



www.mevzuattakip.com.tr

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı

Ekli “Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı”nın kabulü; Ulaştırma, Denizcilik ve Haberleşme Bakanlığının 18/2/2013 tarihli ve 412 sayılı yazısı üzerine, Bakanlar Kurulu’nca 25/3/2013 tarihinde kararlaştırılmıştır.

Karar Sayısı : 2013/4890

Resmî Gazete: 20 Haziran 2013 / 28683

ULUSAL SİBER GÜVENLİK STRATEJİSİ VE 2013-2014 EYLEM PLANI

GİRİŞ

Ülkemizde bilgi ve iletişim sistemlerinin kullanımı hızla yaygınlaşmakta, bilgi ve iletişim sistemleri hayatımızın her alanında önemli roller oynamaktadır. Kamu kurumları yanında enerji, su kaynakları, sağlık, ulaşım, haberleşme ve finansal hizmetler gibi kritik altyapı sektörlerinde faaliyet gösteren kurum ve kuruluşlar da bilgi ve iletişim sistemlerini yoğun olarak kullanmaktadır. Sözü edilen sistemler, verilen hizmetin kalitesini ve hızını artırmakta, dolayısıyla hem ilgili kurumun daha verimli çalışmasını sağlamakta hem de vatandaşlarımızın yaşam standardının yükseltilmesine katkıda bulunmaktadır.

Kurumlarımızın hizmet sunumlarında bilgi ve iletişim sistemlerini her geçen gün daha fazla kullanmaları ile birlikte, söz konusu bilgi ve iletişim sistemlerinin güvenliğinin sağlanması hem ulusal güvenliğimizin, hem de rekabet gücümüzün önemli bir boyutu haline gelmiştir. Bilgi ve iletişim sistemlerinde bulunan güvenlik zafiyetleri, bu sistemlerin hizmet dışı kalmasına veya kötüye kullanılmasına, can kaybına, büyük ölçekli ekonomik zarara, kamu düzeninin bozulmasına ve/veya ulusal güvenliğin

ihlaline neden olabilecektir.

Siber ortamın bilişim sistemlerine ve veriye yapılan saldırılar için anonimlik ve inkâr edilebilirlik fırsatları sunduğu bir gerçektir. Saldırı için gerekli araç ve bilgi çoğu zaman ucuz ve kolay elde edilebilir iken dünyanın herhangi bir yerindeki kişi veya sistemlerin kasıtlı ya da kasıtsız olarak siber saldırılara iştirak ettikleri görülmektedir. Kritik altyapılara ait bilişim sistem ve verilerini hedef alan ısrarcı ve gelişmiş siber saldırıların kimler tarafından finanse ve organize edildiğinin tespiti ise neredeyse imkânsız görülmektedir. Bu durum ve özellikler siber ortamdaki risk ve tehditlerin asimetrik karakterini ortaya koymakta, mücadeleyi güçleştirmektedir.

Tüm bu bilgiler ışığında, Bakanlar Kurulunca alınan 11/6/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, 20/10/2012 tarihli ve 28447 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir. Söz konusu Bakanlar Kurulu Kararı uyarınca;

"Siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla; Ulaştırma, Denizcilik ve Haberleşme Bakanının başkanlığında, Dışişleri, İçişleri, Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme bakanlıkları müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkam, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ile Ulaştırma, Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşan Siber Güvenlik Kurulu kurulmuştur."

Image not found or type unknown

Aynı Bakanlar Kurulu Kararı ile ulusal siber güvenliğin sağlanmasına ilişkin politika, strateji ve eylem planlarını hazırlama görevi Ulaştırma, Denizcilik ve Haberleşme Bakanlığına verilmiştir. Tüm kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler Siber Güvenlik Kurulu tarafından belirlenen politika, strateji ve eylem planları çerçevesinde kendilerine verilen görevleri yerine getirmek ve belirlenen usul, esas ve standartlara uymakla yükümlüdür.

İlgili Karar gereğince hazırlanan bu Eylem Planı, 2013-2014 döneminde gerçekleştirilmesi planlanan işleri tanımlamakla beraber, bu yılları aşan periyodik faaliyetler ile eğitim ve bilinçlendirme çalışmaları gibi sürekli yürütülmesi gereken faaliyetlere de yer vermektedir.

1.1. Tanımlar

Bu belgede geçen;

- a) Bilişim sistemleri: Bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmetin, işlemin ve verinin sunumunda yer alan sistemleri,
- b) Siber ortam: Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortamı,
- c) Kamu bilişim sistemleri: Türkiye Cumhuriyeti kamu kurum ve kuruluşlarına ait olan ve/veya kamu kurum ve kuruluşları tarafından işletilen bilişim sistemlerini,
- ç) Gerçek ve tüzel kişilere ait bilişim sistemleri: Türkiye Cumhuriyeti kanunlarına tabi olarak gerçek ve tüzel kişilere ait olan ve/veya gerçek ve tüzel kişilerce işletilen bilişim sistemlerini,
- d) Ulusal siber ortam: Kamu bilişim sistemleri ile gerçek ve tüzel kişilere ait bilişim sistemlerinden oluşan ortamı,
- e) Gizlilik: Bilişim sistem ve verilerine sadece yetkili kişi veya sistemlerce erişilebilmesini; bilişim sistemlerine ait veya sistemdeki gizli verinin yetkisiz kişi veya sistemlerce ifşa edilmemesini,
- f) Bütünlük: Bilişim sistemlerinin ve bilginin sadece yetkili kişilerce veya sistemlerce değiştirilebilmesini,
- g) Erişilebilirlik: Yetkili kişilerin ve işlemlerin ihtiyaç duyulan zaman içerisinde ve ihtiyaç duyulan kalitede bilişim sistemlerine ve bilgiye erişebilmesini,
- ğ) Kritik altyapılar: İşlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda,
-Can kaybına,
-Büyük ölçekli ekonomik zarara,
-Ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına, yol açabilecek bilişim sistemlerini barındıran altyapıları,
- h) Siber güvenlik olayı: Bilişim sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini,
- ı) Siber güvenlik: Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini,
- i) Ulusal siber güvenlik: Ulusal siber ortamda bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmet, işlem ve verinin ve bunların sunumunda yer alan sistemlerin

siber güvenliğini, ifade eder.

1.2. Amaç

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının amacı;

a) Kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet. işlem ve veri ile bunların sunumunda kullanılan sistemlerin güvenliğinin sağlanmasına,

b) Kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerinin güvenliğinin sağlanmasına,

c) Siber güvenlik olaylarının etkilerinin en düşük düzeyde kalmasına, olayların ardından sistemlerin en kısa sürede normal çalışmalarına dönmeye yönelik stratejik siber güvenlik eylemlerinin belirlenmesine ve oluşan suçun adli makam ve kollukça daha etkin araştırılmasının ve soruşturulmasının sağlanmasına, yönelik bir altyapı oluşturmaktır.

