SİBER GÜVENLİK ÇALIŞTAYI 2011

Bilgi Güvenliği Derneği tarafından Gazi Üniversitesi, Orta Doğu Teknik Üniversitesi, Bilgi Teknolojileri ve İletişim Kurumu işbirliği ile bu yıl ikincisi düzenlenen ve Ana Sponsorluğunu ASELSAN'ın yaptığı **II. Ulusal Siber Güvenlik Çalıştayı** 29 Eylül 2011 tarihinde Ankara'da Türkiye Noterler Birliği Konferans Salonunda düzenlenmiştir.

Siber alanda bilgi güvenliği farkındalığı oluşturmak ve siber tehdide yönelik riskler ve çözüm önerilerini geliştirmek amacıyla gerçekleştirilen Siber Güvenlik Çalıştayı'na kamu, üniversite, özel sektörden 600'ün üzerinde ilgili kişiler katılmıştır. Çalıştay hakkında detaylı bilgiler ile çalıştayda sunulan bildiriler ve davetli konuşmacıların sunumlarına www.iscturkey.org/calistay adresinden erişilebilinir.
Çalıştay açılışını Bilgi Güvenliği Derneği Başkanı Doç. Dr. Mustafa ALKAN ve Bilgi Teknolojileri ve İletişim Kurumu Başkanı Dr. Tayfun ACARER yapmıştır.

BTK Başkanı Acarer, "Türkiye'de genişbant internet kullanan abone sayısının 11,3 milyona ulaştığı, ülkemizin Hollanda ve İngiltere'den sonra Avrupa'da en çok internet kullanan üçüncü ülke konumunda olduğu, ayda yaklaşık 32 saat internetin kullanıldığı, bu artış hızı ile birlikte siber güvenlik konusunun da önemini artırdığını, ülkemizde teknik altyapının, siber savunma sistemlerinin ve bu alana ilişkin idari düzenlemelerin hızlı bir biçimde hayata geçirilmesi gerektiğini" belirtmiştir.
Bilgi Güvenliği Derneği Başkanı Doç. Dr. Mustafa Alkan, "uluslararası savaşların artık siber ortamda gerçekleştiğine 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 gerektiğini, yaşayan bir sistem olarak bilgi güvenliği olgusunun hayata geçirilmesi gerektiğini, siber dünyada her türlü tedbiri almamız ve her türlü tehdit ve tehlikeye karşı hazır olmamız gerektiğini, Bilgi güvenliği konusunda Bilgi Güvenliği Derneği olarak bir uzmanlar kurulu oluşturmaya başladıklarını, bu konuda yetişmiş insan kaynağımızı bir araya getirmek ve yine siber güvenlik konusunda bilim ve danışma kurullarını da hayata geçirmek istediklerini, siber güvenlik konusundaki çalışma ve faaliyetleri canlı tutarak ülkemizi daha güvenli hale getirmeyi hedeflediklerini belirtmişlerdir.
Çalıştayda; "Türkiye ve Siber Güvenlik", "Tehditler ve Olası Önlemler", "Dünyada Siber Güvenlik", "Siber Güvenlik ve Sanal Hava Boşluğu", "Güncel Siber Tehdit İstihbaratı", "Siber Güvenlik Felsefesi", "Siber Güvenlik İçin Milli Çözümler", "Siber Savaş ve Türkiye için Öneriler", "Kritik Altyapılara Yönelik Siber Tehditler ve Türkiye için Önerileri", "Kriptografi ve Siber Güvenlik", "Kritik Altyapı Güvenliğine Yönelik Özgün Çözümler: Sanal Hava Boşluğu", "Açık Kaynak İstihbarat, İnternet ve Siber Güvenlik", "Siber Güvenlik için Yerel Ağ Erişim Kontrolü", "Siber Terör Saldırılarından Korunma" konularında davetli konuşmacılar ile bildirileri kabul edilen araştırmacılar sunumlarını paylaşmışlardır.

Çalıştayın Sonuç Bildirgesi aşağıda sunulmuştur.

