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 oltamda 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 dönmesine 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 oltamda 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 bağlı 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 zaafların 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 sorumluluklarım 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 bitirilme 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

Image not found or type unknown

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

düşen sorumluluklar konusunda bilgilendirilmeleri amacıyla etkinlikler gerçekleştirilecektir. Kurumsal iç denetim süreçlerinde siber güvenliğe ilişkin denetim adımlarının yeterli seviyede ele alınması için çalışmalar yapılacaktır. Ayrıca, siber güvenlik bilincini oluşturmak ve geliştirmek üzere tüm vatandaşlara yönelik bir eğitim platformu oluşturulacak ve bu eyleme hizmet eden girişimler desteklenecektir.

4.6. Siber Güvenlikte Yerli Teknolojilerin Geliştirilmesi

Orta ve uzun vadede siber güvenlik konusunda ülkemizin sahip olduğu teknik birikim, olanak ve kabiliyetler artırılacaktır. Kamu ve özel sektörün araştırma ve geliştirme gereksinimlerinin karşılanmasına yönelik tüm eylemlerde işbirliği içerisinde çalışması sağlanacaktır. Kurumların bilişim sistemlerinde yerli olarak geliştirilmiş ürünleri tercih etmeleri, yerli ürünlerin mevcut olmadığı durumlarda ise güvenlik değerlendirmesi yerli olarak gerçekleştirilmiş sertifikalı ürünleri tercih etmeleri teşvik edilecektir.

4.7. Ulusal Güvenlik Mekanizmalarının Kapsamının Genişletilmesi

Ulusal güvenlikten sorumlu kurumlarımızın görev alanlarının ulusal ve uluslararası siber ortamda gerçekleştirilen zararlı faaliyetlere karşı savunmayı da içerecek şekilde düzenlenmesi için çalışmaların başlatılması gerekmektedir.

5. 2013 -2014 DÖNEMİ ULUSAL SİBER GÜVENLİK EYLEM PLANI

Bu bölümde, ulusal siber güvenlik stratejisi çerçevesinde 2013-2014 dönemi için, ulusal siber güvenliğin belirlenen ilkeler ışığında sağlanmasına yönelik eylemler yer almaktadır. Söz konusu eylemler, bu dokümanın dördüncü bölümünde belirlenmiş olan başlıklara göre gruplandırılmıştır. Her eylem için sadece bir sorumlu kurum ya da kuruluş belirlenmiştir. Ancak, aynı eylemin birden fazla ilgili kurum ya da kuruluşu olabilmektedir. Bu durumda, ilgili tüm kurum ve kuruluşların, sorumlu kurum ve kuruluşun koordinatörlüğünde gerektiğinde işbirliği halinde, gerektiğinde ise paralel olarak hareket ederek eylemin gerektirdiği çalışmaları yürütmeleri öngörülmektedir. Eylem Planında yer alan eylem ve alt eylemlerin bir kısmı için bitirilme tarihi belirlenmiş, periyodik olarak tekrarlanması ve sürekli olarak yürütülmesi öngörülen eylemler ise ayrıca belirtilmiştir. 2013-2014 döneminde, gerçekleştirilmesi planlanan toplam 29 adet eylem maddesi bulunmaktadır

Image not found or type unknown
Image not found or type unknown

-2013-2014 EYLEM PLANI-

I. YASAL DÜZENLEMELER?N 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 uluslararas? 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??? (?) -D??i?leri Bakanl??? (?) ?çi?leri Bakanl??? (?) -Milli Savunma Bakanl??? (?) -Genelkurmay Ba?kanl??? (?) -Kamu Düzeni ve Güvenli?i Müste?arl??? (?) -Bilgi Teknolojileri ve ?leti?im Kurumu (?)
		- 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 (?)