1.3. Kapsam

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, kamu bilişim sistemlerini ve kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerini kapsar.

1.4. Güncelleme

Ulusal Siber Güvenlik Stratejisi gelişen teknoloji, değişen şartlar ve ihtiyaçlar göz önünde bulundurularak kamu ve özel sektörden gelecek talepler doğrultusunda en az yılda bir kez olmak üzere ulusal düzeyde sağlanacak eşgüdüm ile güncellenecektir.

2. SİBER GÜVENLİK RİSKLERİ

Stratejik siber güvenlik eylemlerinin en doğru şekilde belirlenebilmesi için siber güvenliğe yönelik risklerin gerçekçi bir biçimde belirlenmesi gerekmektedir. Mevcut bilgiler ışığında ülkemizde bulunan bilgi ve iletişim sistemleri ile ilişkili başlıca risk unsurları aşağıda sıralanmıştır:

1) Siber ortamın bilişim sistemlerine ve veriye yapılan saldırılar için anonimlik ve inkâr edilebilirlik fırsatları sunması, saldırı için gerekli araç ve bilginin çoğu zaman ucuz ve kolay elde edilebilir olması, dünyanın herhangi bir yerindeki kişi veya sistemlerin kasıtlı ya da kasıtsız olarak siber saldırılara iştirak edebilmeleri nedeniyle tehdidin asimetrik olması.

- 2) Siber ortamın bütünleşik ve kesintisiz iletişime açık yapısı ve siber ortamda bulunan kötücül yazılım ve benzeri tehdit ajanları nedeni ile siber ortamda yer alan tüm bilişim sistemlerinin birbirlerine zarar verebilmesi.
- 3) Günümüzde büyük kitlelere sunulan kritik hizmet ve servislerin birçoğunun bilişim sistemleri tarafından sağlanıyor ya da kontrol ediliyor olması.
- 4) Kritik altyapılara ait bilişim sistemlerinin çoğunun internete bağlı olması.
- 5) Siber güvenliğin ulusal düzeyde bütün vatandaşlarca topyekûn sağlanabileceği gerçeğine rağmen bu konudaki ulusal bilincin yetersiz olması.
- 6) Siber güvenlik alanında paydaş kurumların arasında ulusal koordinasyon eksikliği.
- 7) Kişi ve kurumların kamuoyu önünde saygınlıklarını kaybetmemek amacıyla veya başka sebeplerle kendilerine yönelik saldırıları gizlemesi.
- 8) Siber güvenlik olaylarının araştırma ve soruşturulmasında ulusal ve uluslararası mevzuat yetersizliklerinin işbirliğini güçleştirmesi.
- 9) Kritik altyapı hizmet ve servislerinin, gerçekleştirilen siber saldırılara ek olarak bilişim sistemlerinin kendi hatalarından, kullanıcı hatalarından ya da doğal afetlerden de olumsuz olarak etkilenmesi ve bu tür olaylara yönelik alınabilecek tedbirler açısından gerekli yeterliliğe sahip olunmaması.
- 10) Kurumlarda bilgi güvenliği yönetimi altyapılarının yeterli düzeyde olmaması.
- 11) Siber güvenlik konusunda kurumsal ve kişisel seviyede yeterli bilgi ve bilinç seviyesine ulaşılamamış olması.
- 12) Siber güvenlik konusunda kurumların üst düzey yöneticilerinin yeterli bilince sahip olmamaları veya siber güvenlik konusunu yeterince sahiplenmemeleri.
- 13) Siber güvenlik konusunda kurumların yapılanmalarının yetersiz olması ve siber güvenliğin, kurumların sadece bilgi işlem birimlerinin sorumluluğunda görülmesi.
- 14) Bilgi işlem birimlerinde çalışanların siber güvenlik konusunda yeterli bilgi seviyesine ve tecrübeye sahip olmaması.
- 15) Siber güvenlik olaylarının detaylı araştırılması ve ihlal ile ortaya çıkan suçun soruşturulması alanlarında az sayıda yeterli personel bulunması.
- 16) Kurumsal iç denetim süreçlerinde siber güvenliğe ilişkin denetim adımlarının yeterli seviyede ele alınmaması.

17) Siber güvenliğin, geliştirilen veya tedarik edilen bilişim sistemlerinin vazgeçilmez bir unsuru olarak ele alınmaması, buna bağılı olarak kamu kurumlarının bilgi ve iletişim teknolojileri alanındaki ürün ve hizmet tedariklerinde siber güvenliğin yeterli seviyede göz önünde bulundurulmaması.

18) Donanım ve yazılım alanında yerli üretimin yeterli düzeyde olmaması.

3- İLKELER

Ulusal siber güvenliğin sağlanmasında göz önünde bulundurulacak ilkeler şunlardır:

1) Siber güvenlik, risk yönetimini esas alan, etkin ve sürekli iyileştirmeye dayalı yöntemler aracılığıyla sağlanır.

2) Siber güvenlik için teknik boyutun yanı sıra, hukuki, idari, ekonomik, politik ve sosyal boyutlarda güçlü ve zayıf yönlerin, tehditlerin ve fırsatların belirlenmesini içeren bütüncül bir yaklaşım benimsenir.

3) Risk yönetiminde, teknik zaafpların giderilmesi, saldırı ve tehdidin önlenmesi ile muhtemel zararın en aza indirgenmesi unsurları esas alınır.

4) Siber güvenliğin sağlanmasında birey, kurum, toplum ve devletin tüm hukuki ve sosyal sorumluluklarını yerine getirmesi esas kabul edilir.

5) Kritik altyapıların güvenliğinin sağlanması için, özel sektörle, karar mekanizmalarına katılımı da içeren tam bir işbirliği yapılır.

6) Siber ortam güvenliğinin sağlanması ve sürdürülmesinde kamu, özel sektör, üniversiteler ve sivil toplum örgütleri işbirliğinin yanı sıra uluslararası işbirliği ve bilgi paylaşımı esas kabul edilir.

7) Uluslararası işbirliği ve bilgi paylaşımı için diplomatik, teknik ve kolluk iletişim kanallarının sürekli ve etkin kullanımı esas alınır.

8) İhtiyaç duyulan mevzuat geliştirilirken uluslararası anlaşma ve düzenlemeler göz önünde bulundurulur.

9) Hukukun üstünlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunması ilkeleri temel esas kabul edilir.

10) Siber ortamda şeffaflık, hesap verilebilirlik, etik değerler ve ifade özgürlüğü desteklenir.

11) Güvenlik ile kullanılabilirlik arasında denge kurulur.

12) Düzenleyici ve denetleyici kurumlar sorumlu oldukları alanlarda siber güvenliğin sağlanmasını gözetirler.

