ULUSAL SİBER GÜVENLİK STRATEJİSİ

2020-2023

T.C. ULAŞTIRMA VE ALTYAPI BAKANLIĞI

ULUSAL SİBER GÜVENLİK STRATEJİSİ

2020 - 2023

Milli birlik ve beraberlik içerisinde sürdürdüğümüz kalkınma ve büyüme yolundaki mücadelemizde teknoloji alanında yaşanan gelişmeler önemli bir yer tutuyor. Bu gelişmeler; ekonomiden sağlığa, eğitimden ulaşıma kadar kamu hizmetleri de dâhil olmak üzere hayatın her alanında büyük bir hızla gerçekleşiyor.

Sürekli gelişim ve değişim kaydeden, yaygınlaşarak yaşamımızın ayrılmaz bir parçası haline gelen bilgi ve iletişim teknolojileri bizlere birçok imkân sunarken siber güvenlik risklerini de beraberinde getiriyor. Siber tehditlere karşı, milli güvenliğimizin önemli bir parçası olan ulusal siber güvenliğimizin sağlanması en öncelikli konulardan biri haline gelmiş olup buna yönelik çalışmalarımızı büyük bir azimle sürdürmekteyiz. Bu çerçevede, ortaya çıkan ulusal ihtiyaçlar ile teknolojide yaşanan gelişmeler dikkate alınarak Ulaştırma ve Altyapı Bakanlığınca, kamu, özel sektör, sivil toplum kuruluşları ve üniversitelerle iş birliği içinde Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020 – 2023) hazırlanmıştır.

2023 hedeflerimiz doğrultusunda birçok alanda olduğu gibi siber güvenlik alanında da uluslararası seviyede ülkemizin öncü konumunu daha da ileriye taşıyacağız ve 7/24 görevinin başında olan siber güvenlik organizasyonumuzla birlikte yerli ve milli teknolojilerimizden de yararlanarak siber tehditlerle mücadeleye kararlılıkla devam edeceğiz.

Teknolojiyi güvenle kullanan, "Güçlü ve Büyük Türkiye" için...

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020 – 2023) milletimize ve ülkemize hayırlı olsun.

Recep Tayyip ERDOĞAN

Cumhurbaşkanı

Bilgi ve iletişim teknolojileri; bilgiye erişimi kolaylaştırmakta, gündelik yaşamı daha konforlu hale getirmekte, ekonomik ve sosyal hayat üzerinde giderek daha önemli etkiler oluşturmaktadır. Birçok önemli hizmet vatandaşlarımıza bu teknolojiler vasıtasıyla ulaştırılmakta, iş ve işlemler elektronik ortamda daha hızlı ve pratik biçimde gerçekleştirilmektedir. Hayatımızın her alanında yer edinen bilgi ve iletişim teknolojilerinin güvenli biçimde kullanılması da son derece kritik bir unsur olarak ortaya çıkmaktadır.

Bu kapsamda; etkin ve güçlü bir siber güvenlik anlayışı, ülkelerin ekonomik büyümesinde ve toplumsal refahın artırılmasında önemli rol oynamaktadır. Bugüne kadar, Ulaştırma ve Altyapı Bakanlığı olarak yayımladığımız, 2013-2014 ve 2016-2019 yıllarını kapsayan Ulusal Siber Güvenlik Stratejisi ve Eylem Planları ile önemli çalışmalar gerçekleştirilmiştir.

Sayın Cumhurbaşkanımızın ortaya koyduğu vizyon ve hedefler doğrultusunda; bilgi, tecrübe ve kapasite birikimini kesintisiz biçimde artırarak, siber güvenlik alanındaki kazanımları daha üst seviyelere taşımak için faaliyetlerimizi süreklilik içerisinde yürütme azmi ve kararlılığı içindeyiz. Bu kapsamda, ülke ekonomimizin geliştirilmesini, toplumsal yaşamın korunmasını ve milli güvenliğin sağlanmasını desteklemek ve siber güvenlikte uluslararası alanda marka haline gelmek hedefleriyle Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023) hazırlanmıştır.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023) kapsamında belirlenen hedefler ve eylemlerin ilgili kurum ve kuruluşlarca hayata geçirilmesi, tüm paydaşların etkin iletişimi ve iş birliği içerisinde faaliyetlerini yürütmesi ülkemizin siber güvenliğine büyük katkı sağlayacaktır.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023) kapsamında, ülkemizin ve milletimizin güvenliği için gerçekleştirilecek çalışmaların hayırlı olmasını temenni ediyor, hazırlık aşamasında emeği geçen herkese teşekkür ediyorum.

Adil KARAİSMAİLOĞLU

Ulaştırma ve Altyapı Bakanı

İÇİNDEKİLER

1. YÖNETİCİ ÖZETİ

Bilgi ve iletişim teknolojilerinin getirdiği avantajlardan en üst düzeyde faydalanmak, ulusal siber güvenliğe ilişkin faaliyetlerin etkin bir biçimde ve süreklilik içerisinde gerçekleştirilmesine bağlıdır. Yapısal olarak değişen, gelişen, karmaşıklaşan ve sayıları hızla artan siber tehditler karşısında vatandaşlarımızın, kurumlarımızın, sektörlerimizin, kısacası ulusal siber ortamımızın güvenliği, ülkemizin ekonomik büyümesinde de anahtar rol oynamaktadır. Ekonomik ve toplumsal yaşantıda gözle görülür değişimlerin ortaya çıktığı ve teknolojik dönüşüm dinamiklerinin hızlandığı küresel pandemi ve sonrasına ilişkin koşullar; altyapı, yeni teknolojiler, insan kaynağı ve farkındalık açısından siber güvenlikle ilgili gereksinimleri de artırmıştır.

Ulusal siber güvenlikte çıtanın her geçen gün daha da yukarıya çıkarılması güçlü ulusal stratejilerle mümkündür. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023), ülkemizin siber güvenlik alanındaki vizyonu ve misyonu doğrultusunda önümüzdeki 4 yıllık döneme ilişkin politikalarını konu almakta, bundan önce hayata geçirilen stratejilerde elde edilen kazanımların daha yukarı taşınmasını hedeflemektedir. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023), ulusal siber güvenliğimizi bir adım daha ileriye taşıyacak hamleleri yapmak ve buna yönelik faaliyetleri gerçekleştirmek üzere hazırlanmıştır. Bunun için teknolojik gelişmelerin etkileri, siber tehditlerde ortaya çıkan eğilimler, ulusal ihtiyaçlar ve uluslararası uygulamalar dikkatle incelenerek hedefler ortaya konulmuştur. Söz konusu hedeflere ulaşmak için gereksinimler ile gerçekleştirilecek faaliyetler belirlenerek çalışmalar tamamlanmıştır.

2013-2014 dönemi ile 2016-2019 döneminde gerçekleştirilen ve süreklilik arz eden eylemler, mevcut durum ve planlanan çalışmalar kapsamında gözden geçirilmiş ve gerekli iyileştirmelerin yapılması sağlanmıştır. Bu çerçevede, belirlenen stratejik amaçlar 8 ana başlıkta toplanmıştır:

I. Kritik Altyapıların Korunması ve Mukavemetin Artırılması
II. Ulusal Kapasitenin Geliştirilmesi
III. Organik Siber Güvenlik Ağı
IV. Yeni Nesil Teknolojilerin Güvenliği
V. Siber Suçlarla Mücadele
VI. Yerli ve Milli Teknolojilerin Geliştirilmesi ve Desteklenmesi
VII. Siber Güvenliğin Milli Güvenliğe Entegrasyonu
VIII. Uluslararası İş Birliğinin Geliştirilmesi

Stratejik amaçlar doğrultusunda planlanan kazanımların elde edilmesine yönelik eylemlerin belirlenmesi için ulusal paydaşların katılımıyla düzenlenen Hazırlık Çalıştayı, 67 kurumdan 127 katılımcı ile 19 Şubat 2020 tarihinde gerçekleştirilmiştir.

