2016 2019

ULUSAL SİBER GÜVENLİK STRATEJİSİ

T.C.
Ulaştırma Denizcilik ve
Haberleşme Bakanlığı

T.C.
Ulaştırma Denizcilik ve
Haberleşme Bakanlığı

T.C.
Ulaştırma Denizcilik ve Haberleşme Bakanlığı

2016-2019
ULUSAL SİBER GÜVENLİK STRATEJİSİ

T.C.
Ulaştırma Denizcilik ve
Haberleşme Bakanlığı

İÇİNDEKİLER

T.C.
Ulaştırma Denizcilik ve
Haberleşme Bakanlığı

1 Giriş

Bilgi ve iletişim teknolojileri toplumun ve ekonominin ayrılmaz bileşenleri olmuştur ve kalkınmaya önemli katkı sağlamaktadır. Ülkemizde bilgi ve iletişim sistemlerinin kullanımı kamu kurumlarında, özel sektörde ve vatandaşlara ilave olarak; enerji, su kaynakları, sağlık, ulaşım, haberleşme ve finansal hizmetler gibi kritik altyapı sektörlerinde faaliyet gösteren kurum ve kuruluşlarda da hızla yaygınlaşmaktadır. Bilgi ve iletişim teknolojileri ve özellikle de internet kullanımı siber uzaydaki tüm bileşenlerin birbiriyle bağlantılı olmasını ve bununla birlikte de siber güvenlik risklerini ve belirsizlikleri beraberinde getirmektedir.

Kurum ve kuruluşlarımızın 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 saldırılar dolayısı ile ortaya çıkan maddi zarar olağanüstü boyutlara ulaşmıştır. Hem Dünya Ekonomik Forumunun, hem de güvenlik firmalarının raporları bu gerçeği açıkça ortaya koymaktadır.

Siber uzayın bilişim sistemlerine ve bilgi/veriye yapılan saldırılar için anonimlik ve inkâr edilebilirlik gibi fırsatları sunduğu bir gerçektir. Bilişim sistem ve verilerini hedef alan ısrarcı ve gelişmiş siber saldırıların kimler tarafından finanse ve organize edildiğinin tespiti ise zordur. Bu durum ve özellikler siber uzaydaki risk ve tehditlerin asimetrik karakterini ortaya koymakta, tehditlerle mücadeleyi güçleştirmektedir.

Böyle bir ortamda artık siber güvenliğin mutlak olarak sağlanmasından bahsedilmemekte, bunun yerine siber güvenlik risklerinin yönetilebilir ve kabul edilebilir düzeylerde tutulması hedeflenmektedir. İnternet gibi açık ve bağlantılı bir ortamda bulunmanın artan erişilebilirlikle birlikte bazı riskleri de getireceği kabul edilmektedir. Bu risklerin tüm paydaşları içeren bütüncül bir yaklaşımla yönetilerek siber olaylara karşı hazırlıklı olunması ve bu olaylardan en az zararla çıkılarak sürekliliğin temini esas alınmalıdır.

1.1 Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı

Tüm bu bilgiler ışığında, 20/10/2012 tarih, 28447 sayılı Resmi Gazetede yayınlanan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı" ve 5809 sayılı Elektronik Haberleşme Kanunu gereğince ulusal siber güvenliğin sağlanmasına ilişkin politika, strateji ve eylem planlarını hazırlamak ve koordinasyonunu sağlamak görevi Ulaştırma, Denizcilik ve Haberleşme Bakanlığına verilmiştir.

Bütün kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler, Siber Güvenlik Kurulu (Ek-A) tarafından belirlenen politika, strateji ve eylem planları çerçevesinde kendilerine verilen görevleri yerine getirmek ve belirlenen usul, esas ve standartlara uymakla yükümlüdür.

Bu kapsamda hazırlanan, 2013-2014 döneminde gerçekleştirilmesi planlanan işlere ilave olarak bu yılları aşan periyodik faaliyetler ile eğitim ve bilinçlendirme çalışmaları gibi sürekli yürütülmesi gereken faaliyetlere de yer veren Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı 20/06/2013 tarih, 28683 sayılı Resmi Gazete'de yayınlanarak yürürlüğe girmiştir.