13) Siber güvenlik gereksinimlerinin karşılanmasında yerli ürün ve hizmet kullanımı teşvik edilir, bunların geliştirilmesi için araştırma ve geliştirme projeleri desteklenir, inovasyon (yenileşim) anlayışı esas kabul edilir.

4- STRATEJİK SİBER GÜVENLİK EYLEMLERİ

Siber ortamda sayıları her geçen gün artan tehditleri bertaraf etmek ve ulusal siber ortamda bulunan açıklıkları mümkün olduğunca azaltmak, ülke olarak hedeflemekte olduğumuz bilgi toplumuna dönüşüm sürecinin sağlıklı bir şekilde ilerlemesi açısından büyük önem arz etmektedir. Bilgi toplumuna dönüşüm sürecinde, bilgi ve iletişim teknolojilerinin daha büyük kitleler tarafından etkin, kaliteli ve uygun maliyetle kullanılmasının yanı sıra, söz konusu teknolojilere dayalı bilişim sistemlerinin kullanımında siber güvenliğin tesis edilmesi de son derece önemlidir. Bu bakımdan, bilişim sistemlerinin ve bu sistemler tarafından işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin korunması olarak ifade edilen siber güvenlik; bilgi toplumuna dönüşmeyi hedefleyen ülkemizde toplumun huzur ve refahı, ülkenin ekonomik kalkınması ve istikrarı, ulusal güvenliğin sağlanması gibi pek çok alanı etkileyen çok paydaşlı ve stratejik bir konudur.

Bu çerçevede, 2013-2014 döneminde, belirlenen ilkeler ışığında, ulusal siber güvenliğin sağlanmasına yönelik stratejik eylemlerin gerçekleştirilmesi planlanmıştır. Söz konusu eylemler, gerektiğinde alt eylemlere ayrılarak, planlanan bitirme tarihlerine ve sorumlu/ilgili kuruluşlarına göre ileriki bölümde listelenmiştir. 2013-2014 döneminde gerçekleştirilmesi planlanan stratejik eylemler aşağıdaki başlıklar altında gruplanmıştır.

4.1. Yasal Düzenlemelerin Yapılması

2013-2014 döneminde, ulusal siber güvenliğin sağlanması konusunda gerek kurum ve kuruluşların görev, yetki ve sorumluluklarını tanımlayan, gerekse ihtiyaç duyulan alanlarda mevcut eksiklikleri gidermeyi amaçlayan mevzuatın oluşturulması çalışmalarına başlanacaktır. Söz konusu çalışmalar, ceza hukuku, medeni hukuk, idari yargı ve bunlara ilişkin tüm usul hükümlerinin düzenlenmesine destek olacak bir nitelik arz edecektir. Ayrıca, kavram kargaşasının önüne geçmek amacıyla siber güvenlik terimleri sözlüğü oluşturulacaktır.

4.2 Adli Süreçlere Yardımcı Olacak Çalışmaların Yürütülmesi

Uluslararası hukuk kuralları çerçevesinde, siber saldırılara maruz kalan tarafların haklarının korunabilmesi için, saldırı kaynağının tespiti ve saldırılan sistemler ile bu sistemlerden hizmet alan taraflarda hangi boyutta etki oluştuğunun belirlenmesi

gerekir. Bu bilgilerin üretilmesi için ulusal siber ortamın günün teknolojisine uygun ve güvenilir kayıt mekanizmaları ile donatılması gerekmektedir.

4.3 Ulusal Siber Olaylara Müdahale Organizasyonunun Oluşturulması

Kısa vadede; siber ortamda ortaya çıkan tehditlerin hızla belirlenmesi, yaşanabilecek olayların etkilerini azaltmaya veya ortadan kaldırmaya yönelik önlemlerin geliştirilmesi ve paylaşılması için ulusal ve uluslararası düzeyde etkin bir şekilde çalışacak Siber Olaylara Müdahale Organizasyonu oluşturulacak, böylece kurum ve kuruluşların siber güvenlik olaylarına müdahale yeteneği kazanması sağlanacaktır. Ülkemizi etkileyebilecek tehditlere karşı, 7/24 müdahale esasına göre çalışacak "Ulusal Siber Olaylara Müdahale Merkezi (USOM)" kurularak, USOM'un koordinasyonunda çalışacak sektörel "Siber Olaylara Müdahale Ekipleri (SOME)" oluşturulacaktır. Sektörel SOME'ler siber olaylara müdahalenin yanı sıra kendisinc bağlı SOME'lere ve ilgili olduğu sektöre özel bilgilendirme ve bilinçlendirme faaliyetleri yürütecektir. Kurum ve kuruluşlar bünyesinde de sektörel SOME'lerin koordinasyonunda çalışacak SOME'ler kurulacaktır. USOM ve SOME'ler olaylara müdahale ederken suç soruşturmasına destek sağlayacak verilerin sağlanması için adli makam ve kolluk birimleri ile koordineli hareket edeceklerdir. USOM ulusal temas noktası olarak diğer ülkelerin eşdeğer makamlarıyla ve uluslararası kuruluşlarla yakın işbirliği yapacaktır.

4.4. Ulusal Siber Güvenlik Altyapısının Güçlendirilmesi

Kısa ve orta vadede tüm kurumlar, kurumsal bilişim sistemlerinin siber güvenliğini destekleyecek geniş kapsamlı altyapı projeleri gerçekleştirilecektir. Öncelikli olarak kritik altyapılara ait bilişim sistemleri olmak üzere kurumsal siber güvenliğin sağlanması için çalışmalar yapılacaktır. Kritik altyapılara ait bilişim sistemleri, kritiklik seviyeleri, birbirleriyle ilişkileri ve sorumluları belirlenecektir. Kritik altyapılara ait bilişim sistemlerinin siber güvenliği, teknolojik önlemlerin yanı sıra idari tedbir ve süreçlerle de sağlanacaktır. Bunun için kurumlarda idari ve teknolojik içerikli eğitimler aracılığıyla üst düzey yöneticiler başta olmak üzere tüm çalışanların siber güvenlik konusunda yetkinlik düzeyi artırılacaktır. Kurumsal siber güvenliği sağlama konusunda gerekli yetkinliğe sahip olmayan kurumlar teknolojik ve idari boyutta sağlanacak hizmetlerle desteklenecektir.

4.5. Siber Güvenlik Alanında İnsan Kaynağının Yetiştirilmesi ve Bilinçlendirme Faaliyetleri

Orta ve uzun vadede siber güvenlik alanında yeterli sayıda ve yetkin insan kaynağı oluşturulmasına yönelik çalışmalar yapılacaktır. İlk, orta, lise öğretimi ve yaygın eğitim ile yükseköğretimde siber güvenlik konusunun yer alması için düzenlemeler yapılacaktır. Bilişim sistemleri denetçilerinin, teknoloji geliştiricilerinin, sistem yöneticilerinin ve ilgili tüm tarafların siber güvenlik bilincinin artırılması ve üstlerine

düŖen sorumluluklar konusunda bilgilendirilmeleri amacıyla etkinlikler gerekleŖtirilecektir. Kurumsal i denetim srelerinde siber gvenliĐe iliŖkin denetim adımlarının yeterli seviyede ele alınması iin alıŖmalar yapılacaktır. Ayrıca, siber gvenlik bilincini oluŖturmak ve geliŖtirmek zere tm vatandaŖlara ynelik bir eĐitim platformu oluŖturulacak ve bu eyleme hizmet eden giriŖimler desteklenecektir.

