T.C.
Ulaştırma Denizcilik ve
Haberleşme Bakanlığı

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı

Ocak 2013

[Bu sayfa boş bırakılmıştır.]

İÇİNDEKİLER

[Bu sayfa boş bırakılmıştır.]

1 Giriş

Ülkemizde bilgi ve iletişim sistemlerinin kullanımı hızla yaygınlaşmakta, bilgi ve iletişim sistemleri hayatımızın her alanında önemli rol oynamaktadır. Kamu kurumlarına ilave olarak enerji, haberleşme, su kaynakları, tarım, sağlık, ulaşım, eğitim 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 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" 20 Ekim 2012 tarih 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 Başkanı, 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."*

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 gereği hazırlanan 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 kavramlardan,

Bilişim sistemleri: Bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmetin, işlemin ve verinin sunumunda yer alan sistemleri,

Siber ortam: Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortamı,

Kamu bilişim sistemleri: Türkiye Cumhuriyeti kamu kurum ve kuruluşlarına ait olan ve/veya kamu kurum ve kuruluşları tarafından işletilen bilişim sistemlerini,

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,

Ulusal siber ortam: Kamu bilişim sistemleri ile gerçek ve tüzel kişilere ait bilişim sistemlerinden oluşan ortamı,

Gizlilik: Bilişim sistem ve verilerine sadece yetkili kişi veya sistemlerce erişilebilmesini; bilişim sistemlerine ait veya sistemdeki gizli verinin yetkisiz kişi veya sistemlerce ifşa edilmemesini,

Bütünlük: Bilişim sistemlerinin ve bilginin sadece yetkili kişilerce veya sistemlerce değiştirilebilmesini,

Erişilebilirlik: Yetkili kişilerin ve işlemlerin ihtiyaç duyulan zaman içerisinde ve ihtiyaç duyulan kalitede bilişim sistemlerine ve bilgiye erişebilmesini,

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,

Siber güvenlik olayı: Bilişim sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini,

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,

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;

- Kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda kullanılan sistemlerin güvenliğinin sağlanmasına,
- Kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerinin güvenliğinin sağlanmasına,
- 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 Siber Güvenlik Riskleri

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 topyekün 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 ancak 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 sorumluluklarını yerine getirmesi esas kabul edilir.

5. Kritik altyapıların güvenliğinin sağlanması için, özel sektörle, karar mekanizmalarına katılımı da içeren tam 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. Denetleyici ve düzenleyici 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 anlayışı esas kabul edilir.

4 Stratejik Siber Güvenlik Eylemleri

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 ayrılmakta, planlanan bitirilme tarihlerine ve sorumlu/ilgili kuruluşlarına göre ilerleyen bölümlerde listelenmiştir. 2013-2014 döneminde gerçekleştirilmesi planlanan stratejik eylemler aşağıdaki başlıklar altında gruplanmıştır.

a) 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 terminolojisi ve sözlüğü oluşturulacaktır.

b) 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.

c) 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 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 kendisine 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 ülkeler in eşdeğer makamlarıyla ve uluslararası kuruluşlarla yakın işbirliği yapacaktır.

d) 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 altyapılar 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.

e) 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. Orta ve yüksek öğrenimde 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.

f) 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.

g) 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 Dönemi Ulusal Siber Güvenlik Eylem Planı

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 adet sorumlu kurum ve kuruluş belirlenmişken; aynı eylemin birden fazla ilgili kurum ve kuruluşu olabilir. 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.

5.1 Yasal Düzenlemelerin Yapılması

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
1.	**Siber Güvenlik Kurulunun faaliyetlerine başlaması**	- Siber Güvenlik Kurulunun faaliyetlerine başlaması ve çalışma usul ve esaslarını belirlemesi	Ocak 2013	- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S)
2.	**Siber güvenlik konusunda mevzuat çalışmalarının yapılması**	- Siber güvenlik alanında ulusal ve uluslararası mevzuatın incelenmesi ve ihtiyaç duyulan yasal düzenlemelerin tespit edilmesi	Nisan 2013	- Adalet Bakanlığı (S) - Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (İ) - Dışişleri Bakanlığı (İ) - İçişleri Bakanlığı (İ) - Milli Savunma Bakanlığı (İ) - Kamu Düzeni ve Güvenliği Müsteşarlığı (İ) - Bilgi Teknolojileri ve İletişim Kurumu (İ)
		- Siber güvenlik terminolojisinin ve sözlüğünün oluşturulması	Aralık 2013	- Türk Dil Kurumu (S)