İmage not found or type unknown

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

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

3.	Siber Olaylar?n Delillendirilmesi	-Olay sonras?nda ?ncelenmek üzere güvenilir delillerin cldc edilmesi için tutulacak kay?tlar?n asgari niteliklerinin belirlenmesi	Haziran 2013	-?çi?leri Bakanl??? (S) -Jandarma Genel Komutanl??? (?) -Milli ?stihbarat Te?kilat? Müste?arl??? (?) -Emniyet Genel Müdürlü?ü (?) -Bilgi Teknolojileri ve ?leti?im Kurumu / -Telekomünikasyon ?leti?im Ba?kanl??? (?) -TÜB?TAK (i)
		-Olay sonras?ndan incelenmek üzere güvenilir delillerin elde edilmesi için ilgili kamu kurumlar?n?n, günün teknolojisine ve uluslararas? standartlara uygun kay?t mekanizmalar?n? devreye almas?.	Mart 2014	-Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (S) -?çi?leri Bakanl??? (?) -Adalet Bakanl??? (?) -Tüm kamu kurumlar? (?)
		- Olay sonras?nda incelenmek üzere güvenilir delillerin elde edilmesi için kritik sektörlerde faaliyet gösteren kurulu?lar?n, günün teknolojisine ve uluslararas? standartlara uygun kay?t mekanizmalar?n? devreye almalar?n?n sa?lanmas?.	May?s 2014	- Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (S)

III. ULUSAL S?BER OLAYLARA MÜDAHALE ORGAN?ZASYONUNUN OLU?TURULMASI

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

4.	Ulusal Siber Olaylara Müdahale Merkezinin (USOM) Kurulmas? ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) Olu?turulmas?	- 7/24 esas?na göre çal??acak Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmas?.	Tamamlanm??t?r.	-Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (S)
		Merkezin ulusal koordinasyon ve uluslararas? i?birli?i gerektiren durumlarda devreye girecek çal??ma usul ve esaslar? ile prosedür ve süreçlerinin haz?rlamas?.Siber güvenlikte görevli kamu personeli ?çin merkezi yard?m sayfas? haz?rlanmas?, acil önlem al?nacak konular?n çevrim içi olarak iletilmesinin sa?lanmas?.	Temmuz 2013	-?çi?leri Bakanl???(?) -Bilgi Teknolojileri ve ?leti?im Kurumu / Telekomünikasyon -?leti?im Ba?kanl??? (?) -Emniyet Genel Müdürlü?ü (?) -Jandarma Genel Komutanl??? (?) TÜB?TAK (?)
		Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) olu?turulmas? ve i?letilmesi için çal??ma esaslar?n?n belirlenmesi, rehber dokümanlar?n ve e?itim plan?n?n haz?rlanmas?.	A?ustos 2013	-Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (S) -Bilgi Teknolojileri ve ?leti?im Kurumu / Telekomünikasyon -?leti?im Ba?kanl??? (?) -Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (?) - TÜB?TAK (i)

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

4.	Ulusal Siber Olaylara Müdahale Merkezinin (USOM) Kurulmas? ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) Olu?turulmas?	- Kritik altyap? sektörlerine özel sektörel SOME'lerin kurulmas? ekiplerin olu?turmas?, e?itimlerin al?nmas?.	Aral?k 2013	- USOM (S) Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (?)
		-Sektörel SOME'lerin do?rudan lJSOM'un koordinasyonunda faaliyet yürütmesi. -Sektörel SOME'lerin USOM'un sa?lad??? destekten yararlanmas?.	Mart 2014	-USOM (S) -Kritik sektörleri düzenlemek ve denetlemekle sorumlu krurumlar.
		-Kamu kurumlar? SOME'lcrinin kurulmas?	Eylül 2014	- USOM (S) -Tüm kamu kurumlar? (?)
		-Kamu kurumlar? SOME'lcrin do?rudan USOM'un koordinasyonunda faaliyet yürütmesi. -Km?msal SOME'lerin varsa ba?l? olduklar? sektörel SOME ve USOM'un sa?lad??? destekten yararlanmas?.	Aral?k 2014	-USOM (S) -Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (?) -Tüm kamu kurumlar? (?)