1.2 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planının Hazırlık Süreci

Gelişen bilgi ve iletişim teknolojileri, artan güvenlik gereksinimi ve edinilen tecrübeler doğrultusunda, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından ulusal siber güvenlik stratejisinin güncellenmesi ve 2016-2019 dönemini kapsayan eylemlerin belirlenmesi ihtiyacı doğmuştur. Bu kapsamda öncelikle eski eylem planında sorumlu veya ilgili olarak yer alan kurumlarla 10 Mart - 7 Nisan 2015 tarihlerinde yedi adet değerlendirme toplantısı yapılmıştır. Toplantılarda eski eylem planında yer alan faaliyetlerin gerçekleşme dereceleri ve karşılaşılan güçlüklere ek olarak ileriye dönük değerlendirmeler ve siber güvenlik kapsamında gerçekleştirilmesi gereken faaliyetler de detaylı olarak belirlenmiş ve kaydedilmiştir.

Toplantıların ardından kamu kurumları, kritik altyapı işletmecileri, bilişim sektörü, üniversiteler ve sivil toplum kurumlarını temsilen 73 kurum ve kuruluştan toplam 126 uzmanın katılımı ile Ortak Akıl Platformu gerçekleştirilmiştir. İki gün süren platform çalışmaları kapsamında; Türkiye'nin siber güvenlik boyutunda güçlü ve zayıf yönlerinden hareketle stratejik amaçları ve gerçekleştirmesi gereken eylemler belirlenmiştir.

Siber Güvenlik konusu özellikle 2008 yılından itibaren AB (Avrupa Birliği), OECD (Ekonomik İşbirliği ve Kalkınma Teşkilatı), NATO (Kuzey Atlantik İttifakı) gibi uluslararası kuruluşlara ilave olarak tüm gelişmiş ülkelerin gündemine girmiştir. 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı hazırlanırken paydaşlarla birlikte gerçekleştirilen çalışmalara ilave olarak geri planda kaynak taraması da yapılmış, Amerika, Avrupa ve Uzak Doğu'dan çok sayıda ülkenin siber güvenlik stratejileri gözden geçirilmiş, ülkelerin siber güvenlik alanında kapsam, hedefler, öncelikler, organizasyon yapısı, kaynak tahsisi, Ar-Ge (Araştırma ve Geliştirme) koordinasyonu, kamu-özel sektör işbirliği, eğitim gibi başlıklarda üretmeye çalıştığı çözümler değerlendirilmiştir.

Tüm bu çalışmalar kapsamında üretilen bilginin toplanması, incelenmesi ve değerlendirilmesi sonucunda "2016-2019 Ulusal Siber Güvenlik Stratejisi" ve "2016-2019 Ulusal Siber Güvenlik Eylem Planı" hazırlanmıştır.

1.3 Tanımlar

Bu belgede geçen kavramlardan,

Tehdit: Bir kurumun veya sistemin zarar görmesi ile sonuçlanabilecek istenmeyen bir olayın potansiyel nedenini,

Risk: Tehditlerin bir veya birden çok bilgi varlığındaki açıklığı kullanarak zarar yaratma potansiyelini,

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

Endüstriyel Kontrol Sistemleri: Geleneksel bilişim teknolojileri dışında, programlanabilir mantıksal denetleyiciler aracılığı ile üretim, ürün işleme ve dağıtım kontrolleri gibi endüstriyel işlemler için kullanılan, SCADA (Supervisory Control and Data Acquisition) ve Dağınık Kontrol Sistemleri şeklinde gruplanan bilgi sistemlerini,

Siber uzay: Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal 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 uzay: Kamu bilişim sistemleri ile gerçek ve tüzel kişilerce işletilen/kullanılan bilişim sistemlerinden oluşan ortamı,

Gizlilik: Bilginin yetkisiz kişiler, varlıklar ya da süreçlere kullanılabilir yapılmama ya da açıklanmama özelliğini,

Bütünlük: Varlıkların doğruluğunu ve tamlığını koruma özelliğini,

Erişilebilirlik: Yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliğini,

Kritik hizmet: Verilememesi halinde,

- Can kaybına,
- Büyük ölçekli ekonomik zarara,
- Ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek hizmetleri,

Kritik ürün: Kritik hizmetlerin gizlilik, bütünlük ve erişilebilirliğini sağlayan bilgi teknolojisi ürünlerini,

Kritik altyapılar: İşlediği bilgi/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda,

- Can kaybına,
- Büyük ölçekli ekonomik zarara,
- Ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapıları,