Yürütülen faaliyetler ve çalıştay sonucunda elde edilen veriler ışığında belirlenen 8 stratejik amaca ilişkin olarak kurum ve kuruluşlar tarafından gerçekleştirilecek 38 adet eylem ve 71 adet uygulama adımı, eylem planı kapsamında yer almaktadır. Süreçlerin iyileştirilmesi, teknolojik bileşenlerden azami seviyede istifade edilmesi ve insan kaynağının geliştirilmesine yönelik eylemlerle siber güvenlik seviyesinin daha da yükseltilmesi amaçlanmıştır. Bu doğrultuda; kritik altyapı sektörlerinin korunmasına yönelik düzenlemelerin hayata geçirilmesi, siber risk yönetiminin ve acil durum planlarının geliştirilmesi, kaynağı ve hedefi yurt içi olan internet trafiğinin yurt içinde kalmasının sağlanması ve siber güvenliğin milli güvenlik kapsamında ele alınması gibi hususlarda eylemler belirlenmiştir. Ayrıca siber olaylara müdahale ekiplerinin olgunluk seviyelerinin ölçülmesi, izlenmesi, artırılması ve siber güvenlik alanında yetkin kurumların düzenlediği eğitimlerin geliştirilmesi, ilk ve orta dereceli okullar ile yükseköğrenimde siber güvenlik eğitim içeriklerinin zenginleştirilmesi ve yaygınlaştırılmasını hedef alan eylemlerle bu alandaki insan kaynağının artırılması amaçlanmıştır. 5G, nesnelerin interneti ve bulut bilişim gibi yeni nesil teknolojilerin ülkemizde güvenli bir şekilde adaptasyonu ve kullanılması hedeflenmiştir. Oluşturulması planlanan organik siber güvenlik ağı çerçevesinde ise ileri düzey uzmanlık projelerinin geliştirilmesi ve ülke geneline yayılacak şekilde bu alanda çalışmalar gerçekleştiren kurum ve kişiler ile Ulusal Siber Olaylara Müdahale Merkezi (USOM) arasında bilgi paylaşımının artırılması öncelikli amaçlar

arasında yer almaktadır. Yerli ve milli siber güvenlik teknolojilerinin üretilmesi konusunda özel sektör tarafından gerçekleştirilen çalışmaların desteklenmesine yönelik eylemler ile de teknolojik kazanımlar artırılacaktır. Ayrıca, siber güvenliğin doğası gereği ulusal faaliyetlerin yanında uluslararası iş birliğinin geliştirilmesi de önem arz etmektedir. Bu çerçevede ikili ve çoklu iş birliklerinin artırılması ve bilgi paylaşımının geliştirilmesine yönelik çalışmalar gerçekleştirilecek, siber uzayda uluslararası ortak normların ve standartların oluşturulması için yürütülen faaliyetlere katkı sağlanacaktır.

Stratejik amaçlar kapsamında hayata geçirilecek her bir eylemin gerçekleştirilmesinden sorumlu ve iş birliği yapılacak kurum ve kuruluşlar, eylem kapsamında atılacak adımlar ve eylemlerin gerçekleşme süreleri de belirlenmiştir.

Önümüzdeki dönemde ulusal siber güvenliğin sağlanmasına ilişkin olarak gerçekleştirilecek faaliyetlerin kapsamının belirlendiği Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023) ile bu alanda Türkiye'nin 2023 yılı vizyonunun gerçeğe dönüşmesi hedeflenmektedir.

2. TANIMLAR

Çok paydaşlı ve disiplinler arası bir konu olan siber güvenliğin sağlanmasında anahtar noktalardan bir tanesi, ortak dilin konuşulmasıdır. Siber güvenlik alanında ortak tanımlamaların yapılması, paydaşlar arası iletişimin gelişmesine katkı sağlamaktadır. Bu doğrultuda, Strateji ve Eylem Planı kapsamındaki tanımlar aşağıda yer almaktadır:

Adli Bilişim: Bilişim suçları davalarında, olay kapsamında suça konu olan dijital delillerin zarar görmeyecek şekilde toplanması, değerlendirilmesi, belgelendirilmesi, sınıflandırılması ve bu verilerin yargı sürecinde kullanılabilmesini kapsayan bilim dalı.

Balküpü: Siber saldırıları gerçek sistem sunucularına benzer mimarideki tuzak sistemlere yönlendirerek tehdit ve saldırıları tespit etmek için kullanılan donanım ve yazılım altyapısı bütünü.

BGYS (Bilgi Güvenliği Yönetim Sistemi): Bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak üzere sistemli, kuralları koyulmuş, planlı, yönetilebilir, sürdürülebilir, dokümante edilmiş, kurumun/kuruluşun yönetimince kabul görmüş ve uluslararası güvenlik standartlarının temel alındığı faaliyetler bütünü.

Bilgi Güvenliği: Bilişim sistemlerinin ve bilgilerin izinsiz kullanımını, yetkisiz kişilerce erişilmesini ve ifşa edilmesini, silinmesini, değiştirilmesini ve zarar görmesini, engellemek, bu sistem ve bilgilere yetkili kişiler ve işlemlerin ihtiyaç duyulan zamanda ve kalitede erişebilmesini sağlamak için yürütülen faaliyetler bütünü.

Bilgi Varlığı: Kişi veya organizasyon için kıymetli olan veriler ile bu verilerin taşındığı, saklandığı, aktarıldığı veya işlendiği sistemler, yazılımlar, BT donanımları ve iş süreçleri.

Bütünlük: Bilginin/verinin doğruluğunu ve tamlığını koruma özelliği.

EKS (Endüstriyel Kontrol Sistemi): 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 sistemleri.

Erişilebilirlik: Bilginin/verinin yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliği.

Gizlilik: Bilginin/verinin yetkisiz kişiler, varlıklar ya da süreçler tarafından erişilememesi, kullanılamaması, değiştirilmemesi, depolanmaması, başka bir ortama kaydedilmemesi veya ifşa edilmemesi özelliği.

İDN (İnternet Değişim Noktası): İnternet trafiğinin değişimine imkân veren en az iki bağımsız otonom sistemin birbirine bağlanmasını sağlayan ağ altyapısı.

İleri Düzey Kalıcı Tehdit (APT): İleri seviyeli bilgi birikimiyle ve tekniklerle geliştirilmiş ve amaçlarını gerçekleştirebilmek için çoklu vektör ataklarını kullanabilen tehdit.

KamuNet (Kamu Sanal Ağı): Kamu kurum ve kuruluşları tarafından özel ağ ile internet ortamından yalıtılmış şekilde hizmet, işlem ve veri trafiğinin aktarılacağı, fiziksel ve siber saldırılara karşı daha güvenli kapalı devre ağ altyapısı.

Kritik Altyapı: İşlediği bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar.

Kritik Altyapı Sektörleri: 20 Haziran 2013 tarihli ve 2 sayılı Siber Güvenlik Kurulu kararı uyarınca kritik altyapıları barındırmakta olan "Elektronik Haberleşme", "Enerji", "Finans", "Ulaştırma", "Su Yönetimi" ve "Kritik Kamu Hizmetleri" sektörleri.

Risk Yönetimi: Kuruluşun iş süreçlerini etkileyecek risklerin belirli standart ve metodolojilere uygun olarak belirlenmesi, değerlendirilmesi, ihtiyaç duyulan kontrollerin, politika ve prosedürlerin hayata geçirilmesi ile olası kayıpların azaltılması, izlenmesi ve gözden geçirilmesi.

SCADA: Denetimsel Kontrol ve Veri Toplama.

SGOM: Siber Güvenlik Operasyon Merkezi.

Sıfırıncı Gün (Zero-Day) Zafiyeti: Donanım, işletim sistemleri veya uygulamalarda yeni ortaya çıkmış, henüz herhangi bir yaması veya güncellemesi geliştirilmemiş bir açıklıktan kaynaklanan ve kullanılan saldırı yöntemi ortaya çıkana kadar bilinmeyen zafiyet türü.

Sızma Testi (Pentest): Bilişim sistemlerinin veya ağın güvenlik önlemlerini atlatmanın yollarını belirleme, sisteme sızma ve bu şekilde öncelikli sistem zafiyetlerini ve açıklıklarını belirlemeye yönelik test.

Siber Güvenlik: Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin/verinin gizliliği, bütünlüğü ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber olayların tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber olay öncesi durumlarına geri döndürülmesini kapsayan faaliyetler bütünü.

Siber Olay: Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliğinin ihlal edilmesi.

