğu, gelecekte tüm sistemlerin buluta taşınacağı öngörüldüğünden bu alanda üniversite ile sektör arasında daha çok ortak çalışmalar yapılmalıdır.
5. Siber güvenlik stratejisi eylem planı kapsamında kurumların gerekenleri yaptıkları, bunun kurum kuruluşlara yol gösterici olduğu ve ülke bilgi güvenliğinin sağlanmasına büyük katkılar sağladığı görülmektedir. Bu süreç kararlılıkla sürdürülmelidirler.
6. Ülkemizde kurumsal bilgi güvenliği farkındalığının arttığı fakat bunun daha da geliştirilmesi gereklidir. Sertifikasyona ve belgelendirmeye ağırlık verilmelidir.
7. Yazılım geliştirilirken mevcut olan metotlardan birinin seçilmesi ya da kurumun yapısına, iş akış mantığına, kurum içi dinamiklere uygun olarak kuruma özgü bir metodun geliştirilmesinin gerekli olduğu fakat mevcut durumda kurumlarda işlerin tamamlanmasında çoğunlukla iş odaklı olunmadığı ve bu olmadığı sürece de yüksek seviyede bir güvenlikten bahsedilemeyeceği, kurumlara ve ülkeye özgün milli çözümler geliştirilmelidir.

8. Yazılım geliştirme sürecinde yazılım grubu, test ve analiz gruplarının birbirinden ayrı tutulması, geliştirilen yazılımın aktifleştirilmeden önce kod gözden geçirme yaklaşımıyla kontrol edilmesinin güvenli kodlama bakış açısıyla mevcut yazılımları gözden geçirilmesi ve alınacak veya geliştirilecek yazılımlarında bu bakış açısıyla alınmalı veya geliştirilmelidir.
9. Kurumlarımızda; kod geliştirme, test ve analiz işlemleri için farklı gruplar arasında hiyerarşik bir iş birliğinin oluşturulması ve uygulamaların aktifleştirilmesi için bütün aşamaların onaylanması, bu aşamaların yüksek seviyede yazılım güvenliği için önemlidir. Bu eksikliklerin giderilmesi faydalı olacaktır.
10. Uygulama geliştiriciler ve kullanıcılar dışında yöneticilerin de yeni teknolojileri takip etme, bunların takip edilmesini destekleme, yazılım geliştirme güvenliğinin önemini kavrayarak konuya hassasiyet göstermeleri, eğitim ile farkındalığın arttırılması faaliyetlerine önem vermelidirler. .
11. Ülkemizde yazılım güvenliği konusunda ar-ge çalışmalarına daha çok önem verilmesi gereklidir.
12. Ülkemizde siber saldırı ve savunma amaçlı yazılımların geliştirilmesine önem verilmesi, kaynak ayrılması ve uzman personel desteğinin sağlanması faydalı olacaktır. Kritik sistemlere yönelik yazılımların test edilmesi ve geliştirilmesi için ortak standartların oluşturulması çalışmalarına önem verilmelidir.
13. Siber güvenlik ve yazılım güvenliği konusunda akademik çalışmaların desteklenmesi, üniversitelerdeki eğitim programlarının ve müfredatlarının iyileştirilmesi, siber güvenlik ve bilgi güvenliği kapsamlı eğitim kampları, uygulama laboratuvarları gibi çalışmaların yaygınlaştırılması faydalı olacaktır.
14. Kurumların kendi yapılarını ve kritiklik seviyelerini dikkate alarak, kendilerine özgü siber güvenlik politikalarının geliştirmeleri gerekmektedir.
15. Bireyleri ve toplumu siber güvenlik saldırılarının muhtemel olumsuzluklarından korumak için, mevzuat, standart, eğitim ve denetleme unsurlarının tümünü içerecek kapsamlı bir altyapının ilgili taraflarının katkı ve katılımıyla oluşturulması gereklidir.
16. 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 gereklidir.

17. Kişisel verilerin güvenliği kanun tasarısı tekrar gözden geçirilerek bir an önce kanunlaştırılmalıdır.

Bu konferansta elde edilen tüm çıktılar (sunumlar, bildiriler kitabı, eğitim materyalleri, videolar) toparlanarak her konferans sonunda olduğu gibi ücretsiz olarak kamuoyu ile paylaşılmakta olup konferans hakkında detaylı bilgiler ile sunulan bildiriler, verilen eğitimler ile yapılan bilimsel sunumlarına www.iscturkey.org adresinden erişilebilinir.

Kamuoyuna saygıyla duyurulur.

Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı 2013 Düzenleme Kurulu