4.6. Siber Gvenlikte Yerli Teknolojilerin GeliŖtirilmesi

Orta ve uzun vadede siber gvenlik konusunda lkemizin sahip olduĐu teknik birikim, olanak ve kabiliyetler artırılabilecektir. Kamu ve zel sektrn araŖtırma ve geliŖtirme gereksinimlerinin karŖılanmasına ynelik tm eylemlerde iŖbirliĐi ierisinde alıŖması saĐlanacaktır. Kurumların biliŖim sistemlerinde yerli olarak geliŖtirilmiŖ rnleri tercih etmeleri, yerli rnlerin mevcut olmadıĐı durumlarda ise gvenlik deĐerlendirmesi yerli olarak gerekleŖtirilmiŖ sertifikalı rnleri tercih etmeleri teŖvik edilecektir.

4.7. Ulusal Gvenlik Mekanizmalarının Kapsamının GeniŖletilmesi

Ulusal gvenlikten sorumlu kurumlarımızın grev alanlarının ulusal ve uluslararası siber ortamda gerekleŖtirilen zararlı faaliyetlere karŖı savunmayı da ierecek Ŗekilde dzenlenmesi iin alıŖmaların baŖlatılması gerekmektedir.

5. 2013 -2014 DNEMİ ULUSAL SİBER GVENLİK EYLEM PLANI

Bu blmde, ulusal siber gvenlik stratejisi erevesinde 2013-2014 dnemi iin, ulusal siber gvenliĐin belirlenen ilkeler iŖıĐında saĐlanmasına ynelik eylemler yer almaktadır. Sz konusu eylemler, bu dokmanın drdnc blmnde belirlenmiŖ olan baŖlıklara gre gruplandırılmıŖtır. Her eylem iin sadece bir sorumlu kurum ya da kuruluŖ belirlenmiŖtir. Ancak, aynı eylemin birden fazla ilgili kurum ya da kuruluŖu olabilmektedir. Bu durumda, ilgili tm kurum ve kuruluŖların, sorumlu kurum ve kuruluŖun koordinatrlĐnde gerektiĐinde iŖbirliĐi halinde, gerektiĐinde ise paralel olarak hareket ederek eylemin gerektirdiĐi alıŖmaları yrtmeleri ngrlmektedir. Eylem Planında yer alan eylem ve alt eylemlerin bir kısmı iin bitirilme tarihi belirlenmiŖ, periyodik olarak tekrarlanması ve srekli olarak yrtlmesi ngrlen eylemler ise ayrıca belirtilmiŖtir. 2013-2014 dneminde, gerekleŖtirilmesi planlanan toplam 29 adet eylem maddesi bulunmaktadır

-2013-2014 EYLEM PLANI-

I. YASAL DZENLEMELERİN YAPILMASI

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve ?lgili (?) Kurulu?lar
----	-------	-----------	------------------	--------------------------------------

1.	Siber Güvenlik Kurulunun Faaliyetlerine Ba?lamas?	- Siber Güvenlik Kurulunun faaliyetlerine ba?lamas? ve çal??ma usul ve esaslar?n? belirlemesi.	Tamamlanm??t?r.	- Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (S)
22.	Siber Güvenlik Konusunda Mevzuat Çal??malar?n?n Yap?lmas?	- Siber güvenlik alan?nda ulusal ve uluslararası mevzuat?n incelenmesi ve ihtiyaç duyulan yasal düzenlemelerin tespit edilmesi.	Temmuz 2013	- Adalet Bakanl??? (S) - Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (?) - D??i?leri Bakanl??? (?), - ?çi?leri Bakanl??? (?) - Milli Savunma Bakanl??? (?) - Kamu Düzeni ve Güvenli?i Müste?arl??? (?) - Bilgi Teknolojileri ve ?leti?im Kurumu (?)
		- Siber güvenlik terimleri sözlü?ünün olu?turulmas?.	Aral?k 2014	Türk Dil Kurumu (S)

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve ?lgili (?) Kurulu?lar
2.	Siber Güvenlik Konusunda Mevzuat Çal??malar?n?n Yap?lmas?	- Mevcut birincil mevzuat?n (kanunlar) siber güvenlik konusunda ihtiyaç duyulan hususlar? kapsayacak ?ekilde güncellenmesi ve yeni düzenleme gereksinimlerini kar??layacak birincil mevzuat çal??malar?n?n tamamlanarak Siber Güvenlik Kuruluna sunulmas?.	Eylül 2013	-Adalet Bakanl?? (S) -Ula?t?rma, Denizcilik ve Haberle?me Bakanl?? (S) -D??i?leri Bakanl?? (S) -Çi?leri Bakanl?? (S) -Milli Savunma Bakanl?? (S) -Genelkurmay Ba?kanl?? (S) -Kamu Düzeni ve Güvenli?i Müste?arl?? (S) -Bilgi Teknolojileri ve ?leti?im Kurumu (S)
		- Siber güvenlik hizmetleri ile ilgili ikincil mevzuat (yönetmelik, tebli?) çal??malar?n?n yap?lmas?.	Sürekli	-Ula?t?rma, Denizcilik ve Haberle?me Bakanl?? (S) -Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (S)

II. ADL? SÜREÇLERE YARDIMCI OLACAK ÇALI?MALARIN YÜRÜTÜLMES?

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve ?lgili (?) Kurulu?lar
----	-------	-----------	------------------	--------------------------------------

3.	Siber Olayların Delillendirilmesi	-Olay sonrasında incelenmek üzere güvenilir delillerin elde edilmesi için tutulacak kayıtların asgari niteliklerinin belirlenmesi	Haziran 2013	-Çiğleri Bakanlı?? (S) -Jandarma Genel Komutanlı?? (?) -Milli İstihbarat Teşkilatı Müsteşarlı?? (?) -Emniyet Genel Müdürlüğü (?) -Bilgi Teknolojileri ve İletişim Kurumu / -Telekomünikasyon İletişim Başkanlı?? (?) -TÜBİTAK (i)
		-Olay sonrasından incelenmek üzere güvenilir delillerin elde edilmesi için ilgili kamu kurumlarının, günün teknolojisine ve uluslararası standartlara uygun kayıt mekanizmalarının devreye alması.	Mart 2014	-Ulaştırma, Denizcilik ve Haberleşme Bakanlı?? (S) -Çiğleri Bakanlı?? (?) -Adalet Bakanlı?? (?) -Tüm kamu kurumları (?)
		- Olay sonrasında incelenmek üzere güvenilir delillerin elde edilmesi için kritik sektörlerde faaliyet gösteren kuruluşların, günün teknolojisine ve uluslararası standartlara uygun kayıt mekanizmalarının sağlanması.	Mayıs 2014	- Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (S)