Siber Risk: Siber tehditlerin bir veya birden çok bilgi varlığındaki açıklığı kullanarak zarar yaratma potansiyeli. Siber olayın olumsuz sonuçlarına ilişkin olasılıklar kombinasyonu.

Siber Saldırı: Siber uzaydaki bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın herhangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemler.

Siber Suç: Bir bilişim sisteminin güvenliğini ve/veya buna bağlı verileri ve/veya kullanıcısını hedef alan ve bilişim sistemi kullanılarak işlenen suçlar.

Siber Tehdit: Bir kurumun veya sistemin zarar görmesi ile sonuçlanabilecek istenmeyen bir siber olayın potansiyel nedeni.

Siber Uzay: Doğrudan ya da dolaylı olarak internete, elektronik haberleşme ve bilgisayar ağlarına bağlı olan tüm sistem ve hizmetler.

SOME: Siber Olaylara Müdahale Ekibi.

USOM: Ulusal Siber Olaylara Müdahale Merkezi.

Zafiyet: Siber uzayda yer alan varlıkların herhangi bir siber tehdit tarafından kullanılabilecek zayıflıkları.

3. GİRİŞ

Teknolojinin temel dinamiği, sürekli ve hızlı bir şekilde gerçekleşen değişim ve gelişimdir. Çığır açan bu teknolojik bileşenler/ürünler büyük bir hızla yaygınlaşmakta, gündelik yaşamın vazgeçilmez bir parçası haline gelmektedir. Bilgi ve iletişim teknolojilerinde yaşanan bu gelişmeler, ekonomik ve sosyal olarak küreselleşmenin de temelini oluşturmaktadır.

İnternetin kullanıcı sayısının ulaştığı nokta bu konuya çarpıcı bir örnektir. Uluslararası Telekomünikasyon Birliği (ITU) verilerine göre 2019 yılı sonu itibarıyla dünya nüfusunun yaklaşık %53,6'sının, yani 4,1 milyar insanın, internet kullanıcısı olduğu değerlendirilmektedir. Ülkemizdeki duruma bakıldığında; Bilgi Teknolojileri ve İletişim Kurumu (BTK) Türkiye Elektronik Haberleşme Sektörü 2019 yılı 4. Çeyrek Raporu'na göre 2008 yılında yaklaşık 6 milyon olan genişbant internet abone sayısı, 2019 yılı dördüncü çeyrek sonu itibarıyla 76,6 milyonu aşmıştır. Türkiye İstatistik Kurumu (TÜİK) verilerine göre 2019 itibarıyla ülkemizde 16-74 yaş arası bireylerde internet kullanım oranı %75,3 seviyesindedir.

Artan ilgi ile birlikte bilgi ve iletişim teknolojilerinin güvenli kullanımı, yalnızca ülkemizde değil tüm dünyada bir ihtiyaç olarak öne çıkmaktadır. Özellikle kritik sektörler için stratejik araçlar haline gelen bu teknolojilerin güvenliği her geçen gün daha da önemli hale gelmektedir.

Teknolojik gelişmelere eşzamanlı olarak siber riskler ve tehditler de aynı hızda değişime uğramakta, karmaşıklaşmakta ve artış göstermektedir. Söz konusu

tehditler, fiziki saldırılardan çok daha kapsamlı ve olumsuz sonuçlar doğuracak potansiyele ulaşmış, kamu güvenliği ve devletlerin istikrarı açısından dikkate alınması gereken boyutlara varmıştır. Günümüzde taşınabilir küçük bir bellekten aktarılan basit bir yazılım çok büyük bir güvenlik sorunu haline gelebilmektedir. Finans, elektronik haberleşme, su yönetimi, enerji, ulaştırma gibi kritik altyapı sektörlerinin güvenli bir dijital ortamda hizmet vermesi, maddi kayıpları önleyecek ve insan hayatına yönelebilecek tehditleri bertaraf edecektir.

Siber güvenliğin önemi COVID-19 pandemisi sürecinde bir kez daha anlaşılmıştır. Bu süre içerisinde iş hayatından eğitime, sosyal hayattan bireysel alışkanlıklara kadar hayatın birçok alanında değişiklikler meydana gelmiştir. Pandemi sürecinde başta elektronik ticaret, uzaktan erişim ve video-konferans uygulamaları olmak üzere bilgi ve iletişim teknolojilerinin sunduğu imkânlar uzaktan çalışma ve çevrimiçi eğitim koşullarının oluşturulabilmesini sağlamış, alınan tedbirler kapsamında ekonomik ve sosyal hayat idame ettirilmiştir. Diğer yandan, bu uygulamaları hedef alan siber tehditler, Koronavirüs konulu zararlı yazılımlar ve oltalama (phishing) saldırıları ile sağlık sektörü başta olmak üzere kritik altyapılara yönelik siber tehditlerle mücadele de salgın döneminde öne çıkan hususlardan biri olmuştur. Pandemi ile birlikte, "yeni normal" kavramı ile tanışan ülkeler, bir yandan kontrollü sosyal hayata ilişkin çalışmaları yürütürken diğer yandan da dijital hayatın güvenliği konusuna yoğunlaşmak durumundadır.

Güvenli bir dijital ortamın sağlanmasının yolu teknoloji, insan ve süreç bileşenlerinin güvenliğine bağlıdır. Bu doğrultuda mevcut teknolojilerin yanında, yapay zekâ, nesnelerin interneti, blok zincir, 5G gibi hayatımızda yer edinen yeni nesil teknolojilerin güvenlik kriterleri, yakın gelecekteki siber güvenlik planlamalarında öncelikli olarak yer alacaktır.

Siber tehditler her geçen gün sayısal olarak artarken nitelik olarak da gelişmekte ve yıkıcı sonuçlar doğurabilmektedir. Bu durum, tehditlerle mücadele ederken kaynakların da doğru planlanmasını zorunlu kılmaktadır. Risklerin ve ihtiyaçların iyi analiz edilmesi ve teknolojik trendler doğrultusunda ortaya çıkacak öngörülere dayalı kısa ve uzun vadeli planlamalar, güvenli siber uzayın temelini oluşturacaktır.

4. TÜRKİYE'DE SİBER GÜVENLİK

Bilgi ve iletişim teknolojilerinde yaşanan hızlı ve sürekli gelişim ve değişim bireylerin ve toplumların hayatlarını kolaylaştırırken özellikle elektronik haberleşme, enerji, finans, ulaştırma, su yönetimi gibi kritik sektörleri daha fazla hedef alan siber tehditler, bireysel ve toplumsal güvenliğe karşı riskler oluşturmaktadır.

Bu bağlamda, insanlığın temel ihtiyaçları arasında yer alan "güvenlik" kavramının riskler ve tehditler göz önünde bulundurularak kişisel ve toplumsal ölçekte değerlendirilmesi gerekmektedir.

Bu çerçevede, ulusal siber güvenliğin sağlanması ülkemiz için de en öncelikli konulardan biri haline gelmiştir.

Son dönemde ülkemizde siber güvenliğin sağlanmasına yönelik hız kazanan çalışmalarla, risklerin minimize edilmesi, yönetilebilir ve kabul edilebilir düzeylerde tutulması hedeflenmektedir. Bu kapsamda, 5809 sayılı Elektronik Haberleşme Kanunu'nun 5'inci maddesinin birinci fıkrasının (h) bendi ile "*Ulusal siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere yönelik siber güvenliğin sağlanmasına ilişkin usul ve esasları belirlemek, eylem planlarını hazırlamak, ilgili faaliyetlerin koordinasyonunu sağlamak, kritik altyapılar ile ait oldukları kurumları ve konumları belirlemek, gerekli müdahale merkezlerini kurmak, kurdurmak ve denetlemek, her türlü siber müdahale aracının ve millî çözümlerin üretilmesi ve geliştirilmesi amacı ile çalışmalar yapmak, yaptırmak ve bunları teşvik etmek ve siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları*

yürütmek, siber güvenlik alanında faaliyet gösteren gerçek ve tüzel kişilerin uyması gereken usul ve esasları hazırlamak" görev ve sorumlulukları Ulaştırma ve Altyapı Bakanlığına verilmiştir.