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
2.	**Siber güvenlik konusunda mevzuat çalışmalarının yapılması**	- Mevcut birincil mevzuatın (kanunlar) siber güvenlik konusunda ihtiyaç duyulan hususları kapsayacak şekilde güncellenmesi ve yeni düzenleme gereksinimlerini karşılayacak birincil mevzuat çalışmalarının tamamlanarak Siber Güvenlik Kurulu'na sunulması	Eylül 2013	- Adalet Bakanlığı (S) - Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (İ) - Dışişleri Bakanlığı (İ) - İçişleri Bakanlığı (İ) - Milli Savunma Bakanlığı (İ) - Genelkurmay Başkanlığı (İ) - Kamu Düzeni ve Güvenliği Müsteşarlığı (İ) - Bilgi Teknolojileri ve İletişim Kurumu (İ)
		- Siber güvenlik hizmetleri ile ilgili ikincil mevzuat (yönetmelik, tebliğ) çalışmalarının yapılması	Sürekli	- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) - Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (İ)

5.2 Adli Süreçlere Yardımcı Olacak Çalışmaların Yürütülmesi

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
3.	**Siber olayların delillendirilmesi**	- Olay sonrasında incelenmek üzere güvenilir delillerin elde edilmesi için tutulacak kayıtların asgari niteliklerinin belirlenmesi	Mayıs 2013	- İçişleri Bakanlığı (S) - Jandarma Genel Komutanlığı (İ) - Milli İstihbarat Teşkilatı Müsteşarlığı (İ) - Emniyet Genel Müdürlüğü (İ) - Bilgi Teknolojileri ve İletişim Kurumu / Telekomünikasyon İletişim Başkanlığı (İ) - TÜBİTAK (İ)
		- Olay sonrasından incelenmek üzere güvenilir delillerin elde edilmesi için ilgili kamu kurumlarının, günün teknolojisine ve uluslararası standartlara uygun kayıt mekanizmalarını devreye alması	Mart 2014	- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) - İçişleri Bakanlığı (İ) - Adalet Bakanlığı (İ) - Tüm kamu kurumları (İ)
		- Olay sonrasında incelenmek üzere güvenilir delillerin elde edilmesi için kritik sektörlerde faaliyet gösteren kuruluşların, günün teknolojisine ve uluslararası standartlara uygun kayıt mekanizmalarını devreye almalarının sağlanması	Mayıs 2014	- Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (S)

5.3 Ulusal Siber Olaylara Müdahale Organizasyonunun Oluşturulması

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
4.	**Ulusal Siber Olaylara Müdahale Merkezinin (USOM) kurulması ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) oluşturulması**	- 7/24 esasına göre çalışacak Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulması - Merkezin ulusal koordinasyon ve uluslararası işbirliği gerektiren durumlarda devreye girecek çalışma usul ve esasları ile prosedür ve süreçlerinin hazırlaması - Siber güvenlikte görevli kamu personeli için merkezi yardım sayfası hazırlanması, acil önlem alınacak konuların çevrim içi olarak iletilmesinin sağlanması	Mayıs 2013	- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) - İçişleri Bakanlığı(İ) - Bilgi Teknolojileri ve İletişim Kurumu / Telekomünikasyon İletişim Başkanlığı (İ) - Emniyet Genel Müdürlüğü (İ) - Jandarma Genel Komutanlığı (İ) - TÜBİTAK (İ)
		- Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) oluşturulması ve işletilmesi için çalışma esaslarının belirlenmesi, rehber dokümanların ve eğitim planının hazırlanması	Temmuz 2013	- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) - Bilgi Teknolojileri ve İletişim Kurumu / Telekomünikasyon İletişim Başkanlığı (İ) - Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (İ) - TÜBİTAK (İ)