IV. ULUSAL S?BER ALTYAPISININ GÜÇLEND?R?LMES?

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve ?lgili (?) Kurulu?lar
5.	Kritik Altyap?larda Bilgi Güvenli?i Yönetimi Program?	- Siber tehditlerin do?rudan hedefi haline gelen ve zarar görmesi halinde toplum düzenini bozabilecek kritik altyap?lar?n tespit edilmesi.	Temmuz 2013	-TÜB?TAK (S) -Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (?)
		- Belirlenecek bir kritik altyap?n?n sektörel risk analizinin yap?lmas?.	A?ustos 2013	
		-Sektörel risk analizi yöntemlerinin belirlenmesi.	Eylül 2013	-Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (S) -TÜB?TAK (?) -USOM (?)
		-Sektörel acil eylem planlar?n?n gereksinimlerinin belirlenmesi.	?ubat 2014	

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

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve ?lgili (?) Kurulu?lar
6.	Kamu Bilgi Güvenli?i Program?	Kamu kurumlar?n?n uymas? gereken asgari güvenlik kriterleri doküman?n?n haz?rlanmas?.	A?ustos 2013	TÜB?TAK (S) -Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (?) -USOM (?)
		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.	
		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 gerçekle?tirilmesi.	Aral?k 2013	

		- Bili?im sistemleri güvenli?ine ili?kin s?k?la?t?rma dokümanlar? ve standartlar?n yay?nlanmas? ve güncellenmesi.	Sürekli	-TÜB?TAK (S)
7.	Siber Güvenlik E?itim Altyap?s?n?n Güçlendirilmesi	- Kurumlar?n bilgi sistemlerinden ve siber güvenli?inden sorumlu üst düzey yöneticilerin bilgilendirilmesi.	Tamamlanm??t?r.	-Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (S) -TÜB?TAK (?) Devlet Personel Ba?kanl??? (?)
		Teknik personelin e?itilmesi ve e?itime kat?lan personele sertifika verilmesi. - Kamu kurum ve kurulu?lar?nda çal??an iç denetim birimi personeline bili?im sistemleri denetimi yetene?i kazand?racak e?itimlerin verilmesi.	May?s 2014	

NO	**Eylem**	**Alt Eylem**	**Bitirilme Tarihi**	**Sorumlu (S) ve ?lgili (?) Kurulu?lar**
8.	Siber Güvenlik Tatbikatlar?n?n Düzenlenmesi	- Ulusal ya da uluslararas? niteli?e sahip siber güvenlik tatbikatlar?n?n düzenlenmesi.	2013 'ten itibaren iki y?lda bir düzenlenecektir.	-Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (S) - ?çi?leri Bakanl??? (?) -Bilgi Teknolojileri ve ?leti?im Kurumu (?) Emniyet Genel Müdürlü?ü (?) - Jandarma Genel Komutanl??? (?) -Genelkurmay Ba?kanl??? (?) -TÜB?TAK (?) -USOM (i) -Sektörel SOME'ler (?)

- Ülkemiz liderli?inde Uluslararas? Siber Güvenlik - Tatbikatlar?n?n ilkinin düzenlenmesi.	May?s 2014	-Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (S) D??i?leri Bakanl??? (?) -Bilgi Teknolojileri ve ?leti?im Kurumu (?) -Emniyet Genel Müdürlü?ü (?) -Genelkumay Ba?kanl??? (?) -TÜB?TAK (?)