SİBER GÜVENLİK ÇALIŞTAYI 2011 SONUÇ BİLDİRGESİ

1. Günümüzde, bilgi ve iletişim teknolojilerinin her geçen gün birey ve toplum hayatında çok daha fazla yer işgal ettiği, artık bu sistemler olmadan birçok hizmetin sunulamaz ve alınamaz hala geldiği; bu yönüyle bilgi ve iletişim teknolojilerinin etkin hizmet sunumu ve hızlı üretim imkanı sağladığı, ancak daha önceden var olmayan yeni riskleri de beraberinde getirdiği,

2. Başta kamu olmak üzere tüm kurum ve kuruluşların birçok hizmetlerini internet ortamında sunmaya başlamasıyla birlikte bu ortamda yaşanacak olumsuzlukların sosyal ve ekonomik hayatımızı önemli ölçüde etkileyebileceği, yaşanacak muhtemel siber güvenlik olaylarının kişisel ve toplumsal pek çok ekonomik ve sosyal olumsuz hususu beraberinde getirebileceği ve sonuçta telafisi güç neticelere sebebiyet verebileceği, dolayısıyla elektronik ortamdaki oluşacak kesinti veya saldırıların kişisel, kurumsal ve ulusal anlamda kabul edilemez boyutlara varabileceğinin farkında olunması, bunun tüm kesimler tarafından biliniyor olması ve gerekli önlemlerin arttırılmasının artık zorunluluk olduğu,

3. Ağ ve bilgi sistemlerin ve varlıklarının ülke ekonomisi, kamu refahı ve güvenliği için çok önemli olduğu, dolayısıyla da siber varlıkların güvenliğinin ülke ve toplum güvenliğiyle eşdeğer olduğu, bu hususun her zaman hatırda tutularak kapsamlı ve uzun soluklu adımlar atılması ve çözümler geliştirilmesi gerektiği,

4. Siber tehdit algısının siber ortamı yoğun olarak kullanan kurum ve kuruluşlarca kısmen var olduğu fakat kapsamlı risk değerlendirmesinin kısıtlı sayıdaki kuruluşlarca yapıldığı ve bu sayının arttırılmasının zaruri olduğu,

5. Kritik altyapı güvenliği konusunda ilgili kurumların çalışma yapmalarının ve koruma seviyelerini arttırmalarının gerektiği,

6. Siber güveliğin temel unsurlarından olan güvenlik yazılım ve donanımlarının yerli üretiminin kısıtlı olduğu, bu durumun ülke güvenliği için stratejik öneme sahip olması nedeniyle yerli ürünlerin üretimine daha fazla teşvik verilmesinin gerekli olduğu,

7. Gelişmiş ülkelerde siber güvenlik politika ve projelerinin büyük ölçüde tamamlandığı, bu konuda kurumsal altyapıların tamamlanarak ilgili kurumlarca Siber Güvenlik çalışmalarının yürütüldüğü, Türkiye'de de ivedilikle politika ve strateji belirleme sürecinin hızlandırılması ve beraberinde kurumsal yapılanmanın gerçekleştirilmesi gerektiği,

8. Hızlı artan ve çeşitlenen tehditlere karşı etkin mücadelenin küresel ölçekte örgütlenmiş organizasyonlar eliyle yürütülebileceği, bu yönüyle siber saldırılara karşı uluslararası bilgi paylaşımı ve işbirliklerinin de önem arz ettiği, Türkiye'nin ilgili organizasyonlarla işbirliğini daha da güçlendirmesi gerektiği, hatta bu konuda bölgesel bir siber güvenlik organizasyonunun kurulmasına öncülük etmesinin çok yerinde olacağı ve bölgede lider ülke olma vizyonunu da güçlendireceği,

9. Siber güvenlik tehditlerine karşı koymak için ülkemizde yeterli bilgi birikimi, donanım ve insan kaynağı potansiyelinin olduğu ancak mevcut kaynaklarının verimli kullanılabilmesi için koordinasyonun zorunlu olduğu,

10. Kamu kurumları, STK'lar, sektör ve üniversitelerin beraber çalışarak siber güvenlik konusunda ihtiyaç duyulan strateji ve politikaları geliştirmesi,

11. Ülkemizde üniversitelerin siber güvenlik konusunda lisansüstü eğitimde programlar açmalarının gerekli olduğu, ilgili bölümlerde de konuyla ilgili dersler açılmasının faydalı olacağı,