III. ULUSAL SİBER OLAYLARA MÜDAHALE ORGANİZASYONUNUN OLUŞTURULMASI

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (?) Kuruluşlar
----	-------	-----------	------------------	--------------------------------------

4.	Ulusal Siber Olaylara Müdahale Merkezinin (USOM) Kurulması ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) Oluşturulması	- 7/24 esasına göre yapılacak Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulması.	Tamamlanmamıştır.	-Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S)
		Merkezin ulusal koordinasyon ve uluslararası işbirliği gerektiren durumlarda devreye girecek çalışma usul ve esasları ile prosedür ve süreçlerinin hazırlanması. Siber güvenlikte görevli kamu personeli için merkezi yardım sayfaları hazırlanması, acil önlemler alınacak konuların çevrim içi olarak iletilmesinin sağlanması.	Temmuz 2013	-Çiğli Bakanlığı (?) -Bilgi Teknolojileri ve İletişim Kurumu / Telekomünikasyon İletişim Bakanlığı (?) -Emniyet Genel Müdürlüğü (?) -Jandarma Genel Komutanlığı (?) TÜBİTAK (?)
		Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) oluşturulması ve iletilmesi için çalışma esaslarının belirlenmesi, rehber dokümanların ve eğitim planlarının hazırlanması.	Ağustos 2013	-Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) -Bilgi Teknolojileri ve İletişim Kurumu / Telekomünikasyon İletişim Bakanlığı (?) -Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (?) - TÜBİTAK (i)

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (?) Kurumlar
----	-------	-----------	------------------	------------------------------------

4.	Ulusal Siber Olaylara Müdahale Merkezinin (USOM) Kurulması ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) Oluşturulması	- Kritik altyapı sektörlerine özel sektörel SOME'lerin kurulması ekiplerin oluşturulması, eğitimlerin alınması?	Aralık 2013	- USOM (S) Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (?)
		-Sektörel SOME'lerin doğrudan IJSOM'un koordinasyonunda faaliyet yürütmesi. -Sektörel SOME'lerin USOM'un sağladığı destekten yararlanması?	Mart 2014	-USOM (S) -Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar.
		-Kamu kurumları SOME'lerinin kurulması	Eylül 2014	- USOM (S) -Tüm kamu kurumları (?)
		-Kamu kurumları SOME'lerinin doğrudan USOM'un koordinasyonunda faaliyet yürütmesi. -Kurumsal SOME'lerin varsa bazıları oldukları sektörel SOME ve USOM'un sağladığı destekten yararlanması?	Aralık 2014	-USOM (S) -Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (?) -Tüm kamu kurumları (?)

IV. ULUSAL SİBER ALTYAPISININ GÜÇLENDİRİLMESİ

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (?) Kurumlar
5.	Kritik Altyapılarda Bilgi Güvenliği Yönetimi Programı	- Siber tehditlerin doğrudan hedefi haline gelen ve zarar görmesi halinde toplum düzenini bozabilecek kritik altyapılarının tespit edilmesi.	Temmuz 2013	-TÜBİTAK (S) -Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (?)
		- Belirlenecek bir kritik altyapının sektörel risk analizinin yapılması.	Ağustos 2013	
		-Sektörel risk analizi yöntemlerinin belirlenmesi.	Eylül 2013	-Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (S)
		-Sektörel acil eylem planlarının gereksinimlerinin belirlenmesi.	Şubat 2014	-TÜBİTAK (?) -USOM (?)

-	Mart 2014 Y?ll?k risk analizi raporlama çal??malar?n?n ilkinin tamamlanmas?.
-	Sektörel i? sürekli? planlar?n? gereksinimlerinin belirlenmesi ve uygulanmas?.
-	Sektörel güvenlik önlemlerinin belirlenmesi ve uygulanmas?.

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve ?lgili (?) Kurulu?lar
6.	Kamu Bilgi Güvenli? Program?	Kamu kurumlar?n?n uymas? gereken asgari güvenlik kriterleri doküman?n?n haz?rlanmas?.	A?ustos 2013	TÜB?TAK (S) -Ula?t?ma, Denizcilik ve Haberle?me Bakanl??? (?)
		Sistem yöneticilerine ve ilgili di?er teknik personele öncelikli ihtiyaçlar uyar?nca periyodik siber güvenlik e?itimlerinin ilkinin verilmesi, e?itim alan personelin yeterliliklerinin tespiti.	ilki tamamlanm??t?r.	-USOM (?)
		Kurum baz?nda yap?lmas? zorunlu k?l?nacak y?ll?k güvenlik test ve denetimlerinin ilkinin, önceliklendirilccck kamu kurumlar? için ilgili kurumlarla mutabakat sa?lanarak gerçekte?tirilmesi.	Aral?k 2013	

- Bilişim sistemleri güvenliğine ilişkin sıklıkla ulaştırma dokümanları ve standartların yayınlanması ve güncellenmesi.		-TÜBİTAK (S)		
7.	Siber Güvenlik Eğitim Altyapısının Güçlendirilmesi	- Kurumların bilgi sistemlerinden ve siber güvenliğinden sorumlu üst düzey yöneticilerin bilgilendirilmesi. Teknik personelin eğitilmesi ve eğitime katılan personele sertifika verilmesi. - Kamu kurum ve kuruluşlarında çalışan iç denetim birimi personeline bilişim sistemleri denetimi yeteneği kazandıracak eğitimlerin verilmesi.	Tamamlanmıştır.	-Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) -TÜBİTAK (?) Devlet Personel Bakanlığı (?)
			Mayıs 2014	

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (?) Kuruluşlar
8.	Siber Güvenlik Tatbikatlarının Düzenlenmesi	- Ulusal ya da uluslararası niteliğe sahip siber güvenlik tatbikatlarının düzenlenmesi.	2013 'ten itibaren iki yılda bir düzenlenecektir.	-Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) - İçişleri Bakanlığı (?) -Bilgi Teknolojileri ve İletişim Kurumu (?) Emniyet Genel Müdürlüğü (?) - Jandarma Genel Komutanlığı (?) -Genelkurmay Başkanlığı (?) -TÜBİTAK (?) -USOM (i) -Sektörel SOME'ler (?)

- Ülkemiz liderliğinde Uluslararası Siber Güvenlik Mayıs 2014	-Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) Dışişleri Bakanlığı (?) -Bilgi Teknolojileri ve İletişim Kurumu (?) -Emniyet Genel Müdürlüğü (?) -Genelkurmay Bakanlığı (?) -TÜBİTAK (?)
- Tatbikatların ilkini düzenlenmesi.	