Ayrıca, 10 Temmuz 2018 tarihli ve 30474 sayılı Resmî Gazete'de yayımlanan 1 no'lu Cumhurbaşkanlığı Kararnamesi ile kurulan Dijital Dönüşüm Ofisine (DDO) *"Bilgi güvenliğini ve siber güvenliği artırıcı projeler geliştirmek"* görevi verilmiştir. Bu çerçevede, 2019/12 sayılı Cumhurbaşkanlığı Genelgesi ile Bilgi ve İletişim Güvenliği Tedbirleri yayımlanmıştır.

15 Ağustos 2016 tarihinde 5809 sayılı Elektronik Haberleşme Kanunu'na eklenen hükümler[1] ile BTK'ya siber saldırıların engellenmesi ve caydırıcılığın sağlanması görevleri ile bu görevler kapsamında yükümlülüklerini yerine getirmeyen ilgili taraflara yaptırım uygulama yetkisi verilmiştir.

Ülkemizde siber güvenlik alanında ilk olan "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", 20 Haziran 2013 tarihli ve 28683 sayılı Resmî Gazete' de yayımlanarak yürürlüğe girmiştir. 2 yıllık bu dönem içerisinde siber güvenlik mevzuatının geliştirilmesi, kritik altyapıların güvenliğinin sağlanması, toplumda siber güvenlik farkındalığının oluşturulması, siber tehditlerin tespiti ve önlenmesi konularında çalışmalar yürütülmüştür.

Ayrıca 2013 yılında, BTK bünyesinde faaliyetlerini sürdüren Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuş, belirlenen kritik altyapı sektörleri başta olmak üzere kurum ve kuruluşlarda Siber Olaylara Müdahale Ekipleri (SOME) faaliyetlerine başlamıştır. Ulusal siber güvenlik organizasyonunun oluşturulmasıyla ülkemizde kurumsal ve organizasyonel yapıların kurularak güçlendirilmesi sağlanmıştır.

Sonrasında yayımlanan "2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" ile de siber güvenlik risklerinin yönetilebilir ve kabul edilebilir düzeylerde tutulabilmesi için siber savunmanın güçlendirilmesi, kritik altyapıların korunması, siber suçlarla mücadele edilmesi, farkındalık ve insan kaynağı geliştirilmesi, siber güvenlik ekosisteminin geliştirilmesi ve siber güvenliğin milli güvenliğe entegrasyonu konularında çalışmalar yürütülmüştür. Bu çerçevede, son dönemde;

[1] MADDE 60 (11) Kurum, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alır veya aldırır. (12) Kurum, görevi kapsamında ilgili yerlerden bilgi, belge, veri ve kayıtları alabilir ve değerlendirmesini yapabilir; arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilir, bunlarla irtibat kurabilir ve bu kapsamda diğer gerekli önlemleri alabilir veya aldırabilir. Kurum, bu fıkrada belirtilen görevlerin ifasında bakanlıklar, kurum ve kuruluşlar ile işbirliği içerisinde çalışır. Bu kapsamda Kurum tarafından istenen her türlü bilgi ve belge talebi; ilgili bakanlık, kurum ve kuruluşlar tarafından gecikmeksizin yerine getirilir. Bu fıkraya göre bilgi ve belge talebinde bulunulması ve bu taleplerin yerine getirilmesine ilişkin usul ve esaslar ile diğer hususlar Cumhurbaşkanlığınca belirlenir. (13) Gerçek kişiler ile özel hukuk tüzel kişileri, Kurumun bu maddedeki görevleri ile ilgili taleplerini, tabi oldukları mevzuat hükümlerini gerekçe göstermek suretiyle yerine getirmekten kaçınamazlar. İşletmeciler dışında Kurumun görevleri ile ilgili yükümlülüklerini yerine getirmeyenlere bu maddenin ikinci fıkrasındaki yaptırım uygulanır.

- Ulusal siber güvenlik kapasite inşası programı kapsamında SOME'lerin insan kaynağının iyileştirilmesi ve siber olaylara hazırlık seviyesinin artırılması, ülkemizin ihtiyaç duyduğu insan kaynağının yetiştirilmesine yönelik olarak eğitim, kamp ve yarışma gibi faaliyetler,

- Teknolojik önlemler programı kapsamında, yapay zekâ ve makine öğrenmesi imkânlarını kullanan AVCI, AZAD ve KASIRGA gibi hızlı tespit ve erken müdahale sistemlerinin geliştirilmesi,

- Tehdit istihbaratı edinimi, üretimi ve paylaşımı programı kapsamında ulusal ve uluslararası paydaşlarla iki yönlü bilgi paylaşımı ve koordinasyon çalışmaları ve

- Kritik altyapıların korunması programı kapsamında kritik altyapıların hizmet sürekliliğinin takibine yönelik izleme faaliyetleri, zafiyet tarama çalışmaları ve bilgi güvenliği açısından düzenleme ve denetleme çalışmaları yürütülmüştür.

Tüm bu çalışmalar kapsamında, Uluslararası Telekomünikasyon Birliği Global Siber Güvenlik Endeksi'nin 2019'da yayınlanan sonuçlarına göre ülkemiz bir önceki yıla göre 23 sıra birden yükselerek 2018 yılında dünyada 20'nci sırada, Avrupa'da 11'inci sırada yer almıştır.

Ulusal siber güvenlik faaliyetleri ülkemizde en üst düzeyde takip edilerek desteklenmekte olup bu kapsamda 10 Şubat 2020 tarihinde Ulusal Siber Olaylara Müdahale Merkezinin resmi açılışı bizzat Sayın Cumhurbaşkanımız Recep Tayyip ERDOĞAN tarafından gerçekleştirilmiş ve bu alanda ülkemizin dünya markası olması yönünde bir vizyon ortaya konulmuştur.

Teknolojinin vazgeçilmezliği ve sürekli gelişimiyle birlikte siber güvenliğe ilişkin faaliyetlerin de süreklilik içerisinde yürütülmesi gerekmektedir. Bu doğrultuda, Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023), bugüne kadar gerçekleştirilen çalışmalarda elde edilen kazanımların daha ileriye taşınması amacıyla hazırlanmıştır. Siber tehditlerin etkilerinin azaltılması, ulusal kabiliyetlerin geliştirilmesi, güvenli bir ulusal siber ortamın oluşturulması ve ülkemizin siber güvenlik alanında uluslararası seviyede en üst sıralarda yer alması hedeflenmektedir.

5. VİZYON VE MİSYON

VİZYON

Ülke ekonomisinin geliştirilmesini, toplumsal yaşamın korunmasını ve milli güvenliğin sağlanmasını desteklemek için; ülkemizde güvenli biçimde işleyen bir siber ortama sahip olmak ve siber güvenlikte uluslararası alanda marka haline gelmek.

MİSYON

Siber güvenliğin milli güvenliğimizin ayrılmaz bir parçası olduğu bilinci ile kritik altyapılarımız başta olmak üzere siber uzaydaki varlıklarımızın tehditlerden korunmasına ve siber olayların muhtemel etkilerini azaltmaya yönelik çalışmaları ilgili tüm paydaşlarla koordineli olarak gerçekleştirmek.

6. YÖNTEM

Stratejik yaklaşımların ilk adımı doğru yöntemi belirlemekten geçmektedir. Siber güvenlik gibi toplumun tüm kesimlerini kapsayan bir konuda seçilen yaklaşımın anlaşılır, uygulanabilir, ilkeli, kaynakların doğru ve zamanında kullanımını içeren temeller üzerine inşa edilmesi, hedeflenen sonuca ulaşmayı kolaylaştıracaktır.

İnsanlığın temel ihtiyaçlarından biri olan güvenliğin, teknolojik boyutta da uygun biçimde ele alınarak benimsenmesi, kapsamlı ve planlı çalışmalar gerektirmektedir. Ortaya konulan vizyon ve misyon somut kazanımlara dönüşürken göz ardı edilmemesi gereken bir diğer nokta, bu dönüşüm esnasında izlenmesi gereken ilkelerin varlığıdır. Dayandığı ilkeler doğrultusunda hazırlanan stratejilerin etkileri, paydaşlara olumlu olarak yansıyacak, belirlenen hedeflere ulaşılmasını sağlayacaktır.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023), belirlenen faaliyetler ve bu faaliyetlerden oluşan eylemlerin hayata geçirilmesini amaçlamaktadır. Söz konusu eylemler bütününün tamamlanması ise tespit edilen stratejik amaçlara ulaşmayı sağlayacaktır. Böylece Ulusal Siber Güvenlik Stratejisi ve Eylem Planı hedef odaklı bir yapıda planlanmıştır.