12. Ülkemizde yürütülen siber güvenlik tatbikatların, bu alanda farkındalığın oluşması ve gerekli tedbirlerin alınmasına büyük katkılar sağladığı/sağlayacağı, devlet koordinasyonunda daha geniş katılımlı Siber Güvenlik Tatbikatlarının yapılmasının ve desteklenmesinin gerekli olduğu,

13. Ulusal ve uluslararası siber saldırıların izlenmesinin ve bunları kapsayan bir veritabanının teşkil edilmesinin muhtemel saldırıların tespiti noktasında fayda sağlayacağı,

14. Siber saldırılarla mücadele ve gerekli savunma unsurlarının hazırlanması için gerekli yapısal düzenlemelerin ivedilikle hayata geçirilmesi gerektiği,

15. Kurumların ve bireylerin maruz kaldıkları siber saldırılara karşı hukuki düzenlemelerin ihtiyaca cevap verecek biçimde yeniden ele alınması gerektiği,

16. Siber bilgi güvenliğini yüksek oranda sağlamada en önemli hususun başında "bilgiyi ve teknolojiyi üreten ülke" olmak gerektiğinin her zaman hatırda bulunarak gerekli adımların atılması gerektiği,

17. Gizli ve açık siber saldırılara karşı sadece reaktif tutum izlemenin yeterli olmayacağı, kısmen oluşturulan mevcut karşı savunma gücünün geliştirilmesinin ihtiyaç olduğu,

18. Kurum ve kuruluşların kendi siber savunma talimatlarının oluşturulması ve bu talimatlarda ilgili çalışanların görev ve sorumluluklarının da tanımlanması gerektiği, ayrıca talimattaki hususlara uyulup uyulmadığının uzman kurullarca denetlenmesinin, kurum ve kuruluşların güvenliği için önem arz ettiği,

19. Siber güvenlik ve savunma konularında bilgi birikimlerinin ve tecrübelerin paylaşımını temin etmek amacıyla kurumlar arası işbirliğinin güçlendirilmesi gerektiği,

20. Kurumların bilgi varlıklarını savunmalarına destek olmak, gerektiğinde müdahale etmek ve toplu saldırılar karşısında gerekli savunmayı yapmak ve koordinasyonu sağlamak amacıyla 'Acil Kriz Yönetimi ve Müdahale Merkezi' kurulmasının gerekliliği,

21. Elektronik ortamlarda hizmet veren veya iş ve işlemleri yürüten tüm kamu kurum ve kuruluşlar ile özel sektör kuruluşlarının uluslararası güvenlik standartlarıyla belgelendirilmesinin artık bir zorunluluk haline geldiği ve bu hususun kısa sürede tamamlanmasının fayda getireceği,

22. Uzman kişilerin bilgi ve becerilerinden faydalanmak amacıyla, kamuda sözleşmeli siber güvenlik uzmanlarının istihdamıyla ilgili düzenlemelerin yapılması gerektiği,

23. Kişisel kurumsal ve ulusal bazda bütüncül tedbir ve çözümlerin ortaya konulacağı siber güvenlik ulusal eylem planına ihtiyaç duyulduğu,

24. Ulusal farkındalığın arttırılmasına katkı sağlamak amacıyla ABD'de olduğu gibi Eylül ayının "Siber Güvenlik Farkındalık Ayı" olarak kabul edilmesi ve tüm kamu ve özel sektör kurumlarının bu ayda konuyla ilgili olarak belirli bir plan dahilinde çalışmalar yürütmesinin faydalı olacağı, İnternet Kurulunda bu konunun detaylı olarak tartışıldıktan sonra bu ayın belirlenerek gerekli faaliyetlerin bu yıldan başlamak üzere başlatılmasının faydalı olacağı ve

25. Bilgi Güvenliği Derneği tarafından başlatılan "Siber Güvenlik Ulusal Koordinasyon Kurulu" oluşturulması çalışmalarına ilgili tüm tarafların katılımının sağlanması, bu kurul marifetiyle Kurumsal, Ulusal ve Uluslararası ölçekte siber güvenlik çalışmalarının yürütülmesinin ülke siber güvenlik ve savunma stratejilerinin kapsamlı olarak oluşturulması ve geliştirilmesine büyük katkılar sağlayacağı

değerlendirilmiştir.

Kamuoyuna saygıyla duyurulur.

Siber Güvenlik Çalıştayı 2011 Düzenleme Kurulu