Kritik altyapı sektörleri: 20/06/2013 tarih, 2 sayılı Siber Güvenlik Kurulu kararı uyarınca kritik altyapıları barındırmakta olan "Elektronik Haberleşme", "Enerji", "Su Yönetimi", "Kritik Kamu Hizmetleri", "Ulaştırma" ve "Bankacılık ve Finans" sektörlerini,

Kurum: Kamu kurumları ve kritik altyapı işleten kamu ya da özel sektör kuruluşlarını,

Siber olay: Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilgi/verinin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya teşebbüste bulunulmasını,

Siber saldırı: Ulusal siber uzayda bulunan bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın her hangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemleri,

Sınır güvenliği: Bilişim sistemlerinin güvenlik duvarı ve saldırı engelleme sistemleri gibi erişim kontrolü sağlayan sistemler aracılığı ile dış ağlardan gelebilecek saldırılardan korunmasını,

Siber güvenlik: Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilgi/verinin 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 uzayı oluşturan bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmet, işlem, bilgi/verinin ve bunların sunumunda yer alan donanım ve yazılım sistemlerinin ulusal ölçekte sağlanan siber güvenliğini, ifade eder.

1.4 Misyon

Ulusal siber güvenliğin sağlanması amacıyla, etkin ve sürdürülebilir politikaları belirlemek, koordinasyonu sağlamak ve uygulanmasını gerçekleştirmektir.

1.5 Vizyon

Toplumun refahı ve güvenliği ile ülke ekonomisinin büyümesine ve verimliliğine katkı sağlamak üzere bilgi ve iletişim teknolojilerinden en etkin şekilde faydalanılabilmesi için, siber güvenlikle ilgili tüm paydaşların işbirliği içinde siber uzaydaki riskleri yetkin bir biçimde yönettikleri, siber güvenlik alanında uluslararası rekabet gücüne sahip bir eko-sistemin oluşmasıdır.

1.6 Amaç

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planının ana amacı; siber güvenliğin ulusal güvenliğin ayrılmaz bir parçası olduğu anlayışının tüm kesimlerde yerleşmesi, ulusal siber uzayda bulunan sistem ve paydaşların tamamının güvenliğini sağlamak üzere idari ve teknolojik önlemlerin alınmasını sağlayacak yetkinliğin eksiksiz bir şekilde kazanılmasıdır. Bu ana amacı gerçekleştirmek üzere, hedeflerin ve alt eylem maddelerinin belirlenmesi, bunların gerçekleştirilmesinin sağlanması ve denetlenmesi de bu dokümanın amaçlarındandır.

Bu amaçlar doğrultusunda:

- Ulusal siber uzayın tamamını kapsamak şartıyla, bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve bilgi/veri ile bunların sunumunda kullanılan sistemlerin güvenliğinin, gizliliğinin ve mahremiyetinin 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 kolluk kuvvetlerince daha etkin araştırılmasının ve soruşturulmasının sağlanmasına,
- Siber güvenliğin, gizliliğin ve mahremiyetin sağlanmasında kritik teknolojilerin ve ürünlerin ülkemizde üretilmesine, üretilemiyorsa, dışarıdan alınan teknoloji ve ürünlerin salt bu maksatla ve güvenle kullanılabilmesini sağlayacak önlemlerin alınmasına

yönelik bileşenler bu planda yer almaktadır.

1.7 Kapsam

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, kamu bilişim sistemlerine ve kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerine ilave olarak küçük ve orta ölçekli sanayi, tüm özel ve tüzel kişiler de dâhil olmak üzere ulusal siber uzayın ülkemiz ölçeğindeki bütün bileşenlerini kapsar.

1.8 Güncelleme

Ulusal Siber Güvenlik Stratejisi gelişen teknoloji, değişen koşullar ve gereksinimler göz önünde bulundurularak, kamu ve özel sektörden gelecek talepler doğrultusunda, ulusal düzeyde sağlanacak eşgüdüm ile güncellenecektir.

Bu eylem planında yer alan ve 2019 sonunda tamamlanmayan eylemler bir sonraki eylem planına aktarılacaktır.

1.9 Dünyada Siber Güvenlik Stratejileri ve Eylem Planları

Bu bölümde farklı ülkeler tarafından yayınlanan Siber Güvenlik Strateji dokümanlarında dikkat çeken hususlara yer verilmiştir.