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
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 oluşturması, eğitimlerin alınması	Aralık 2013	- USOM (S) - Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (İ)
		- Sektörel SOME'lerin doğrudan USOM'un koordinasyonunda faaliyet yürütmesi - Sektörel SOME'lerin USOM'un sağladığı destekten yararlanması	Mart 2014	- USOM (S) - Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (İ)
		- Kamu kurumlarının SOME'lerinin kurulması	Eylül 2014	- USOM (S) - Tüm kamu kurumları (İ)
		- Kamu kurumları SOME'lerin doğrudan USOM'un koordinasyonunda faaliyet yürütmesi - Kurumsal SOME'lerin varsa bağlı oldukları sektörel SOME ve USOM'un sağladığı destekten yararlanması	Aralık 2014	- USOM (S) - Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (İ) - Tüm kamu kurumları (İ)

5.4 Ulusal Siber Güvenlik Altyapısının Güçlendirilmesi

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
5.	**Kritik Altyapılarda Bilgi Güvenliği Yönetimi Programı**	- Siber tehditlerin doğrudan hedefi haline gelen ve zarar görmesi halinde toplum düzenini bozabilecek kritik altyapıların tespit edilmesi	Şubat 2013	- TÜBİTAK (S) - Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (İ)
		- Belirlenecek bir kritik altyapının sektörel risk analizinin yapılması	Mayıs 2013	
		- Sektörel risk analizi yöntemlerinin belirlenmesi	Eylül 2013	- Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (S) - TÜBİTAK (İ) - USOM (İ)
		- Sektörel acil eylem planlarının gereksinimlerinin belirlenmesi	Şubat 2014	
		- Yıllık risk analizi raporlama çalışmalarının ilkinin tamamlanması	Mart 2014	
		- Sektörel iş sürekliliği planlarının gereksinimlerinin belirlenmesi ve uygulanması	Mart 2014	
		- Sektörel güvenlik önlemlerinin belirlenmesi ve uygulanması	Sürekli	

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
6.	**Kamu Bilgi Güvenliği Programı**	- Kamu kurumlarının uyması gereken asgari güvenlik kriterleri dokümanının hazırlanması	Mayıs 2013	- TÜBİTAK (S) - Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (İ) - USOM (İ)
		- Sistem yöneticilerine ve ilgili diğer teknik personele öncelikli ihtiyaçlar uyarınca periyodik siber güvenlik eğitimlerinin ilkinin verilmesi, eğitim alan personelin yeterliliklerinin tespiti	Mayıs 2013	
		- Kurum bazında yapılması zorunlu kılınacak yıllık güvenlik test ve denetimlerinin ilkinin, önceliklendirilecek kamu kurumları için ilgili kurumlarla mutabakat sağlanarak gerçekleştirilmesi	Aralık 2013	
		- Bilişim sistemleri güvenliğine ilişkin sıkılaştırma dokümanları ve standartların yayınlanması ve güncellenmesi	Sürekli	- TÜBİTAK (S)

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
7.	**Siber güvenlik eğitim altyapısının güçlendirilmesi**	- Kurumların bilgi sistemlerinden ve siber güvenliğinden sorumlu üst düzey yöneticilerin bilgilendirilmesi	Mart 2013	- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) - TÜBİTAK (İ) - Devlet Personel Başkanlığı (İ)
		- Teknik personelin eğitilmesi ve eğitime katılan personele sertifika verilmesi - Kamu kurum ve kuruluşlarında çalışan iç denetim birimi personeline bilişim sistemleri denetimi yeteneği kazandırılacak eğitimlerin verilmesi	Mayıs 2014	

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
8.	**Siber güvenlik tatbikatları düzenlenmesi**	- Ulusal niteliğe sahip siber güvenlik tatbikatlarının düzenlenmesi	2013'ten itibaren iki yılda bir düzenlenecektir.	- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) - İçişleri Bakanlığı (İ) - Bilgi Teknolojileri ve İletişim Kurumu (İ) - Emniyet Genel Müdürlüğü (İ) - Jandarma Genel Komutanlığı (İ) - Genelkurmay Başkanlığı (İ) - TÜBİTAK (İ) - USOM (İ) - Sektörel SOME'ler (İ)
		- Ülkemiz liderliğinde Uluslararası Siber Güvenlik Tatbikatlarının ilkinin düzenlenmesi	Mayıs 2014	- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) - Dışişleri Bakanlığı (İ) - Bilgi Teknolojileri ve İletişim Kurumu (İ) - Emniyet Genel Müdürlüğü (İ) - Genelkurmay Başkanlığı (İ) - TÜBİTAK (İ)