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve ?lgili (?) Kurulu?lar
9.	Kamu Güvenli ?leti?im Kurallar?n?n Belirlenmesi	Kamu kurumlar? aras?nda güvenli veri payla??m?n? sa?lamak üzere kurallar?n ve prosedürlerin belirlenmesi.	Aral?k 2013	-Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (S) -USOM (?) -Bilgi Teknolojileri ve ?leti?im Kurumu (?) -Kamu Düzeni ve Güvenli?i Müste?arl??? (?) -TÜB?TAK(?)
10.	Yaz?l?m Güvenli?i Program?n?n Yürütülmesi	- Yaz?l?m güvenli?i ile ilgili e?itimlerin haz?rlanmas? ve yaz?l?m geli?tiricilere verilmeye ba?lanmas?.	Aral?k 2013	-TÜB?TAK (S) -Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (?) -Türk Standardlar? Enstitüsü (?)
		- Kritik altyap?larda kullan?lmak üzere geli?tirilen yaz?l?mlar için programlama dili ba??ms?z güvenli yaz?l?m geli?tirme temel kurallar? doküman?n?n yay?mlanmas?.	Aral?k 2013	
		-Kritik altyap?lar için geli?tirilen yaz?l?mlar?n güvenlik de?erlendirmeleri kapsam?nda ilgili kurumlar?n bünyesinde gerekli teknik isterlerin uygulanmas? ve kontrolüne yönelik fizibilitenin haz?rlanarak Siber Güvenlik Kuruluna sunulmas?.	Mart 2014	

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve ?lgili (?) Kurulu?lar
11	Siber Tehditleri Onleme Projesinin Yürütülmesi	Siber tehditleri tespit amac?yla Balküpü Sistemi kurulmas?.	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 kurulmas? 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 Urünlcrin 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 bulunmas? gereken asgari özelliklerin belirlemesi ve belgelendirme sürecinin tasarlanmas?.	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 Urünlerin ve Hizmet Sa?lay?c?lar?n Belgelendirilmesi	- Kamu kurumlar? taraf?ndan kullan?lan ve siber güvenlik aç?s?ndan kritik öneme sahip bilgi teknolojileri ve bilgi sistemleri ürünlerinin ve bunlar?n sahip olmas? gereken asgari güvenlik gereksinimlerinin belirlenmesi ve belirlenen bu belgelendirmenin yap?lmas?.	A?ustos 2014	-Türk Standardlar? Enstitüsü (S) -Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (?) -TURKAK (?) -TÜB?TAK (?)

13.	Adli Bili?im Konusunda Hizmet Sa?lay?c?lara Güvenlik Belgesi Verilmesine Yönelik Kurallar?n Belirlenmesi	- Adli bili?im ile ilgili hizmet sunan gerçek ve tüzel ki?ilerde bulunmas? gereken asgari özelliklerin belirlenmesi ve belgelendirme sürecinin tasarlanmas?.	May?s 2014	-Adalet Bakanl??? (S) -?çi?leri Bakanl??? (?) -Emniyet Genel Müdürlü?ü (?) -Jandarma Genel Komutanl??? (?)