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında olduğu gibi diğer ülkelerin strateji dokümanlarında da olası siber güvenlik risklerine ve riskleri ortadan kaldıracak eylemler uygulanırken göz önünde bulundurulacak ilkelere yer verilmekte, risklerin ve ilkelerin ülkeden ülkeye çok fazla değişiklik arz etmediği gözlemlenmiştir.

Bu kapsamda dikkat çeken ilkeler şunlardır:

a. Siber güvenliğin sağlanmasında birey, kurum, toplum ve devletin tüm hukuki ve sosyal sorumluluklarını yerine getirmeleri,

b. Kamu, özel sektör, üniversiteler ve sivil toplum örgütleri koordinasyonu, müşterek katılım, iş birliği ve bilgi paylaşımı,

c. Uluslararası Siber Güvenlik Operasyon Merkezleri arasında gelişmiş siber olay yönetimi işbirliği.

İncelenen dokümanlarda dikkat çeken riskler ise şunlardır:

a. Toplumun sosyal ağlara bağımlılığı,

b. Kritik kurum ve kuruluşların siber uzaydaki konumları,

c. Çeşitli siber casusluk çalışmaları ve hedefli saldırılar,

ç. Personel ve yetkinlik bağlamında yetersizlik,

d. Kurumlar arası koordinasyon eksikliği,

e. Siber uzayda faaliyet gösteren farklı ölçeklerdeki sektörlere yönelik ekonomik kaygılar.

Bu ilkeler ve riskler de göz önünde bulundurularak ulusal siber güvenlik ilkeleri, riskleri, stratejik siber güvenlik amaçları ve eylem planı belirlenmiştir.

2 İlkeler

Ulusal siber güvenliğin sağlanmasında göz önünde bulundurulacak ilkeler şunlardır:

1. Siber güvenlik, risk yönetimini esas alan etkin ve sürekli değerlendirmeye ve iyileştirmeye dayalı yöntemler aracılığıyla sağlanır. Oluşturulan risk yönetimi metotlarının tehdit ve açıklıkları ele alarak bunlardan dolayı ortaya çıkacak riskleri belirlemesi, bu riskleri kabul edilebilir düzeye indirmek için yöntemler sunması hedeflenir.
2. Siber güvenliğin sağlanması için tüm paydaşların siber güvenlik risklerini bilmeleri, bu risklerin yönetilmesine ilişkin yaklaşımlarının kendileri kadar başkalarını da etkileyebileceğinin bilincinde olmaları gerekir. Bu farkındalık ve yetkinliğin sağlanması için tüm paydaşların gerekli eğitim ve deneyimi kazanmaları sağlanır. Teknik boyutun yanı sıra; hukuki, idari, ekonomik, politik ve sosyal boyutları da içeren bütüncül bir yaklaşım benimsenir.
3. Risk yönetimi, teknik zaafların hızla giderilmesini, saldırı ve tehditlerin önlenmesini, fark edilmesini, yanıtlanmasını ve muhtemel zararın en aza indirgenmesini içerir. Zararların asgari düzeyde tutulması için siber olaylara karşı bir hazırlık ve süreklilik planının bulunmasına ve uygulanmasına önem verilir.
4. Siber uzay güvenliğinin sağlanması ve sürdürülmesinde; kamu, özel sektör, üniversiteler, sivil toplum kuruluşları ve bireyler dâhil tüm paydaşlar arasında işbirliğinin yanı sıra uluslararası işbirliği ve bilgi paylaşımı esas kabul edilir ve güven inşa edilir.
5. Tüm paydaşlar, siber uzay güvenliğinin sağlanması için çalışırken, hukukun üstünlüğü, ifade özgürlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunması ilkelerini gözetir.
6. Paydaşlar siber uzaydaki risklerin yönetimi ile ilgili sorumluluklarını yerine getirirken şeffaflık, hesap verilebilirlik ve etik değerleri göz önünde bulundurur.
7. Alınan siber güvenlik önlemlerinin ilgili risklerle orantılı olması, olumlu ve olumsuz etkilerinin değerlendirilmesi ve dengelenmesi sağlanır.
8. Siber güvenlik gereksinimlerinin karşılanmasında yerli ürün ve hizmet kullanımı teşvik edilir, bunların geliştirilmesi için araştırma ve geliştirme projeleri desteklenir, yenilikçilik anlayışı esas kabul edilir.