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
9.	**Kamu Güvenli İletişim Kurallarının Belirlenmesi**	- Kamu kurumları arasında güvenli veri paylaşımını sağlamak üzere kuralların ve prosedürlerin belirlenmesi	Aralık 2013	- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) - USOM (İ) - Bilgi Teknolojileri ve İletişim Kurumu (İ) - Kamu Düzeni ve Güvenliği Müsteşarlığı (İ) - TÜBİTAK(İ)
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 (İ) - Türk Standardları Enstitüsü (İ)
		- Kritik altyapılar için geliştirilen yazılımlar için güvenli yazılım geliştirme temel kurallarının yayımlanması	Aralık 2013	
		- Kritik altyapılar için geliştirilen yazılımların güvenlik değerlendirmeleri için ilgili kurumların bünyesinde gerekli teknik altyapının kurulmasına yönelik fizibilitenin hazırlanarak Siber Güvenlik Kuruluna sunulması	Mart 2014	

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
11.	**Siber Tehditleri Önleme Projesinin yürütülmesi**	- Siber tehditleri tespit amacıyla balküpü sistemi kurulması	Temmuz 2013	- Bilgi Teknolojileri ve İletişim Kurumu / Telekomünikasyon İletişim Başkanlığı (S) - Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (İ) - TÜBİTAK (İ)
		- Ulusal siber saldırı raporlama sisteminin kurulması ve geliştirilmesi	Aralık 2013	
		- Siber tehditlerle ilgili yıllık istatistik üretilmesi	Aralık 2013	
		- Siber tehditlerin tespit edilmesi, izlenmesi ve önlenmesine ilişkin gerekli mekanizmaların geliştirilmesi	Aralık 2014	
12.	**Siber güvenlik konusunda ürünlerin ve hizmet sağlayıcıların akredite edilmesi**	- Bilgi sistemlerinin güvenlik testlerini yapan, siber güvenlik konusunda eğitim ve danışmanlık veren, siber güvenlik konusunda belirlenecek diğer alanlarda hizmet sunan gerçek ve tüzel kişilerde bulunması gereken asgari özelliklerin belirlenmesi ve belgelendirme sürecinin tasarlanması	Mayıs 2013	- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) - TÜBİTAK (İ)

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
12.	**Siber güvenlik konusunda ürünlerin ve hizmet sağlayıcıların akredite edilmesi**	- Kamu kurumları tarafından kullanılan ve siber güvenlik açısından kritik öneme sahip bilgi teknolojileri ve bilgi sistemleri ürünlerinin ve bunların sahip olması gereken asgari güvenlik gereksinimlerinin belirlenmesi	Ağustos 2014	- Türk Standardları Enstitüsü (S) - Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (İ) - TURKAK (İ) - TÜBİTAK (İ)
13.	**Adli bilişim konusunda hizmet sağlayıcılara güvenlik belgesi verilmesine yönelik kuralların belirlenmesi**	- Adli bilişim ile ilgili hizmet sunan gerçek ve tüzel kişilerde bulunması gereken asgari özelliklerin belirlenmesi ve belgelendirme sürecinin tasarlanması	Mayıs 2014	- Adalet Bakanlığı (S) - İçişleri Bakanlığı (İ) - Emniyet Genel Müdürlüğü (İ) - Jandarma Genel Komutanlığı (İ)

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
14.	**İş sürekliliği ve veri yedekleme sistemleri kurulması**	- Kamu kurum ve kuruluşlarının ve kritik bilgi sistem altyapılarını işleten özel sektör kuruluşlarınınhassas verilerinin yedeklenme usul ve esaslarının belirlenmesi	Ağustos 2013	- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) - TÜBİTAK (İ) - Tüm kamu kurum ve kuruluşları (İ) - Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar (İ)
		- Kamu kurumlarının ve kritik bilgi sistem altyapılarını işleten özel sektör kuruluşlarının elektronik ortamda işlem yapan sistemlerinin ve verilerinin güvenlik risk seviyelerinin belirlenmesi	Eylül 2013	
		- Tüm kamu kuruluşları ve kritik bilgi sistem altyapılarını işleten özel sektör kuruluşları tarafından iş sürekliliği planları yapılması	Aralık 2013	
		- İş sürekliliği planları gereği bilişim sistemlerinin kurulması	Temmuz 2014	
		- İş sürekliliği planlarına uygun tatbikatların düzenlenerek sonuçlarının Siber Güvenlik Kuruluna sunulması	Aralık 2014	