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (?) Kuruluşlar
9.	Kamu Güvenli İletişim Kurallarının Belirlenmesi	Kamu kurumları arasında güvenli veri paylaşımını sağlamak üzere kurulların ve prosedürlerin belirlenmesi.	Aralık 2013	-Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) -USOM (?) -Bilgi Teknolojileri ve İletişim Kurumu (?) -Kamu Düzeni ve Güvenliği Müsteşarlığı (?) -TÜBİTAK(?)
10.	Yazılım Güvenliği Programının Yürütülmesi	- Yazılım güvenliği ile ilgili eğitimlerin hazırlanması ve yazılım geliştiricilere verilmeye başlanması.	Aralık 2013	-TÜBİTAK (S) -Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (?) -Türk Standardları Enstitüsü (?)
		- Kritik altyapılarda kullanılmak üzere geliştirilen yazılımlar için programlama dili başlıca güvenli yazılım geliştirme temel kurulların dokümanlarının yayımlanması.	Aralık 2013	
		-Kritik altyapılar için geliştirilen yazılımların güvenlik deęerlendirmeleri kapsamında ilgili kurumların bünyesinde gerekli teknik isterlerin uygulanması ve kontrolüne yönelik fizibilitenin hazırlanarak Siber Güvenlik Kuruluna sunulması.	Mart 2014	

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve ?lgili (?) Kurulu?lar
11	Siber Tehditleri Onleme Projesinin Yürütülmesi	Siber tehditleri tespit amacıyla Balküpü Sistemi kurulması?	Temmuz 2013	-Bilgi Teknolojileri ve ?leti?im Kurumu / Telekomünikasyon ?leti?im Ba?kanl??? (S) -Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (?) -TÜB?TAK (?)
		- Ulusal siber sald?r? raporlama sisteminin kurulması ve geli?tirilmesi.	Aral?k	
		- Siber tehditlerle ilgili y?ll?k istatistik üretilmesi.	Aral?k 2013	
		- Siber tehditlerin tespit edilmesi, izlenmesi ve önlenmesine ili?kin gerekli mekanizmalar?n geli?tirilmesi.	Aral?k 2014	
12	Siber Güvenlik Konusunda Ürünlerin ve Hizmet Sa?lay?c?lar?n Belgelendirilmesi	Bilgi sistemlerinin güvenlik testlerini yapan, siber güvenlik konusunda e?itim ve dan??manl?k veren, siber güvenlik konusunda belirlenecek di?er alanlarda hizmet sunan gerçek ve tüzel ki?ilerde bulunması gereken asgari özelliklerin belirlenmesi ve belgelendirme sürecinin tasarlanması?	Eylül 2013	-Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (S) -TÜB?TAK (?) -Türk Standardlar? Enstitüsü (?)

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve ?lgili (?) Kurulu?lar
12.	Siber Güvenlik Konusunda Ürünlerin ve Hizmet Sa?lay?c?lar?n Belgelendirilmesi	- Kamu kurumlar? tarafından kullanılan ve siber güvenlik aç?s?ndan kritik öneme sahip bilgi teknolojileri ve bilgi sistemleri ürünlerinin ve bunlar?n sahip olması gereken asgari güvenlik gereksinimlerinin belirlenmesi ve belirlenen bu belgelendirmenin yapılması?	A?ustos 2014	-Türk Standardlar? Enstitüsü (S) -Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (?) -TURKAK (?) -TÜB?TAK (?)

13.	Adli Bilişim Konusunda Hizmet Sağlayıcılara Güvenlik Belgesi Verilmesine Yönelik Kuralların Belirlenmesi	- Adli bilişim ile ilgili hizmet sunan gerçek ve tüzel kişilerde bulunması gerekten asgari özelliklerin belirlenmesi ve belgelendirme sürecinin tasarlanması.	Mayıs 2014	-Adalet Bakanlığı (S) -Çiğleri Bakanlığı (?) -Emniyet Genel Müdürlüğü (?) -Jandarma Genel Komutanlığı (?)
-----	--	---	---------------	---

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (?) Kuruluşlar
14	?? Sürekliliği ve Veri Yedekleme Sistemleri Kurulması	Kamu kurumlarının ve kritik bilgi sistem altyapılarının işleten özel sektör kuruluşlarının elektronik ortamda işlem yapan sistemlerinin ve verilerinin güvenlik risk seviyelerinin belirlenmesi.	Eylül 2013	-Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) -TÜBİTAK (i) -Tüm kamu kurum ve kuruluşları (?) -Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (?)
		- Kamu kurum ve kuruluşlarının ve kritik bilgi sistem altyapılarının işleten özel sektör kuruluşlarının hassas verilerinin yedekleme usul ve esaslarının belirlenmesi.	Kasım 2013	
		- Tüm kamu kuruluşları ve kritik bilgi sistem altyapılarının işleten özel sektör kuruluşları tarafından işletme sürekliliği planları yapılması.	Ocak 2014	
		- ?? sürekliliği planları gereği bilişim sistemlerinin kurulması.	Temmuz 2014	
		- ?? sürekliliği planlarına uygun tatbikatların düzenlenerek sonuçlarının Siber Güvenlik Kuruluna sunulması.	Aralık 2014	

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve ?lgili (?) Kurulu?lar
15	Kamu Kurum ve Kurulu?lar?n?n ?nternet Sayfalar?n?n Yerli Veri Merkezlerine Ta??nmas?	- Kamu kurumlar?n?n internet sitelerinin yerli ve güvenilir bir veri merkezinde tutulmas?n? teminen veri merkezi hizmeti sunacak kurulu?un veya kurulu?lar?n belirlenmesi.	Ekim 2013	-Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (S) Bilgi Teknolojileri ve ?leti?im Kurumu (?) -TÜB?TAK (?)
		- Internet sayfalar?n? kendi bünyesinde bar?nd?rmayan belediyeler, hastaneler, il/ilçe kamu birimleri gibi kamu kurumlar?n?n internet sitelerini belirlenen veri merkezine/merkezlerine ta??mas?.	Aral?k 2013	- Tüm kamu kurum ve kurulu?lar? (S)
		Belirlenen veri merkezlerinin güvenlik denetimlerinin düzenli olarak yap?lmas?.	Sürekli	-Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (S)
16	Veri S?zmas?n? Tespite Yönelik Test Altyap?s? Geli?tirilmesi ve Uygulamaya Al?nmas?	-Kritik kurumlardan veri s?zmas?n? tespit edecek analiz altyap?s? geli?tirilmesi.	Aral?k 2013	- Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (S) -TÜB?TAK (?)
		- Siber Güvenlik Kurulu taraf?ndan bu test altyap?s?n?n uygulanaca?? kun?mlar?n tespit edilmesi.	Ocak 2014	
		-Veri s?zma tespitine yönelik testlerin yap?lmas? ve sonuçlar?n?n raporlanmas?.	May?s 2014	