3 Siber Güvenlik Riskleri

Siber güvenlik kapsamında stratejik amaçların en doğru şekilde tanımlanabilmesi için siber güvenlik riskleri gerçekçi bir biçimde değerlendirilmiş ve belirlenen başlıca riskler aşağıda sıralanmıştır:

1. Kritik altyapıların kullandığı bilişim sistemlerine yapılacak hizmet dışı bırakma ve benzeri hedef odaklı saldırılar sonucunda enerji, ulaştırma, vb. kritik hizmetlerin kesintiye uğraması.
2. Kamu ve kritik altyapıların kullandığı bilişim sistemlerine yapılacak hedefe yönelik saldırılar sonucunda; vatandaşa ait kişisel bilgilerin veya kamuya ait gizli bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi.
3. Araştırma, geliştirme ve üretim yapan kurum ve kuruluşların (özel firmalar, araştırma kurumları ve savunma sanayi) ticari sırlarını ve bilgi birikimini elde etmeye yönelik hedef odaklı saldırılar sonucunda hassas veya ticari değere sahip bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi.
4. Propaganda amaçlı bilgisayar korsanlığı (hacktivizm) saldırıları sonucu çeşitli kurum ve kuruluşların itibarının zarar görmesi veya hassas bilgi/verinin ifşa olması, değiştirilmesi veya yok edilmesi.
5. E-ticaret yapan kuruluşların, E-posta hizmeti veren kuruluşların, sosyal medya hizmeti veren kuruluşların hizmet dışı bırakma ve benzeri saldırılar sonucunda hizmet verememesi nedeniyle maddi kayba uğraması, sahte işlem kaydı oluşturulması, gizli bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi.
6. E-ticaret yapan kuruluşların, finans sektörü veya çevrimiçi ödeme ya da para transferine imkan veren diğer kuruluşların müşterilerine ait hassas bilgilerin saldırganlar tarafından ele geçirilmesi nedeni ile itibar kaybına uğraması, toplumda çevrimiçi işlemlere yönelik güven kaybı oluşması, bu hizmetlerden faydalanan müşterilerin maddi kayba uğraması.
7. Küçük ve orta ölçekli sanayi, ticaret ve hizmet sektöründeki kuruluşların faaliyetlerinin bilişim sistemlerindeki güvenlik önlemlerinin eksikliğinden veya kullanıcı hatalarından dolayı kesintiye uğraması, hassas veya ticari değere sahip bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi.

8. Toplumun internete ve sosyal ağlara olan bağımlılığı, siber güvenlik alanında yeterli düzeyde bilgi ve bilinç seviyesine sahip olmaması, mobil ve sabit bilgi sistemlerinde kişisel güvenlik önlemlerini almaması gibi nedenlerle kötücül yazılım ve oltalama saldırılarına, dolandırıcılık ve kimlik hırsızlığına maruz kalması, kişisel bilgilerin ve cihazların saldırganlar tarafından ele geçirilmesi, değiştirilmesi veya yok edilmesi, sahte işlem yapılması.
9. Her türlü kurum ve kuruluşta yığın posta, kötücül yazılım ve benzeri saldırılar sonucunda dolandırıcılıkla karşı karşıya kalınması.
10. Her türlü kurum ve kuruluşta, kullanıcı hataları ya da doğal afetler sonucunda bilişim sistemleri aracılığı ile verilen hizmet ve faaliyetlerin kesintiye uğraması.

4 Stratejik Siber Güvenlik Amaçları ve Eylemleri

2016-2019 döneminde, mevcut riskleri, belirlenen ilkeler ışığında asgari düzeye indirmeyi hedefleyen stratejik amaçlar şunlardır:

1. Ulusal kritik altyapı envanterinin oluşturulması, kritik altyapıların güvenlik gereksinimlerinin karşılanması ve bu kritik altyapıların bağlı oldukları düzenleyici kurumlar (Ek-B) tarafından denetlenmesi.
2. Siber güvenlik alanında denetim yaklaşımını da içeren uluslararası standartlara uygun mevzuatın oluşturulması.
3. Sektör düzenleyici kurum, bakanlık vb. kuruluşların siber güvenlik kapsamında düzenleme ve denetleme farkındalıklarının ve yetkinliklerinin geliştirilmesi.
4. Kurumların bilişim sistemlerinin sadece saldırılardan değil, kullanıcı hataları ve afetlerden de korunması için düzenlemelerin yapılması.
5. Her kurumun kendi bilgi güvenliği yönetim sürecini çalıştıracak yetkinliğe ulaşması.
6. Siber güvenlik konusunda kurum yöneticilerinin farkındalığının artırılması.
7. Siber güvenlik alanında yetkin personel yetiştirilmesi ve bu alanda uzmanlaşmak isteyen personel, araştırmacı ve öğrencilerin teşvik edilmesi.
8. Toplumun her kesiminde siber güvenlik bilincinin oluşturulması, eğitim kurumlarının çalışmalarına ilave olarak yazılı ve görsel medyada farkındalık çalışmalarının yapılması.
9. Kamu kurumlarında siber güvenlik alanında uzman personel istihdam edilmesi için mevzuat desteği sağlanması ve personelin özlük haklarının iyileştirilmesi.