7. İLKELER

Ulusal siber güvenliğin sağlanmasına yönelik strateji ve eylemlerin etkin ve dengeli biçimde belirlenen ilkeler üzerine inşa edilmesi, sürekli gelişen ve güçlenen ülkemizin ekonomik ve toplumsal refahına da katkı sağlayacaktır.

Ulusal ve uluslararası normlar ile güncel teknolojik yaklaşımlar doğrultusunda ulusal siber güvenliğin sağlanmasında temel aldığımız ilkeler şu şekilde öne çıkmaktadır:

1. Siber güvenlik, ulusal güvenliğin ayrılmaz bir parçasıdır. Ulusal güvenliğin tam olarak sağlanabilmesi, siber güvenlik alanında belirlenen hedeflere ulaşılabilmesine dayanır.

2. Siber güvenlik ile ilgili çalışmalar geçmişten geleceğe kazanımlar, hedefler, programlar ve projeler açısından kurumsallık, süreklilik ve sürdürülebilirlik ilkelerine göre yürütülür.

3. Dijitalleşmenin başarılı ve sürdürülebilir olması için siber güvenliğin hayati bir öneme sahip olduğu göz önünde bulundurulur.

4. Siber güvenlik politikalarının uygulanmasına yönelik tüm çalışmalar, paydaşların etkin iletişimi ve koordineli iş birliği içerisinde ve uygun metodolojilerle yürütülür.

5. Paydaşlar, siber uzaydaki risklerin yönetimi ile ilgili sorumluluklarını yerine getirirken şeffaflığı, hesap verebilirliği ve etik değerleri göz önünde bulundurur.

6. Siber güvenlik riskleri etkin bir şekilde belirlenir ve yönetilir.

7. Özellikle kritik altyapılar aracılığıyla verilen hizmetlerin kesintisiz ve etkin olarak sunulması esastır.

8. Hizmet ve ürünlerin ortaya konmasında, tasarımından son kullanıcıya erişimine kadar baştan sona tüm süreçlerde siber güvenlik kavramının dikkate alınması esastır.

9. Yürütülen iş ve işlemlerde bilginin "gizlilik-bütünlük-erişilebilirlik" dengesinin sağlanması ve "bilmesi gereken prensibi" gibi temel siber güvenlik prensiplerine sadık kalınması esastır.

10. Güçlü hukuki temeller üzerine güçlü bir siber güvenlik inşa edilmesi esastır.

11. Ar-Ge, yenilikçilik ve güçlü teknolojik altyapı anlayışı ile siber güvenlikte yerli ve milli ürün ve hizmet kullanımı teşvik edilir.

8. HEDEFLER

Geliştirilen politika ve stratejilerin başarı oranı, doğru hedeflerin ortaya konması ve o hedeflere ulaşmak için gerekli faaliyetlerin süreklilik içinde yürütülmesine bağlıdır.

Siber güvenlik, *"siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin/verinin gizliliği, bütünlüğü ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber olayların tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber olay öncesi durumlarına geri döndürülmesini kapsayan faaliyetler bütünü"* olarak ifade edilmektedir. Bu çerçevede, ulusal siber ortamda güvenliği sağlamak için katkı verecek tüm paydaşların temel hedefi *"siber tehditlerin, risklerin ve bunların etkilerinin en aza indirgenmesi"* olarak ortaya çıkmaktadır. Siber güvenlik alanında insan kaynağının doğru ve etkin kullanımı, süreçlerin iyileştirilmesi ve teknolojik gelişim hem istikrarlı büyümeyi hem de kalkınmayı tamamlayıcı unsurlar olarak öne çıkmaktadır.

Bu açıdan bakıldığında, Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023) kapsamında belirlenecek ve gerçekleştirilecek hedeflerin, ülkemizin kısa, orta ve uzun vadede daha büyük ölçekli hedeflerine de katkı sağlayacağı değerlendirilmektedir.

Ülkemizin 2023 yılı vizyonu çerçevesinde belirlenen

ULUSAL SİBER GÜVENLİK HEDEFLERİMİZ

Kritik altyapılarımızın siber güvenliğinin 7/24 korunması.
Ulusal seviyede siber güvenlik alanında en son teknolojik imkânlara sahip olunması.
Operasyonel ihtiyaçlar çerçevesinde yerli ve milli teknolojik imkânların geliştirilmesi.
Siber olaylara müdahalenin olay öncesi, esnası ve sonrasını kapsayan bir bütün olmasından hareketle; proaktif siber savunma anlayışının geliştirilmeye devam edilmesi.
Siber olaylara müdahale ekiplerinin yetkinlik seviyelerinin ölçülmesi ve izlenmesi.
Siber olaylara müdahale ekiplerinin yetkinliklerinin artırılması.
Kurumsal, sektörel ve ulusal bazda siber olaylara hazırlık seviyelerinin risk temelli analizler ve planlamalara dayalı yaklaşımlarla artırılması.
Kurum ve kuruluşlar arası veri paylaşımının güvenli biçimde sağlanması.
Kaynağı ve hedefi yurt içi olan veri trafiğinin yurt içinde kalması.
Kritik altyapı sektörlerinde düzenleme ve denetlemeye dayalı siber güvenlik yaklaşımının geliştirilmesi.
Kritik altyapı sektörlerinde, BT ürünlerinde üretici bağımlılığının önüne geçilmesi.
Yeni nesil teknolojilerin güvenliğinin sağlanmasına yönelik gereksinimlerin belirlenmesi.
Yenilikçi fikirlerin ve Ar-Ge faaliyetlerinin desteklenerek yerli ve milli ürün ve hizmetlere dönüşümünün gerçekleştirilmesi.
Toplumun tüm kesimleri tarafından siber uzayın güvenle kullanılması.
Siber güvenlik farkındalığının tüm toplumda üst seviyede tutulmasına yönelik etkinliklerin sürdürülmesi.
Kurum ve kuruluşlarda kurumsal bilgi güvenliği kültürünün yerleşmesi.
Çocukların siber ortamda korunmasının sağlanması.
Siber güvenliğe ilgi duyan veya uzmanlaşmak isteyen bireylere yönelik projelerle insan kaynağının güçlendirilmesi.
Örgün ve yaygın eğitimde siber güvenlik eğitiminin yaygınlaştırılması ve eğitim içeriklerinin zenginleştirilmesi.
Ulusal ve uluslararası düzeydeki paydaşlarla bilgi paylaşımı ve iş birliğini sağlayacak mekanizmaların geliştirilmesi.
Siber suçların en aza indirgenmesi ve caydırıcılığın artırılması.
İnternet ve sosyal medyada doğru ve güncel bilgi paylaşımının sağlanmasına yönelik mekanizmaların geliştirilmesi.

9. STRATEJİK AMAÇLAR

Teknolojik gelişimin her unsurunda olduğu gibi bu teknolojilerin ayrılmaz bir parçası olan siber güvenlikte de belirlenen hedeflere ulaşılması için, belli odak alanları öne çıkmaktadır.

2020-2023 dönemi için bu temel odak alanları "stratejik amaçlar" olarak ifade edilmektedir. Siber güvenlikte ülkemizin 2023 vizyonunun gerçekleşmesi ve 2023 sonrasına güvenle yol alınması amacıyla belirlenen stratejik amaçlar aşağıda yer almakta ve daha detaylı olarak açıklanmaktadır:

I
Kritik Altyapıların Korunması ve Mukavemetin Artırılması

II
Ulusal Kapasitenin Geliştirilmesi

III
Organik Siber Güvenlik Ağı

IV
Yeni Nesil Teknolojilerin Güvenliği

V
Siber Suçlarla Mücadele

VI
Yerli ve Milli Teknolojilerin Geliştirilmesi ve Desteklenmesi

VII
Siber Güvenliğin Milli Güvenliğe Entegrasyonu

VIII
Uluslararası İş Birliğinin Geliştirilmesi

I. Kritik Altyapıların Korunması ve Mukavemetin Artırılması

"Siber Uzayda Ulusal Güvenlik"

Kritik altyapılar; "İşlediği verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar" olarak tanımlanmaktadır. Tüm vatandaşların günlük hayat içerisinde ihtiyaç duyduğu ve faydalandığı hizmetlerin sunulduğu bu altyapılar siber tehditler tarafından özellikle hedef alınmaktadır. Bu tehditlerin söz konusu altyapı ve hizmetlere yönelik olumsuz etkilerinin yıkıcı boyutlara ulaşabilmesi ve çok geniş bir kapsamda etki oluşturabilmesi, saldırganların temel motivasyonunu tanımlamaktadır.