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
15.	**Kamu kurum ve kuruluşlarının internet sayfalarının yerli veri merkezlerine taşınması**	- Kamu kurumlarının internet sitelerinin yerli ve güvenilir bir veri merkezinde tutulmasını teminen veri merkezi hizmeti sunacak kuruluşun veya kuruluşların belirlenmesi	Haziran 2013	- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) - Bilgi Teknolojileri ve İletişim Kurumu (İ) - TÜBİTAK (İ)
		- İnternet sayfalarını kendi bünyesinde barındırmayan belediyeler, hastaneler, il/ilçe kamu birimleri gibi kamu kurumlarının internet sitelerini belirlenen veri merkezine/merkezlerine taşıması	Aralık 2013	- Tüm kamu kurum ve kuruluşları (S)
		- Belirlenen veri merkezlerinin güvenlik denetimlerinin düzenli olarak yapılması	Sürekli	- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S)
16.	**Veri sızmasını tespite yönelik test altyapısı geliştirilmesi ve uygulamaya alınması**	- Kritik kurumlardan veri sızmasını tespit edecek analiz altyapısı geliştirilmesi	Aralık 2013	- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) - TÜBİTAK (İ)
		- Siber Güvenlik Kurulu tarafından bu test altyapısının uygulanacağı kurumların tespit edilmesi	Ocak 2014	
		- Veri sızma tespitine yönelik testlerin yapılması ve sonuçlarının raporlanması	Mayıs 2014	

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
17.	**Kamu kurumlarında verilere erişim düzeylerinin belirlenmesi**	- Uluslararası standartlarla (örn. TS ISO/IEC 27001) uyumlu erişim kontrol prensiplerinin oluşturulması	Ağustos 2013	- Siber Güvenlik Kurulu (S) - Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (İ) - TÜBİTAK (İ) - Tüm kamu kurum ve kuruluşları (İ)
		- Kamu e-devlet uygulamalarının internet üzerinden yetkisiz veriye erişimi engelleyecek şekilde tekrar düzenlenmesi	Aralık 2013	
18.	**Açık kaynak kodlu ürünlerin kullanımının teşvik edilmesi**	- Kamu ve özel sektör kurumlarının kullanabileceği, belirlenmiş asgari güvenlik kriterlerini sağlayan açık kaynak kodlu mevcut güvenlik ürünleri hakkında bilgilendirme yapılması	Ağustos 2013	- TÜBİTAK(S) - Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (İ) - Üniversiteler (İ)
		- Açık kaynak kodlu yeni siber güvenlik ürünlerinin geliştirilmesi için platformların oluşturulması	Aralık 2013	
		- Uygun kritik bilişim sistemlerinin açık kaynak kodlu işletim sistemlerine taşınması için planlama yapılması	Mart 2014	

5.5 Siber Güvenlik Alanında İnsan Kaynağının Yetiştirilmesi ve Bilinçlendirme Faaliyetleri

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
19.	**Siber güvenlik konusunda akademisyen yetiştirilmesi**	- Siber güvenlik konusunda doktora ve yüksek lisans yapmaları için öğrencilere burs verilmeye başlanması	Ağustos 2013	- Yükseköğretim Kurulu Başkanlığı (S) - Milli Eğitim Bakanlığı (İ) - TÜBİTAK (İ) - Üniversiteler (İ)
20.	**Üniversitelerde siber güvenlik eğitimlerinin yaygınlaştırılması**	- Siber güvenlik altyapısının geliştirilmesi ile ilgili YÖK'te bir komisyonun kurulması	Mart 2013	- Yükseköğretim Kurulu Başkanlığı (S) - TÜBİTAK (İ) - Üniversiteler (İ)
		- İlgili branşların lisans, yüksek lisans ve doktora seviyesi müfredatlarına siber güvenlik ile ilgili derslerin eklenmesi	Aralık 2013	
		- Siber güvenlik alanında Türkçe kitap, dergi, makale kaynakların çoğaltılması	Sürekli	
		- En az iki siber güvenlik yüksek lisans programının açılması	Eylül 2013	
		- En az bir siber güvenlik doktora programının açılması	Eylül 2014	