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve ?lgili (?) Kurulu?lar
----	-------	-----------	------------------	--------------------------------------

17	Kamu Kurumlarında Verilere Erişim Düzeylerinin Belirlenmesi	- Uluslararası standartlarla (öm. TS ISO/IEC 27001) uyumlu erişim kontrol prensiplerinin oluşturulması?	Ekim 2013	-Siber Güvenlik Kurulu (S) -Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) -TÜBİTAK (S) -Tüm kamu kurum ve kuruluşları (S)
		- Kamu e-devlet uygulamalarının internet üzerinden yetkisiz veriye erişimi engelleyecek şekilde tekrar düzenlenmesi.	Şubat 2014	
18	Açık Kaynak Kodlu Ürünlerin Kullanımının Teşvik Edilmesi	- Kamu ve özel sektör kurumlarının kullanabileceği, belirlemeye asgari güvenlik kriterlerini sağlayan açık kaynak kodlu mevcut güvenlik ürünleri hakkında bilgilendirme yapılması?	Ekim 2013	-TÜBİTAK(S) -Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) -Üniversiteler (S)
		- Açık kaynak kodlu yeni siber güvenlik ürünlerinin geliştirilmesi için platformlarının oluşturulması?	Şubat 2014	
		- Uygun kritik bilişim sistemlerinin açık kaynak kodlu işletim sistemlerine taşınması için planlama yapılması?	Mayıs 2014	

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (S) Kuruluşlar
19	Siber Güvenlik Konusunda Akademisyen Yetiştirilmesi	- Siber güvenlik konusunda doktora ve yüksek lisans yapmalarını için öğrencilere burs verilmeye başlanması?	Ekim 2013	-Yükseköğretim Kurulu Bakanlığı (S) -Milli Eğitim Bakanlığı (S) -TÜBİTAK (S) -Üniversiteler (S)
20	Üniversitelerde Siber Güvenlik Eğitimlerinin Yaygınlaştırılması	- Siber güvenlik altyapısının geliştirilmesi ile ilgili YÖK'te bir komisyonun kurulması?	Tamamlanmıştır.	-Yükseköğretim Kurulu Bakanlığı (S) -TÜBİTAK (S) -Üniversiteler (S)

-	Mart 2014 İlgili branşların lisans, yüksek lisans ve doktora seviyesi müfredatlarına siber güvenlik ile ilgili derslerin eklenmesi.
-	Sürekli Siber güvenlik alanında Türkçe kitap, dergi, makale kaynakların çözümlenmesi.
-	Ekim 2013 En az iki siber güvenlik yüksek lisans programının açılması.
En az bir	Ekim 2014 siber güvenlik doktora programının açılması.

**V. SİBER GÜVENLİK ALANINDA İNSAN KAYNAĞININ YETİTİLMESİ VE
BENİMLENİMLERİNE FAALİYETLERİ**

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili Kuruluşlar
21	Siber Güvenlik Uzmanlığına Yönlendirme Programının Yürütülmesi	Siber güvenlik konusunda uzmanlaşmak isteyen öğrenciler için burs programlarının oluşturulması.	Eylül 2014	-Yükseköğretim Kurulu Başkanlığı (S) -Milli Eğitim Bakanlığı -TÜBİTAK (?) -Üniversiteler (?)
		- Siber güvenlik konusunda yaz kampları düzenlenmesi.	2013 yılından itibaren düzenlenecektir.	- TÜBİTAK (S)
		- Siber güvenlik staj programlarının oluşturulması.	Eylül 2014	- Yükseköğretim Kurulu Başkanlığı (S)
		- Üniversitelerde siber güvenlik ile ilgili tanıtım faaliyetleri düzenlenmesi.	Sürekli	

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve ?lgili Kurulu?lar
21.	Siber G?venlik Uzmanl???na Y?nlendirme Program?n?n Y?r?t?lmesi	- Universiteler aras? siber savunma yar??malar?n?n d?zenlenmesi.	Her y?l d?zenlenecektir.	-T?B?TAK (S) -Y?ksek?retim Kurulu Ba?kanl??? (?)
		- ?lk, orta, lise ve ?niversite kategorilerinde bilgi g?venli?i bilin?lendirme video/poster yar??malar? d?zenlenmesi.	Her y?l d?zenlenecektir.	- Milli E?itim Bakanl??
		USOM ve SOME'lerde ?al??an uzmanlar?n e?itim almas? ve uygulama deneyimi kazanmas?.	S?rekli	Ula?t?rma, Denizcilik ve Haberle?me Bakanl?? -Bilgi Teknolojileri ve ? Kurumu (?) -USOM (i) -SOME'ler (?)
		- Siber g?venlik olaylar?na m?dahale edecek g?venlik birimlerinin kapasitelerinin an??lmas?, uzmanlar?n e?itimi ve uzmanlara uygulama deneyimi kazand??lmas?.	S?rekli	-?çi?leri Bakanl??? (S) T?B?TAK (?)

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve ?lgili (?) Kurulu?lar
----	-------	-----------	------------------	--------------------------------------

22.	İlk, Orta, Lise Öğretimi ve Yaygın Eğitimde Siber Güvenlik Eğitimlerinin Yaygınlaştırılması	<p>-Meslek liselerinin bilgisayar programcılarının bölümlerinin müfredatına siber güvenliğin eklenmesi.</p> <p>-Bilgi teknolojileri alanında yer alan kurs programları arasında siber güvenlik konusuna yer verilmesi.</p> <p>-FATİH Projesi kapsamına siber güvenlik eğitimlerinin dâhil edilmesi.</p> <p>-Bilgi teknolojileri eğitimlerinde açık kaynak kodlu ürünlerin de yer alması.</p>	Mart 2014	<p>-Milli Eğitim Bakanlığı (S) - TÜBİTAK (?)</p> <p>-Bilgi Teknolojileri ve İletişim Kurumu (?)</p>
23.	Bilgisayar Kullanıcılarının Siber Güvenlik Konusunda Bilinçlendirilmesi	<p>Bilgisayar kullanıcılarının siber güvenlik konusunda bilinç düzeyinin artırılması için çalışmalar yapılması (seminerler, broşürler, yaygın eğitim faaliyetleri, basın ve yaygın organlar aracılığıyla uzaktan eğitim ve bilinçlendirme).</p> <p>- İnternetin güvenli kullanımı ve "güvenli internet hizmeti" konusunda bilinç düzeyinin artırılması, söz konusu hizmetin geliştirilmesi ve yaygınlaştırılması.</p>	Sürekli	<p>-Bilgi Teknolojileri ve İletişim Kurumu (S)</p> <p>-Milli Eğitim Bakanlığı (?)</p> <p>-Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (?)</p> <p>-Radyo ve Televizyon Üst Kurulu(?)</p>