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve ?lgili (?) Kurulu?lar
14	?? Süreklili?i ve Veri Yedekleme Sistemleri Kurulmas?	Kamu kurumlar?n?n ve kritik bilgi sistem altyap?lar?n? i?leten özel sektör kurulu?lar?n?n elektronik ortamda i?lem yapan sistemlerinin ve verilerinin güvenlik risk seviyelerinin belirlenmesi.	Eylül 2013	-Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (S) -TÜB?TAK (i) -Tüm kamu kurum ve kurulu?lar? (?) -Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (?)
		- Kamu kurum ve kurulu?lar?n?n ve kritik bilgi sistem altyap?lar?n? i?leten özel sektör kurulu?lar?n?n hassas verilerinin yedeklenme usul ve esaslar?n?n belirlenmesi.	Kas?m 2013	
		- Tüm kamu kurulu?lar? ve kritik bilgi sistem altyap?lar?n? i?leten özel sektör kurulu?lar? taraf?ndan i? süreklili?i planlar? yap?lmas?.	Ocak 2014	
		- ?? süreklili?i planlar? gere?i bili?im sistemlerinin kurulmas?.	Temmuz 2014	
		- ?? süreklili?i planlar?na uygun tatbikatlar?n düzenlenerek sonuçlar?n?n Siber Güvenlik Kuruluna sunulmas?.	Aral?k 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 Kurumlar?nda Verilere Eri?im Düzeylerinin Belirlenmesi	- Uluslararas? standartlarla (öm. TS ISO/IEC 27001) uyumlu eri?im kontrol prensiplerinin olu?turulmas?.	Ekim 2013	-Siber Güvenlik Kurulu (S) -Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (?) - TÜB?TAK (?) -Tüm kamu kurum ve kurulu?lar? (?)
		- Kamu e-devlet uygulamalar?n?n internet üzerinden yetkisiz veriye eri?imi engelleyecek ?ekilde tekrar düzenlenmesi.	?ubat 2014	
18	Aç?k Kaynak Kodlu Ürünlerin Kullan?m?n?n Te?vik Edilmesi	- Kamu ve özel sektör kurumlar?n?n kullanabilece?i, belirlemi? asgari güvenlik kriterlerini sa?layan aç?k kaynak kodlu mevcut güvenlik ürünleri hakk?nda bilgilendirme yap?lmas?.	Ekim 2013	-TÜB?TAK(S) -Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (i) -Üniversiteler (?)
		- Aç?k kaynak kodlu yeni siber güvenlik ürünlerinin geli?tirilmesi için platformlar?n olu?turulmas?.	?ubat 2014	
		- Uygun kritik bili?im sistemlerinin aç?k kaynak kodlu i?letim sistemlerine ta??nmas? için planlama yap?lmas?.	May?s 2014	

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve ?lgili (?) Kurulu?lar
19	Siber Güvenlik Konusunda Akademisyen Yeti?tirilmesi	- Siber güvenlik konusunda doktora ve yüksek lisans yapmalar? için ö?rencilere burs verilmeye ba?lanmas?.	Ekim 2013	-Yüksekö?retim Kurulu Ba?kanl??? (S) Milli E?itim Bakanl??? (?) -TÜB?TAK (?) -Üniversiteler (?)
20	Universitelerde Siber Güvenlik E?itimlerinin Yayg?nla?t?r?lmas?	- Siber güvenlik altyap?s?n?n geli?tirilmesi ile ilgili YÖK'te bir komisyonun kurulmas?.	Tamamlanm??t?r.	-Yüksekö?retim Kurulu Ba?kanl??? (S) -TÜB?TAK (?) -Üniversiteler (?)

- ?lgili bran?lar?n lisans, yüksek lisans ve doktora seviyesi müfredatlar?na siber güvenlik ile ilgili derslerin eklenmesi.	Mart 2014
- Siber güvenlik alan?nda Türkçe kitap, dergi, makale kaynaklar?n ço?alt?lmas?.	Sürekli
- En az iki siber güvenlik yüksek lisans program?n?n aç?lmas?.	Ekim 2013
En az bir siber güvenlik doktora program?n?n aç?lmas?.	Ekim 2014

V. S?BER GÜVENL?K ALANINDA ?NSAN KAYNA?ININ YET??T?R?LMES? VE B?L?NÇLEND?R?LME FAAL?YETLERi

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve ?lgili Kurulu?lar
21	Siber Güvenlik Uzmanl???na Yönlendirme Program?n?n Yürütülmesi	Siber güvenlik konusunda uzmanla?mak isteyen ö?renciler için burs programlar?n?n olu?turulmas?.	Eylül 2014	-Yüksekö?retim Kurulu Ba?kanl??? (S) -Milli E?itim Bakanl??? -TÜB?TAK (?) -Üniversiteler (?)
		- Siber güvenlik konusunda yaz kamplar? düzenlenmesi.	2013 y?l?ndan itibaren düzenlenecektir.	- TÜB?TAK (S)
		- Siber güvenlik staj programlar?n?n olu?turulmas?.	Eylül 2014	- Yüksekö?retim Kurul Ba?kanl??? (S)
		- Universitelerde siber güvenlik ile ilgili tan?t?m faaliyetleri düzenlenmesi.	Sürekli	