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) 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 (İ) - TÜBİTAK (İ) - Üniversiteler (İ)
		- Siber güvenlik konusunda yaz kampları düzenlenmesi	2013'den itibaren her yıl 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 İlgili (İ) Kuruluşlar
21.	**Siber güvenlik uzmanlığına yönlendirme programının yürütülmesi**	- Üniversiteler arası siber savunma yarışmalarının düzenlenmesi	Her yıl düzenlenecektir	- TÜBİTAK (S) - Yükseköğretim Kurulu Başkanlığı (İ)
		- İlk, orta, lise ve üniversite kategorilerinde bilgi güvenliği bilinçlendirme video/poster yarışmaları düzenlenmesi	Her yıl düzenlenecektir	- Milli Eğitim Bakanlığı (S)
		- USAM ve SOME'lerde çalışan uzmanların eğitim alması ve uygulama deneyimi kazanması	Sürekli	- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) - Bilgi Teknolojileri ve İletişim Kurumu (İ) - USOM (İ) - SOME'ler (İ)
		- Siber güvenlik olaylarına müdahale edecek güvenlik birimlerinin kapasitelerinin artırılması, uzmanların eğitimi ve uzmanlara uygulama deneyimi kazandırılması	Sürekli	- İçişleri Bakanlığı (S) - TÜBİTAK (İ)

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
22.	**İlk, orta ,lise öğretimi ve yaygın eğitimde siber güvenlik eğitimlerinin yaygınlaştırılması**	- Meslek liselerinin bilgisayar programcılığı bölümlerinin müfredatına siber güvenliğin eklenmesi - Bilişim teknolojileri alanı altında yer alan kurs programları arasında siber güvenlik konusuna yer verilmesi - FATİH Projesi kapsamına siber güvenlik eğitimlerinin dâhil edilmesi - Bilgi teknolojileri eğitimlerinde açık kaynak kodlu ürünlerin de yer alması	Eylül 2013	- Milli Eğitim Bakanlığı (S) - TÜBİTAK (İ) - Bilgi Teknolojileri ve İletişim Kurumu (İ)
23.	**Bilgisayar kullanıcılarının siber güvenlik konusunda bilinçlendirilmesi**	- Bilgisayar kullanıcıların siber güvenlik konusunda bilinç düzeyinin artırılması için çalışmalar yapılması (seminerler, broşürler, yaygın eğitim faaliyetleri, basın ve yayın organları aracılığı ile uzaktan eğitim ve bilinçlendirme)	Sürekli	- Bilgi Teknolojileri ve İletişim Kurumu (S) - Milli Eğitim Bakanlığı (İ) - Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (İ) - Radyo ve Televizyon Üst Kurulu (İ)
		- İnternetin güvenli kullanımı ve "güvenli internet hizmeti" konusunda bilinç düzeyinin artırılması, söz konusu hizmetin geliştirilmesi ve yaygınlaştırılması	Sürekli	

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
24.	**Ulusal ve uluslararası siber güvenlik etkinlikleri düzenlenmesi**	- Siber güvenlik ile ilgili olarak, konunun ekonomik, sosyal ve hukuki boyutlarını da ele alacak şekilde konferans ve sempozyumlar düzenlenmesi - Siber güvenlik konulu uluslararası konferans, toplantı, seminer ve tatbikat çalışmalarına katılımın sağlanması	Sürekli	- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) - Dışişleri Bakanlığı (İ) - Bilgi Teknolojileri ve İletişim Kurumu (İ) - TÜBİTAK (İ) - Tüm kamu kurum ve kuruluşlar (İ) - Üniversiteler (İ) - STK'lar (İ)

5.6 Siber Güvenlikte Yerli Teknolojilerin Geliştirilmesi

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
25.	**Ar-Ge faaliyetlerinin teşvik edilmesi**	- Ülkenin siber güvenlik ihtiyacını karşılayacak teknolojilerin listesinin oluşturulması	Aralık 2012	- Bilim ve Teknoloji Yüksek Kurulu (S) - Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (İ) - Bilim, Sanayi ve Teknoloji Bakanlığı (İ) - TÜBİTAK (İ)
		- Mevcut proje teşvik sistemleri içerisine siber güvenliğin öncelikli konu olarak dâhil edilmesi	Eylül 2013	
		- Siber güvenlik ile ilişkili yazılım, donanım ve benzeri bilişim teknolojisi ürünlerine yönelik ulusal Ar-Ge faaliyetleri teşvik mekanizmalarının oluşturulması	Aralık 2013	
26.	**Siber güvenlik konusunda Ar-Ge laboratuarlarının kurulması**	- Zararlı yazılımları ve bu yazılımların bilişim sistemlerinde yaptığı etkileri belirleyebilecek laboratuar altyapısının kurulması	Eylül 2013	- TÜBİTAK (S)