Ülkemizde "Elektronik Haberleşme", "Enerji" "Finans", "Ulaştırma", "Su Yönetimi" ve "Kritik Kamu Hizmetleri" olarak tanımlanan kritik altyapı sektörlerinin korunmasına yönelik önemli faaliyetler gerçekleştirilmiştir. Süreklilik içerisinde yürütülmesi gerekli bu faaliyetlerin, değişen siber tehdit vektörleri ve ortaya çıkan ulusal ihtiyaçlar ile teknolojide yaşanan gelişmeler dikkate alınarak daha etkin bir şekilde yürütülmesine devam edilecektir. Bu amaçla kritik altyapıların korunması stratejik amaçlardan biri olarak belirlenmiştir. Siber tehditler karşısında kamu ve özel sektörün korunmasını sağlayacak tedbirler alınarak ulusal mukavemetin artırılması hedeflenmektedir.

Bu çerçevede gerçekleştirilecek çalışmalarda; uluslararası bilgi güvenliği standartlarının kamu ve özel sektörde uygulanmasının yaygınlaştırılması, altyapılarda üretici bağımlılığının önüne geçilmesi, yurt içinde üretilen verilerin yurt içinde kalması gibi konular anahtar rol oynayacaktır. Bunun yanında, sektörel düzenlemelerin geliştirilmesi ve denetim mekanizmalarının oluşturulması, acil durum hazırlık planlarının hayata geçirilmesi ve güvenli bir teknolojik dönüşümün sağlanması önceliklerimiz arasında yer almaktadır.

Sonuç olarak, kritik altyapılarımızın ve siber uzaydaki tüm ulusal varlıklarımızın siber tehditlere karşı etkin şekilde korunması ve siber olaylara müdahale kabiliyetlerimizin daha da güçlendirilmesi hedeflenmektedir. Buna ilave olarak, sektörel ve ulusal ölçekte bir risk yönetimi anlayışıyla tehditlerin ve oluşturdukları olumsuz etkilerin en aza indirgenmesi amaçlanmaktadır.

II. Ulusal Kapasitenin Geliştirilmesi

"İnsan Kaynağının Güçlendirilmesi"

Ulusal siber güvenliğin sağlanmasındaki en önemli bileşenlerden birisi uzman insan kaynağına sahip olmaktır. Ülkemizin bu alandaki ihtiyacını karşılamak amacıyla yürütülecek faaliyetler mevcut insan kaynağının bilgi düzeyi ve tecrübesini artırmayı amaçlamaktadır. Ayrıca, bu alanda nitelikli insan gücünün yetiştirilmesi de bir diğer odak alanını oluşturmaktadır.

Bu kapsamda, siber olaylara hazırlık seviyesinin geliştirilmesi amacıyla SOME'lerin olgunluk seviyelerinin ölçülerek mevcut durumun belirlenmesi ve gelişim ihtiyacı bulunan alanlara odaklanılarak yetkinliklerinin daha da üst düzeylere çıkarılması amaçlanmaktadır. Ayrıca sektörel, ulusal ve uluslararası seviyede düzenli olarak gerçekleştirilecek siber güvenlik tatbikatları ve eğitimler ile de yetkinliğin artırılması hedeflenmektedir.

Bununla birlikte siber güvenlik uzmanlığı kavramının geliştirilerek mesleki nitelik kazandırılması, üniversitelerde siber güvenlik ve ilgili alanlardaki programların yaygınlaştırılması ve siber suçla mücadelede görev yapan personelin uzmanlık seviyesinin artırılmasına yönelik faaliyetler gerçekleştirilecektir. Bu çalışmalara ilave olarak, toplumda bu alanda uzmanlaşmak isteyen bireylerin yarışma, yaz kampları ve eğitim faaliyetleriyle desteklenmesi sağlanacak ve ülkemizdeki nitelikli insan kaynağı güçlendirilecektir.

"Toplumsal Farkındalığın Artırılması ve Çocukların Çevrimiçi Korunması"

Toplumun tüm kesimlerinde siber güvenlik kültürünün yerleşmesi çağın gereklerinden biridir. Bu kültürün temeli ise yüksek düzeyde farkındalığın sağlanmasına dayanmaktadır. Teknolojinin güvenli kullanımının önemi tüm bireyler tarafından benimsendiğinde, riskler ve tehditlerin hayata olumsuz etkileri gözle görülür biçimde azalacaktır.

Bu bağlamda bireysel, kurumsal ve ulusal ölçeklerde, yani tüm toplum genelinde, farkındalığı artırıcı çalışmaların gerçekleştirilmesi; aileler, çocuklar, öğrenciler, gençler, kadınlar, yaşlılar ve engellilere yönelik faaliyetlerle her kesime ulaşılması öncelikli hedefler arasında yer almaktadır. Çocukların siber ortamda korunmasına yönelik farkındalık kampanyaları ve ailelere düşen sorumluluklara ilişkin bilinç düzeyini artırıcı etkinlikler de bu kapsamda önem derecesi yüksek çalışmalar olacaktır.

III. Organik Siber Güvenlik Ağı

"İleri Seviye Tehditlerle Mücadele"

Siber tehditler giderek karmaşık hale gelmekte, tespiti zorlaşmakta ve ulusal güvenliği tehdit edici bir unsur olarak yaygınlaşmaktadır. Fidye yazılımları ve oltalama gibi saldırı yöntemlerinin yanı sıra APT'ler ve sıfırıncı gün saldırıları gibi öngörülmesi ve tespit edilmesi oldukça zor tehditler oluşturma eğilimi, özellikle büyük ölçüde zararlar vermek isteyen saldırganların başvurduğu yöntemler olarak karşımıza çıkmaktadır.

Bu tür tehditlere karşı koymak için ileri seviye uzmanlık projelerinin geliştirilmesi, kalıcı tehditlerin analiz edilmesi ve uzun soluklu çalışmaların yapılması, ekiplerimizin olgunluklarının geliştirilmesine bağlıdır.

"Birlikte Daha Güçlüyüz"

Organik bir siber güvenlik ağı ile siber güvenlik alanında çalışan veya siber güvenliğe ilgi duyan her kesimden insanın bilgi ve tecrübe paylaşımına katılmasına imkân ve yön verecek iş birliği çalışmalarının geliştirilmesi amaçlanmaktadır.

Çeşitlenerek geniş bir yelpazede farklı motivasyonlarla karşımıza çıkan saldırı profillerine ilişkin bilgilerin tek bir kaynaktan elde edilmesi mümkün olamamaktadır. Bu çerçevede, bilgi ve istihbarat paylaşımlarının anahtar hale geldiği siber güvenlikte kaynakların çeşitlenmesi ve artırılması gerekmektedir. Özellikle bu çeşitlenen kaynaklardan edinilecek bilgilerle ulusal siber güvenlik faaliyetlerine girdi sağlanması, teknik seviyede siber olaylara müdahale yapılanmamızın omurgasını oluşturan USOM ve SOME'lerin gücüne güç katacaktır.

Bu kapsamda, USOM'un mevcut paydaşları ile olan bilgi alışverişinin ve etkileşiminin daha ileriye taşınması hedeflenmektedir. Bir yandan kamu kurumlarımız ve özel sektörümüz ile siber tehditlere ilişkin bilgi paylaşımını artırırken diğer yandan da ülke genelinde siber güvenlik konusunda çalışmalar yürüten gençlerimiz başta olmak üzere bu alandaki paydaşlarla yeni bağlar kurmak önem arz etmektedir. Bu doğrultuda, karşılıklı destek ve geri bildirim mekanizmaları ile ulusal siber güvenliğe katkı sağlanması amaçlanmaktadır. Böylece tüm paydaşlarla 7/24 etkileşimin sürdürülerek ulusal çapta canlı, aktif ve organik bir siber güvenlik ağı oluşturulması hedeflenmektedir.