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve ?lgili Kurulu?lar
21.	Siber Güvenlik Uzmanl???na Yönlendirme Program?n?n Yürütülmesi	- Universiteler aras? siber savunma yar??malar?n?n düzenlenmesi.	Her y?l düzenlenecektir.	-TÜB?TAK (S) -Yüksekö?retim Kurulu Ba?kanl??? (?)
		- ?lk, orta, lise ve üniversite kategorilerinde bilgi güvenli?i bilinçlendirme video/poster yar??malar? düzenlenmesi.	Her y?l düzenlenecektir.	- Milli E?itim Bakanl??
		USOM ve SOME'lerde çal??an uzmanlar?n e?itim almas? ve uygulama deneyimi kazanmas?.	Sürekli	Ula?t?rma, Denizcilik v Haberle?me Bakanl?? -Bilgi Teknolojileri ve ? Kurumu (?) -USOM (i) -SOME'ler (?)
		- Siber güvenlik olaylar?na müdahale edecek güvenlik birimlerinin kapasitelerinin an?r?lmas?, uzmanlar?n e?itimi ve uzmanlara uygulama deneyimi kazand?r?lmas?.	Sürekli	-?çi?leri Bakanl??? (S) TÜB?TAK (?)

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

22.	?lk, Orta, Lise Ö?retimi ve Yayg?n E?itimde Siber Güvenlik E?itimlerinin Yayg?nla?t?r?lmas?	-Meslek liselerinin bilgisayar programc?l??? bölümlerinin müfredat?na siber güvenli?in eklenmesi. -Bili?im teknolojileri alan? alt?nda yer alan kurs programlar? aras?nda siber güvenlik konusuna yer verilmesi. -FAT?H Projesi kapsam?na siber güvenlik e?itimlerinin dâhil edilmesi. -Bilgi teknolojileri e?itimlerinde aç?k kaynak kodlu ürünlerin de yer almas?.	Mart 2014	-Milli E?itim Bakanl??? (S) - TÜB?TAK (?) -Bilgi Teknolojileri ve ?leti?im Kurumu (?)
23.	Bilgisayar Kullan?c?lar?n?n Siber Güvenlik Konusunda Bilinçlendirilmesi	Bilgisayar kullan?c?lar?n siber güvenlik konusunda bilinç düzeyinin art?r?lmas? için çal??malar yap?lmas? (seminerler, bro?ürler, yayg?n e?itim faaliyetleri, bas?n ve yay?n organlar? arac?l??? ?le uzaktan e?itim ve bilinçlendirme).	Sürekli	-Bilgi Teknolojileri ve ?leti?im Kurumu (S) -Milli E?itim Bakanl??? (?) -Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (?) -Radyo ve Televizyon Üst Kurulu(?)
		- ?nternetin güvenli kullan?m? ve "güvenli internet hizmeti" konusunda bilinç düzeyinin art?r?lmas?, söz konusu hizmetin geli?tirilmesi ve yayg?nla?t?r?lmas?.	Sürekli	

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

24	Ulusal ve Uluslararas? Siber Güvenlik Etkinlikleri Düzenlenmesi	-Siber güvenlik ile ilgili olarak, konunun ekonomik, sosyal ve hukuki boyutlar?n? da ele alacak ?ekilde konferans ve sempozyumlar düzenlenmesi. -Siber güvenlik konulu uluslararas? konferans, toplant?, serniner ve tatbikat çal???nalar?na kat?l?m?n sa?lanmas?.	Sürekli	-Ula?t?rma, Denizcilik ve -Haberle?me Bakanl??? (S) -D??i?leri Bakanl??? (?) -Bilgi Teknolojileri ve ?leti?inm Kurumu (?) -TÜB?TAK (?) -Tüm kamu kurum ve kurulu?lar? (i) -Üniversiteler (?) -STK'lar (i)