10. Kurumsal ve Sektörel SOME'lerin (Siber Olaylara Müdahale Ekibi) (Ek-C) etkinliğinin arttırılması için mevzuat desteğinin sağlanması, mali düzenlemelerin yapılması, yetkin personel ihtiyacının karşılanması, bilişim altyapısının sağlanması ve ulusal siber olaylara müdahale organizasyonu kapsamında bilgi paylaşımının geliştirilmesi.
11. Siber güvenlik alanında koordinasyonu sağlayacak güçlü bir merkezi kamu otoritesi oluşturulması.
12. Kamu kurumları, özel sektör, STK'lar (Sivil Toplum Kuruluşu), denetleyici kurumlar, üniversiteler, geliştirici firmalar ve tüm diğer paydaşların katılım ve koordinasyon hedefi ile ulusal siber güvenlik eko-sisteminin oluşturulması.
13. Ulusal Siber güvenlik eko-sistemi içinde iyi örneklerin yaygınlaştırılması, danışmanlık hizmetlerinin verilmesi, açıklık, tehdit ve faydalı uygulamaların paylaşılması.
14. Bilişim sistemlerinin kritik noktalarında kullanılan, yerli veya yabancı donanım ve yazılım ürünlerinin içerdiği açıklıkların kötüye kullanılmasına engel olmak üzere açıklık analizi ve sertifikasyon çalışmalarının yapılması.
15. Güvenli yazılım geliştirme ve tedarik yönetimi kültürünün oluşturulması.
16. Siber güvenlikte dışa bağımlılığı azaltmak için Ar-Ge faaliyetlerine önem verilerek yerli ürünlerin geliştirilmesi.
17. Tehdit unsurlarının saldırı yapmadan önce bertaraf edilmesi için ulusal proaktif siber savunma yeteneğinin geliştirilmesi.
18. Tehdit unsurlarının siber uzaydaki en büyük avantajı olan anonimliği ortadan kaldırmak için etkin kayıt yönetimi ve IPv6 (Internet Protokolü sürüm 6) teknolojilerinin yaygınlaştırılması.

Önceki bölümde belirtilen stratejik amaçlara ulaşmak için gerçekleştirilecek eylemler beş stratejik eylem başlığı altında toplanmaktadır. Söz konusu stratejik eylem başlıkları eylemlere ayrılmış, planlanan bitirilme tarihlerine ve sorumlu/ilgili kuruluşlarına göre "2016-2019 Ulusal Siber Güvenlik Eylem Planı"nda listelenmiştir. 2016-2019 döneminde gerçekleştirilmesi planlanan stratejik eylemler aşağıdaki başlıklar altında gruplanmıştır:

4.1 Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması

Bu stratejik eylem kapsamında devleti ve ulusal ekonomiyi, kritik altyapıları ve toplumu etkileyebilecek riskleri azaltmaya dönük eylemlerin gerçekleştirilmesi planlanmaktadır.

4.2 Siber Suçlarla Mücadele

Bu stratejik eylem kapsamında kurumları ve bireyleri etkileyen, ağırlıklı olarak maddi kayba yol açan riskleri azaltmaya dönük eylemlerin gerçekleştirilmesi planlanmaktadır.

4.3 Farkındalık ve İnsan Kaynağı Geliştirme

Bu stratejik eylem kapsamında kurum yöneticilerinden bilgisayar kullanıcısı vatandaşa kadar toplumun tüm kesimlerine siber güvenlik kültürünün kazandırılmasına yönelik eylemlerin gerçekleştirilmesi ve siber güvenlik uzmanı yetiştirilmesi planlanmaktadır.