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (?) Kuruluşlar
----	-------	-----------	------------------	--------------------------------------

24	Ulusal ve Uluslararası Siber Güvenlik Etkinlikleri Düzenlenmesi	<p>-Siber güvenlik ile ilgili olarak, konunun ekonomik, sosyal ve hukuki boyutları da ele alacak şekilde konferans ve sempozyumlar düzenlenmesi.</p> <p>-Siber güvenlik konulu uluslararası konferans, toplantı, serniner ve tatbikat çalışmaları katılmaları sağlanması.</p>	Sürekli	<p>-Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S)</p> <p>-Dışişleri Bakanlığı (?)</p> <p>-Bilgi Teknolojileri ve İletişim Kurumu (?)</p> <p>-TÜBİTAK (?)</p> <p>-Tüm kamu kurum ve kuruluşları (i)</p> <p>-Üniversiteler (?)</p> <p>-STK'lar (i)</p>
----	---	---	---------	--

VI. SİBER GÜVENLİKTE YERLİ TEKNOLOJİLERİN GELİTİRİLMESİ

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (?) Kuruluşlar
25	AR-GE Faaliyetlerinin Tevik Edilmesi	-Ülkenin siber güvenlik ihtiyacı karşılayacak teknolojilerin listesinin oluşturulması ve güncel tutulması.	Sürekli	<p>-Bilim ve Teknoloji Yüksek Kurulu (S)</p> <p>Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (?)</p> <p>-Bilim, Sanayi ve Teknoloji Bakanlığı (?)</p> <p>-TüBİTAK (?)</p>
		-Mevcut proje tevik sistemleri içerisinde siber güvenliğin öncelikli konu olarak dâhil edilmesi.	Mart 2014	
		-Siber güvenlik ile ilgili yazılım, donanım ve benzeri bilişim teknolojisi ürünlerine yönelik ulusal AR-GE faaliyetleri tevik mekanizmaları oluşturulması.	Mart 2014	
26	Siber Güvenlik Konusunda AR-GE Laboratuvarlarının Kurulması	Zararlı yazılımlar ve bu yazılımların bilişim sistemlerinde yaptıkları etkileri belirleyebilecek laboratuvar altyapısının kurulması.	Eylül 2013	- TÜBİTAK (S)

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve ?lgili (?) Kurulu?lar
26	Siber Güvenlik Konusunda AR-GE Laboratuvarlar?n?n Kurulmas?	-Üniversitelerde siber güvenlik konusunda AR-GE laboratuvarlar?n?n kurulmas?n? te?vik edecek ve destekleyecek programlar?n olu?turulmas?.	Mart 2014	-Yüksekö?retim Kurulu -Ba?kanl??? (S) -Kalk?nma Bakanl??? (?) -Ula?t?rma, Denizcilik ve -Haberle?me Bakanl??? (?)
		-Üniversitelerde program kapsam?nda ilk siber güvenlik -AR-GE la boratuvar?n?n kurulmas?.	Eylül 2014	-Bilim, Sanayi ve Teknoloji -Bakanl??? (?) - TÜB?TAK (?)
27	Siber Güvenlikte Yerli Ürün ve Çözüm Çal??malar?	- Kamu ve özel sektör, üniversite, sivil toplum kurulu?u ve benzeri tüm bilgi güvenli?i payda?lar?n?n kat?laca?? düzenli çal??malar yap?lmas?. -Kat?l?mc?lar?n?n, bilgi teknolojileri ürünlerinin siber güvenlik kapsam?nda do?ru kullan?m?, teknolojik önlemler ve gereksinimler, AR-GE gereksinimleri, geli?tirilmekte olan bilgi teknolojileri ürünleri ile idari önlemler ve mevzuat konular?nda i?birli?i yapmas?.	Kas?m 2013	-Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (S) Bilgi Teknolojileri ve ?leti?im Kurumu (?) -TÜB?TAK (i) - Üniversiteler (?) -STK'lar (?)

28	Yerli Ürünlerin Teşvik Edilmesi	<p>- Kurumların bilgi ve iletişim sistemlerinde,</p> <p>a) Yerli olarak geliştirilmiş, güvenlik değerlendirilmesi ve sertifikalandırılması gerçekleştirilmiş ürünleri tercih etmeleri,</p> <p>b) Yerli ürünlerin mevcut olmadıkları durumlarda güvenlik değerlendirilmesi ve sertifikalandırılması gerçekleştirilmiş ürünleri tercih etmeleri, için teşvik mekanizmaları oluşturulması.</p>	Şubat 2014	<p>-Bilim, Sanayi ve Teknoloji Bakanlı??? (S)</p> <p>-Ulaştırma, Denizcilik ve Haberleşme Bakanlı??? (?)</p> <p>-Kalkınma Bakanlı??? (?)</p> <p>Gümrük ve Ticaret Bakanlı??? (?)</p> <p>-Ekonomi Bakanlı??? (?)</p> <p>Maliye Bakanlı??? (?)</p> <p>Kamu ihale Kurumu (?)</p>
----	---------------------------------	---	------------	---

VII. ULUSAL GÜVENLİK MEKANİZMALARININ KAPSAMININ GELİŞTİRİLMESİ

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (?) Kuruluşlar
29	Ulusal Siber Güvenliğin Milli Güvenliğe Entegrasyonu	<p>-Siber ortamda çeşitli siber güvenlik olayları meydana geldiğinde kurumların sorumluluklarının ve ulusal düzeyde koordinasyonun nasıl sağlanacağına belirlenmesi.</p>	Mart 2014	<p>-Siber Güvenlik Kurulu (S)</p> <p>Çiğleri Bakanlı??? (?)</p> <p>Milli Savunma Bakanlı??? (?)</p> <p>-Adalet Bakanlı??? (?)</p> <p>-Milli Güvenlik Kurulu Genel Sekreterliği (?)</p>
		<p>Ülkemizi hedef alan olasılıkların senaryolarının ve bunların yaratabileceği etkilerin belirlenmesi.</p>	Mart 2014	<p>-Genelkurmay Başkanlı??? (?)</p> <p>-Milli İstihbarat Teşkilatı Müsteşarı??? (?)</p> <p>-Kamu Düzeni ve Güvenliği Müsteşarı??? (?)</p> <p>-Emniyet Genel Müdürlüğü (?)</p> <p>-Jandarma Genel Komutanlı??? (?)</p>

-
Siber
ortamda
meydana
gelebilecek
çe?itli
olaylarda
devreye
girecek
mekanizmalar?
mevcut Eylül 2014
durumunun
analizi
ve
iyile?tirilmeleri
için
gerçekle?tirilmesi
gereken
öncelikli
eylemlerin
belirlenmesi.

Telefon: +90 (312) 473 84 23

E-Posta: mts@mevzuattakip.com.tr

Adres: Çetin Emeç Bulvarı Hürriyet Cad. No: 2/12 Çankaya ANKARA