VI. S?BER GÜVENL?KTE YERL? TEKNOLOJ?LER?N GEL??T?R?LMES?

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve ?lgili (?) Kurulu?lar
25	AR-GE Faaliyetlerinin Te?vik Edilmesi	-Ülkenin siber güvenlik ihtiyac?n? kar??layacak teknolojilerin listesinin olu?turulmas? ve güncel tutulmas?.	Sürekli	-Bilim ve Teknoloji Yüksek Kurulu (S) Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (?) -Bilim, Sanayi ve Teknoloji Bakanl??? (?) -TüBiTAK (?)
		-Mevcut proje te?vik sistemleri içerisine siber güvenli?in öncelikli konu olarak dâhil edilmesi.	Mart 2014	
		-Siber güvenlik ?le ili?kili yaz?l?m, donan?m ve benzeri bili?im teknolojisi ürünlerine yönelik ulusal AR-GE faaliyetleri te?vik mekanizmalar?n?n olu?turulmas?.	Mart 2014	
26	Siber Güvenlik Konusunda AR-GE Laboratuvarlar?n?n Kurulmas?	Zararl? yaz?l?mlar? ve bu yaz?l?mlar?n bili?im sistemlerinde yapt??? etkileri belirleyebilecek laboratuvar ' altyap?s?n?n kuruln?as?.	Eylül 2013	- TÜB?TAK (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??? (?) -Bilim, Sanayi ve Teknoloji -Bakanl??? (?) - TÜB?TAK (?)
		-Üniversitelerde program kapsam?nda ilk siber güvenlik -AR-GE la boratuvar?n?n kurulmas?.	Eylül 2014	
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 Urünlerin Te?vik Edilmesi	- Kurumlar?n bilgi ve ileti?im sistemlerinde, a)Yerli olarak geli?tirilmi?, güvenlik de?erlendirmesi ve sertifikaland?rmas? gerçekle?tirilmi? ürünleri tercih etmeleri, b)Yerli ürünlerin mevcut olmad??? durumlarda güvenlik de?erlendirmesi ve sertifikaland?rmas? gerçekle?tirilmi? ürünleri tercih etmeleri, için te?vik mekanizmalar? olu?turulmas?.	?ubat 2014	-Bilim, Sanayi ve Teknoloji Bakanl??? (S) -Ula?t?rma, Denizcilik ve Haberle?me Bakanl??? (?) -Kalk?nma Bakanl??? (?) Gümrük ve Ticaret Bakanl??? (?) -Ekonomi Bakanl??? (?) Maliye Bakanl??? (?) Kamu ihale Kurumu (?)

VII. ULUSAL GÜVENL?K MEKAN?ZMALARININ KAPSAMININ GEL??T?R?LMES?

NO	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve ?lgili (?) Kurulu?lar
29	Ulusal Siber Güvenli?in Milli Güvenli?e Entegrasyonu	-Siber ortamda çe?itli siber güvenlik olaylar? meydana geldi?inde kurumlar?n sorumluluklar?n?n ve ulusal düzeyde koordinasyonun nas?l sa?lanaca??n?n belirlenmesi.	Mart 2014	-Siber Güvenlik Kurulu (S) ?çi?leri Bakanl??? (?) Milli Savunma Bakanl??? (?) -Adalet Bakanl??? (?) -Milli Güvenlik Kurulu Genel Sekreterli?i (?) -Genelkurmay Ba?kanl??? (?) -Milli ?stihbarat Te?kilat? Müste?arl??? (?) -Kamu Düzeni ve Güvenli?i Müste?arl??? (?) -Emniyet Genel Müdürlü?ü (?) -Jandarma Genel Komutanl??? (?)
		Ülkemizi hedef alan olas? sald?r? senaryolar?n?n ve bunlar?n yaratabilece?i etkilerin belirlenmesi.	Mart 2014	

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

Telefon: +90 (312) 473 84 23
E-Posta: mts@mevzuattakip.com.tr
Adres: Çetin Emeç Bulvari Hürriyet Cad. No: 2/12 Çankaya ANKARA