Gerçekleştirilecek çalışmalarla, proaktif savunmanın pekiştirilmesi, siber caydırıcılığın sağlanması ve saldırıların oluşmadan tespit edilerek önlem alınması sağlanacak ve siber uzayda birlikten doğan kuvvetle gücümüz artacaktır.

IV. Yeni Nesil Teknolojilerin Güvenliği

"Güvenle Gelen Yeni Nesil Teknolojiler"

Ülkemizde de birçok uygulamayla hayatımızın merkezi olmaya başlayan yeni nesil teknolojiler bu stratejide öncelikli olarak değerlendirilen konular arasında yer almaktadır. Nesnelerin interneti, bulut bilişim ve yakın zamanda hayata geçecek 5G gibi teknolojilerin güvenli kullanımı sürdürülebilir ulusal ekonomik kalkınmayı destekleyecek unsurlardır. Bununla birlikte, yapay zekânın ve blok zincir teknolojilerinin siber güvenlik için kullanım alanlarının belirlenmesi ve geliştirilecek yerli ve milli teknolojiler ile katma değer oluşturması amaçlanmaktadır.

V. Siber Suçlarla Mücadele

"Güvenli Siber Ortam"

Suçların siber uzaya taşınması, buradaki bileşenler kullanılarak işlenmesi, bireylerin hak ve özgürlüklerini tehdit eder hale gelmesi ve bilişim sistemlerini hedef alan saldırılar; tüm dünyanın karşı karşıya kaldığı ve çözüm üretmek üzere yoğun çalışmalar yürüttüğü konulardır. Siber suçlarla mücadele yöntemlerinin sürekli geliştirilmesi, önleyici, caydırıcı ve etkili çalışmalar yapılması gerekmektedir. Bu bağlamda 2020-2023 döneminde de siber suçla mücadelenin daha güçlü şekilde sürdürülmesi için bu alandaki ulusal kapasitenin ve teknolojik imkânların artırılması amaçlanmaktadır.

"Uluslararası Mücadele"

Siber suçlarla mücadele alanında özellikle uluslararası seviyede iş birliği ihtiyacı ortaya çıkmaktadır. Siber uzayın mekândan bağımsız olması bu alandaki suçluların ulusal sınırların ötesinden faaliyet gösterebilmelerine imkân sağlamaktadır. Bu noktada siber suçun kaynağına ve suçluya en etkin biçimde ulaşılabilmesi için bilgi paylaşımı ve uluslararası iş birliğinin daha da geliştirilmesi hedeflenmektedir.

VI. Yerli ve Milli Teknolojilerin Geliştirilmesi ve Desteklenmesi

"Türkiye'nin Teknolojisi"

Yeni nesil teknolojilerin entegre edildiği yerli ve milli siber güvenlik çözümlerinin sayısının artırılması ve kullanımının yaygınlaşması ülkemizin 2023 vizyonu

kapsamındaki hedeflerine ulaşmamıza katkı sağlayacaktır. Ülke olarak siber güvenlik alanında öncü olmak hedefi ile yürütülen çalışmalar kapsamında özel sektörün gelişimi, büyümesi, ihracat kapasitesini artırarak ekonomiye katkı sağlaması ve teknolojiye yön veren bir konumda olması temel hedeftir.

"Teknoloji Geliştirmede İş Birliği ve Destek Mekanizmaları"

Siber güvenlik ekosistemimizin büyümesi ve gelişmesi için kamu-akademi-özel sektör arasındaki iş birliklerinin geliştirilmesi ve daha üst seviyeye çıkarılması amaçlanmaktadır. Bu iş birlikleri yerli ve milli ürünlerin geliştirilmesine doğrudan etkide bulunabilecek ve ortaya konulan hizmetler ile ürünlerin ihtiyaca yönelik olmasını sağlayacaktır. Özellikle girişimciliğin, araştırma ve geliştirme çalışmalarının ve faaliyetine yeni başlayan firmalar (start-up) ile küçük ve orta büyüklükteki işletmeler başta olmak üzere özel sektörün desteklenmesi için mevcut mekanizmalardan faydalanmak ve yeni mekanizmalar ile bu desteğin artırılmasını sağlamak amaçlanmaktadır.

Siber güvenliğimizin yerli ve milli ürünlerimizle sağlanması, özellikle kritik altyapılarımızın yerli ve milli güvenlik çözümleriyle korunması, öncelikli hedefler arasında yer almaktadır.

"Siber Güvenlik Test ve Sertifikasyon Sistemi"

Ulusal kaynaklarımızla üretilen ürün ve hizmetlerin marka değerinin katlanarak artması ve artan ihracatla beraber dünyaya açılması temel hedeftir. Bu hedef doğrultusunda yerli ürün ve hizmetleri uluslararası pazarda rekabet edebilecek seviyelere çıkarmak adına siber güvenlik ve performans bakımından yeterliliklerinin test edilmesi ve ürünlerin sertifikasyonu için gerekli ulusal mekanizmanın kurulması amaçlanmaktadır. Ayrıca, söz konusu mekanizma ile ülkemizde kullanılan yabancı menşeli bilişim ürünlerinin de siber güvenlik bakımından test edilmesi sağlanacaktır.

VII. Siber Güvenliğin Milli Güvenliğe Entegrasyonu

"Ulusal Güvenlik İçin Siber Güvenlik"

Siber güvenlik ulusal güvenliğin ayrılmaz bir parçasıdır. Bu bağlamda üst düzey milli güvenlik politikalarımızda siber güvenliğe ilişkin hususların da azami derecede dikkate alınması, bu politikalarda kara, hava, deniz ve uzay güvenliğinin yanında siber savunmanın da yerini alması, ülkemizin diğer unsurlarla birlikte siber unsurları da içeren hibrit tehditlerden korunması ve caydırıcılığın artırılması amaçlanmaktadır.

VIII. Uluslararası İş Birliğinin Geliştirilmesi

"Sınıraşan Tehditlerle Mücadele"

Siber uzayda kesin çizgilerle çizilmiş sınırlar bulunmamaktadır. Siber uzay her dakika, her saniye yeni cihazların, sistemlerin, kullanıcıların birbirine bağlanmasıyla gitgide genişleyen bir yapıya sahiptir. Siber güvenlik, bütün dünyanın gündeminde olan ve uluslararası seviyede çalışmaların yürütüldüğü bir konudur. Bu nedenle, ülkemizde ve dünyada ulusal siber güvenlik faaliyetlerinin yanı sıra bunları tamamlayacak ve bunların sağladığı kazanımları artıracak uluslararası faaliyetler gerçekleştirilmektedir.

Siber güvenlikte politika belirleme, siber olaylara müdahale ve siber suçlarla mücadele bağlamında; ikili ve çok taraflı olarak hayata geçirilen iş birlikleri bulunmaktadır. Bu kapsamda yürütülen faaliyetlerle, siber uzayda uluslararası mekanizmalardaki çalışmalara yön verilmekte, bilgi ve tecrübe alışverişi gerçekleştirilmektedir.

Uluslararası organizasyonlar nezdinde siber uzayda güveni artırmaya yönelik önlemlerin belirlenmesi ve üye ülkeler tarafından uygulanması, ortak stratejilerin ve uygulamaların geliştirilmesi, teknik seviyede iş birlikleri, uzmanlar arası iletişimin artırılması gibi çalışmalar siber uzayın gündeminde bulunmaktadır. Bununla birlikte, ülkemizde ve dünyada siber olaylara müdahale kabiliyetlerinin güçlendirilmesine, bilgi ve hazırlık seviyelerinin artırılmasına yönelik siber güvenlik tatbikatları, konferanslar, seminerler, çalıştaylar gibi etkinlikler ile kapasite geliştirmeye yönelik uluslararası faaliyetler düzenlenmektedir.