4.4 Siber Güvenlik Ekosisteminin Geliştirilmesi

Bu stratejik eylem kapsamında kamu, özel sektör, STK ve diğer paydaşların koordineli katkısıyla mevzuattan teknolojiye kadar gereksinimlerin belirlenmesine ve uygulamaya dökülmesine yönelik eylemlerin gerçekleştirilmesi planlanmaktadır.

4.5 Siber Güvenliğin Milli Güvenliğe Entegrasyonu

Bu stratejik eylem kapsamında devleti ve ulusal ekonomiyi, kritik altyapıları ve toplumu etkileyebilecek, iyi organize olmuş tehdit unsurları tarafından gerçekleştirilecek kasıtlı saldırıların verebileceği zararı azaltmaya dönük eylemlerin gerçekleştirilmesi planlanmaktadır.

EK - A: Siber Güvenlik Kuruluna Üye Kurumlar Listesi

1. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDHB)

2. Dışişleri Bakanlığı

3. İçişleri Bakanlığı

4. Milli Savunma Bakanlığı (MSB)

5. Kamu Düzeni ve Güvenliği Müsteşarlığı

6. Milli İstihbarat Teşkilatı (MİT)

7. Genelkurmay Başkanlığı

8. Bilgi Teknolojileri ve İletişim Kurumu (BTK)

9. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK)

10. Mali Suçları Araştırma Kurulu

11. Telekomünikasyon İletişim Başkanlığı (TİB)

EK - B: Düzenleyici ve Denetleyici Kurum Listesi

1. Bankacılık Düzenleme ve Denetleme Kurumu (BDDK)

2. Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı (BTK)

3. Enerji Piyasası Düzenleme Kurumu Başkanlığı (EPDK)

4. Hâkimler ve Savcılar Yüksek Kurulu Başkanlığı (HSYK)

5. İstanbul Tahkim Merkezi Başkanlığı

6. Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumu Başkanlığı

7. Kamu İhale Kurumu Başkanlığı (KİK)

8. Radyo ve Televizyon Üst Kurulu Başkanlığı (RTÜK)

9. Rekabet Kurumu Başkanlığı

10. Şeker Kurumu Başkanlığı

11. Sermaye Piyasası Kurulu Başkanlığı (SPK)

12. Türkiye Cumhuriyeti Merkez Bankası Başkanlığı (TCMB)

13. Tütün ve Alkol Piyasası Düzenleme Kurumu Başkanlığı (TAPDK)

14. Yüksek Seçim Kurulu Başkanlığı (YSK)

15. Yükseköğretim Kurulu Başkanlığı (YÖK)

EK - C: Sektörel SOME Listesi

Kritik Kamu Hizmetleri ve Su Yönetimi Sektörlerinde Sektörel SOME'ler

1. İçişleri Bakanlığı

2. Adalet Bakanlığı

3. Maliye Bakanlığı

4. Çevre ve Şehircilik Bakanlığı

5. Çalışma ve Sosyal Güvenlik Bakanlığı

6. Gıda, Tarım ve Hayvancılık Bakanlığı

7. Orman ve Su İşleri Bakanlığı

8. Sağlık Bakanlığı

Ulaştırma Sektöründe Sektörel SOME'ler

1. UDHB Karayolu Düzenleme Genel Müdürlüğü

2. UDHB Demiryolu Düzenleme Genel Müdürlüğü

3. UDHB Deniz ve İçsular Düzenleme Genel Müdürlüğü

4. UDHB Sivil Havacılık Genel Müdürlüğü

Elektronik Haberleşme, Enerji ve Finans Sektörlerinde Sektörel SOME'ler

1. Haberleşme Sektörü: Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı (BTK)

2. Finans Sektörü: Bankacılık Düzenleme ve Denetleme Kurumu Başkanlığı (BDDK)

3. Enerji Sektörü: Enerji Piyasası Düzenleme Kurumu Başkanlığı (EPDK)

4. Finans Sektörü: Sermaye Piyasası Kurulu Başkanlığı (SPK)

“Güvenli Bir Dünya İçin Siber Güvenlik”

T.C.
Ulaştırma Denizcilik ve Haberleşme Bakanlığı

T.C. ULAŞTIRMA DENİZCİLİK VE HABERLEŞME BAKANLIĞI
HABERLEŞME GENEL MÜDÜRLÜĞÜ
Hakkı Turayliç Caddesi No:5 Emek/ANKARA
www.udhb.gov.tr