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
26.	**Siber güvenlik konusunda Ar-Ge laboratuarlarının kurulması**	- Üniversitelerde siber güvenlik konusunda Ar-Ge laboratuarlarının kurulmasını teşvik edecek ve destekleyecek programların oluşturulması	Aralık 2013	- Yükseköğretim Kurulu Başkanlığı (S) - Kalkınma Bakanlığı (İ) - Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (İ) - Bilim, Sanayi ve Teknoloji Bakanlığı (İ) - TÜBİTAK (İ)
		- Üniversitelerde program kapsamında ilk siber güvenlik Ar-Ge laboratuarının kurulması	Eylül 2014	
27.	**Siber güvenlikte yerli ürün ve çözüm çalışmaları**	- Kamu ve özel sektör, üniversite, sivil toplum kuruluşu ve benzeri tüm bilgi güvenliği paydaşlarının katılacağı düzenli çalışmalar yapılması - Katılımcılarının, bilgi teknolojileri ürünlerinin siber güvenlik kapsamında doğru kullanımı, teknolojik önlemler ve gereksinimler, Ar-Ge gereksinimleri, geliştirilmekte olan BT ürünleri ile idari önlemler ve mevzuat konularında işbirliği yapması	Haziran 2013	- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (S) - Bilgi Teknolojileri ve İletişim Kurumu (İ) - TÜBİTAK (İ) - Üniversiteler (İ) - STK'lar (İ)

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
28.	**Yerli ürünlerin teşvik edilmesi**	- Kurumların bilgi ve iletişim sistemlerinde, a. Yerli olarak geliştirilmiş, güvenlik değerlendirmesi ve sertifikalandırması gerçekleştirilmiş ürünleri tercih etmeleri, b. Yerli ürünlerin mevcut olmadığı durumlarda güvenlik değerlendirmesi ve sertifikalandırması gerçekleştirilmiş ürünleri tercih etmeleri için teşvik mekanizmaları oluşturulması	Aralık 2013	- Bilim, Sanayi ve Teknoloji Bakanlığı (S) - Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (İ) - Kalkınma Bakanlığı (İ) - Gümrük ve Ticaret Bakanlığı (İ) - Ekonomi Bakanlığı (İ) - Maliye Bakanlığı (İ) - Kamu İhale Kurumu (İ)

5.7 Ulusal Güvenlik Mekanizmalarının Kapsamının Genişletilmesi

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
29.	**Ulusal siber güvenliğin milli güvenliğe entegrasyonu**	- Siber ortamda çeşitli siber güvenlik olayları meydana geldiğinde kurumların sorumluluklarının ve ulusal düzeyde koordinasyonun nasıl sağlanacağının belirlenmesi	Eylül 2013	- Siber Güvenlik Kurulu (S) - İçişleri Bakanlığı (İ) - Milli Savunma Bakanlığı (İ) - Adalet Bakanlığı (İ) - Milli Güvenlik Kurulu Genel Sekreterliği (İ) - Genelkurmay Başkanlığı (İ) - Milli İstihbarat Teşkilatı Müsteşarlığı (İ) - Kamu Düzeni ve Güvenliği Müsteşarlığı (İ) - Emniyet Genel Müdürlüğü (İ) - Jandarma Genel Komutanlığı (İ)
		- Ülkemizi hedef alan olası saldırı senaryolarının ve bunların yaratabileceği etkilerin belirlenmesi	Aralık 2013	
		- Siber ortamda meydana gelebilecek çeşitli olaylarda devreye girecek mekanizmaların mevcut durumunun analizi ve iyileştirilmeleri için gerçekleştirilmesi gereken öncelikli eylemlerin belirlenmesi	Mart 2014	

[Bu sayfa boş bırakılmıştır.]