Önümüzdeki dönemde de uluslararası siber güvenlik faaliyetlerine artan bir oranda katılım ve katkı sağlanarak ülkemizin bu alandaki söz sahibi konumunun daha da pekiştirilmesi ve dünyadaki iyi uygulama örneklerinin tespit edilerek ulusal siber güvenlik çalışmalarına sağlanan girdilerin artırılması amaçlanmaktadır.

10. GERÇEKLEŞTİRME YAKLAŞIMI

10.1. Eylem Planı

Ulusal Siber Güvenlik Stratejisi (2020-2023) ile ortaya konulan vizyon ve misyon doğrultusunda, sahip olduğumuz ilkeler çerçevesinde, ulusal siber güvenliğin sağlanması için tüm paydaşlarımızın katılımıyla gerekli adımların atılarak amaçlarımızın gerçekleştirilmesi yüksek öneme sahiptir. Kamu, özel sektör, akademi ve STK'lardan temsilcilerin geniş katılımıyla gerçekleştirilen hazırlık çalıştayında stratejik amaçlar kapsamında ulusal hedeflere ulaşabilmek için gerekli eylemler ve yürütülecek faaliyetler konusunda ilgili tarafların görüşleri alınmıştır. Hazırlanan taslak doküman ilgili kurum ve kuruluşların görüşlerine açılmış, alınan görüşler kapsamında revize edilmiş ve nihai haline kavuşmuştur.

Stratejimizin tamamlayıcı dokümanı olan Ulusal Siber Güvenlik Eylem Planı (2020-2023); her bir eylemin açıklamasıyla beraber eylemlerden sorumlu kurumları, iş birliği yapılacak kurumları, eylemlerin amaçlarını ve uygulama adımlarını, bunların gerçekleştirilmeleri için belirlenen yöntemleri ve beklenen gerçekleştirilme sürelerini detaylı olarak ele almaktadır.

Gerçekleştirilmesi hedeflenen toplam 8 adet stratejik amaçla ilişkilendirilen 38 adet eylem ve 71 adet uygulama adımı Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023) kapsamında yer almaktadır.

10.2. İzleme ve Ölçüm

Ulusal Siber Güvenlik Eylem Planı (2020-2023), başarısı kapsadığı eylemlerin gerçekleştirilmesine dayanan bir tamamlayıcı belgedir. Söz konusu eylemlerin

her birinin tamamlanıp tamamlanmadığını ölçümlemek yapılan çalışmaların başarısının somut biçimde ortaya konması anlamına gelmektedir. Bu amaçla, eylemlerin içerdiği her bir uygulama adımına yönelik ölçüm kriterleri belirlenmiş olup Eylem Planı'nın gerçekleşme oranının bu kriterler üzerinden belirlenmesi planlanmıştır. Söz konusu ölçüm kriterleri belirlenirken, her bir eylemin içerdiği uygulama adımları ve bunların gerçekleştirilmesi için belirtilen yöntemler dikkate alınmıştır.

Eylem Planı'nın izlenmesi ve ölçümü; belirlenen uygulama adımları, yürütülen faaliyetler ve ölçüm kriterleri temelinde periyodik olarak eylemlerden sorumlu ve ilgili kurum ve kuruluşlardan alınacak girdilerle sağlanacaktır.

10.3. Paydaşlar

Eylemlerin niteliği, yürütülmesi gerekli faaliyetler, kaynak ihtiyacı ve faaliyetlerin sürekliliği dikkate alınarak tamamlanma tarihleri planlanmış, her bir uygulama adımı için sorumlu kurum/kuruluş belirlenmiştir. Bununla birlikte, iş birliği yapılabilecek birden fazla kurum veya kuruluş olabilmektedir. Her bir uygulama adımının, sorumlu kurumun koordinatörlüğünde ilgili kurumlarla/kuruluşlarla iş birliği halinde yürütülecek çalışmalarla gerçekleştirilmesi, Eylem Planı'nın başarısında ve ulusal siber güvenliğimizin sağlanmasında önemli bir unsur olarak değerlendirilmektedir.

Siber uzayda yer alan paydaşlarımız arasında ülkemizden kamu kurum ve kuruluşları, kritik altyapılarda faaliyet gösterenler başta olmak üzere özel sektör kurum ve kuruluşları, üniversiteler, sivil toplum kuruluşları, araştırma toplulukları ve ülkemizdeki bireyler ile uluslararası paydaşlarımız bulunmaktadır. Tüm paydaşlarımızın doğrudan veya dolaylı katkılarıyla, belirlenen hedeflere ulaşılması amaçlanmaktadır.

10.4. Kapsam

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023); kamu bilişim sistemlerini, kamu ve özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerini, küçük ve orta ölçekli sanayi, tüm özel ve tüzel kişiler de dâhil olmak üzere siber uzayın ülkemiz ölçeğindeki tüm bileşenlerini kapsar.

10.5. Güncelleme

Ülkemizin siber güvenlik alanındaki politika belgesi olma özelliği taşıyan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023); teknolojik gelişmeler, güncel koşullar, değişen ulusal ihtiyaçlar ve gereksinimler göz önünde bulundurularak

ihtiyaç duyulması halinde güncellenecektir. Ayrıca, bu Eylem Planı'nda yer alan ve faaliyet dönemi içerisinde tamamlanamayan eylem maddeleri ihtiyaç halinde bir sonraki Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'na aktarılacaktır.

10.6. Stratejik Amaçlar-Eylem Maddeleri İlişkisi

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023) kapsamında belirlenen hedeflere ulaşılabilmesi için 8 stratejik amacın her biri, gerçekleştirilmesi planlanan 38 eylem maddesiyle ilişkili biçimdedir. Söz konusu eylem maddeleri ise toplam 71 uygulama adımından oluşmaktadır. Eylem maddelerinde yer alan faaliyetler sorumlu 14 farklı kamu kurumu ve iş birliği yapılacak 32 farklı kamu kurumunun çalışmalarıyla yürütülecektir. Ayrıca, bazı uygulama adımları için tüm bakanlıklar ile düzenleyici ve denetleyici kurumlar, üniversiteler ve STK'lar da sorumlu ve iş birliği yapılacak kurumlar arasında yer almaktadır. Belirlenen stratejik amaçların, eylem maddeleri ile ilişkisi aşağıdaki tabloda açıklanmaktadır.

	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	E12	E13	E14	E15	E16	E17	E18	E19
I. Kritik Altyapıların Korunması ve Mukavemetin Artırılması	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓								✓	
II. Ulusal Kapasitenin Geliştirilmesi							✓	✓		✓	✓	✓	✓	✓	✓	✓	✓		✓
III. Organik Siber Güvenlik Ağı																		✓	
IV. Yeni Nesil Teknolojilerin Güvenliği												✓							
V. Siber Suçlarla Mücadele																	✓	✓	
VI. Yerli ve Milli Teknolojilerin Geliştirilmesi ve Desteklenmesi												✓							
VII. Siber Güvenliğin Milli Güvenliğe Entegrasyonu																			
VIII. Uluslararası İş Birliğinin Güçlendirilmesi										✓								✓	

	E20	E21	E22	E23	E24	E25	E26	E27	E28	E29	E30	E31	E32	E33	E34	E35	E36	E37	E38
I. Kritik Altyapıların Korunması ve Mukavemetin Artırılması	✓		✓	✓	✓	✓	✓								✓		✓	✓	
II. Ulusal Kapasitenin Geliştirilmesi	✓	✓						✓	✓	✓				✓					
III. Organik Siber Güvenlik Ağı	✓	✓																	
IV. Yeni Nesil Teknolojilerin Güvenliği			✓	✓	✓	✓	✓												
V. Siber Suçlarla Mücadele	✓	✓	✓			✓		✓	✓	✓	✓	✓	✓	✓					✓
VI. Yerli ve Milli Teknolojilerin Geliştirilmesi ve Desteklenmesi					✓		✓					✓			✓	✓	✓		
VII. Siber Güvenliğin Milli Güvenliğe Entegrasyonu																		✓	
VIII. Uluslararası İş Birliğinin Güçlendirilmesi													✓	✓					✓

T.C. ULAŞTIRMA VE ALTYAPI BAKANLIĞI

Hakkı Turayliç Caddesi No:5 Emek
Çankaya / Ankara / Türkiye
www.uab.gov.tr