ULUSAL SİBER GÜVENLİK STRATEJİSİ VE EYLEM PLANI

2024-2028

ULUSAL SİBER GÜVENLİK STRATEJİSİ

2024-2028

Türkiye olarak büyük hedeflerimiz var. Tarihimizden aldığımız güçle, birikim ve tecrübelerimizle geleceğimizin inşası için tüm gücümüzle çalışmayı sürdürüyoruz.

Hedeflerimize emin adımlarla yürürken en güncel ve en etkili teknolojik imkanların bizlere eşlik etmesi fark yaratıyor. Ülkemiz ekonomik ve sosyal kalkınma yolundaki kazanımlarını, bilgi ve iletişim teknolojilerindeki gelişmelerle daha da ileriye taşıyor.

Teknolojiyi yalnızca kullanan değil üreten bir ülke olarak çalışmalarımızı sürdürüyoruz. Vatandaşlarımızın, kurum ve kuruluşlarımızın, haberleşme, finans, sağlık, ulaştırma gibi kritik altyapılarımızın; teknolojinin getirdiği siber risklerden ve tehditlerden korunması için de gerekli ve etkili adımları atıyoruz.

Siber tehditlerle mücadelemizi, 7/24 görevinin başında olan siber güvenlik organizasyonumuzla birlikte yerli ve milli teknolojilerimizden de yararlanarak gerçekleştiriyoruz.

Siber güvenlik, milli güvenliğimizin ayrılmaz bir parçasıdır. Bu çerçevede, teknoloji ve siber güvenlik alanlarındaki dünya gündeminin yanı sıra ulusal ihtiyaçlarımız dikkate alınarak Ulaştırma ve Altyapı Bakanlığı tarafından kamu, özel sektör, sivil toplum kuruluşları ve üniversitelerle iş birliği içinde hazırlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024–2028) 'nın milletimize ve ülkemize hayırlı olmasını diliyorum.

Güvenli bir Türkiye Yüzyılı'nın inşası için siber güvenlik çalışmalarımıza kararlılıkla devam edeceğiz.

Recep Tayyip ERDOĞAN

Cumhurbaşkanı

Teknolojik gelişmeler büyük bir hızla ilerlerken siber güvenlik çalışmalarımız aralıksız devam ediyor. Yeni teknolojiler ile gelişen ve karmaşıklaşan siber risk ve tehditler karşısında siber sahamızın 7/24 korunması için özverili teknik çalışmalar gerçekleştiriyor, politika ve stratejilerimizi inşa ediyoruz.

Türkiye olarak siber güvenlik alanında çalışmalarını ilk gerçekleştiren, tedbirlerini alan, ulusal siber güvenlik politikaları oluşturan ülkeler arasındayız. Süreklilik arz eden ve güncellenen stratejik yaklaşımımızın parçası olarak siber güvenlik alanında ülke vizyonumuzu ve gerçekleştireceğimiz çalışmaları ortaya koyan, Ulaştırma ve Altyapı Bakanlığı olarak yayımladığımız ve 2013-2014, 2016-2019, 2020-2023 yıllarını kapsayan Ulusal Siber Güvenlik Stratejisi ve Eylem Planları doğrultusunda birçok kazanımı hep birlikte elde ettik.

Kritik altyapılarımızın korunmasından yerli ve milli siber güvenlik teknolojilerimizin geliştirilmesine ve kullanılmasına, yetkin insan kaynağımızın geliştirilmesinden uluslararası siber güvenlik çalışmalarımıza tüm boyutlarıyla siber güvenliğe yön verecek faaliyetlerimiz önümüzdeki dönemde de artarak devam edecek.

Sayın Cumhurbaşkanımızın liderliğinde ortaya koyduğumuz Türkiye Yüzyılı vizyonu doğrultusunda hazırlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028) kapsamında gerçekleştirilecek çalışmaların hayırlı olmasını temenni ediyor, hazırlık aşamasında emeği geçen tüm paydaşlarımıza teşekkür ediyorum.

Abdulkadir URALOĞLU

Ulaştırma ve Altyapı Bakanı

İÇİNDEKİLER

1. GİRİŞ

Küreselleşmenin itici güçlerinden biri olan bilgi ve iletişim teknolojileri, günümüzde toplumsal hayatın ve ekonominin önemli bir parçası haline gelmiştir. Kamu, özel sektör ve bireyler tarafından yaygın olarak kullanılan bu teknolojiler, sürdürülebilir büyüme ve kalkınmada anahtar rol oynamaktadır.

Bu konuya ilişkin çarpıcı verilerden biri internet kullanıcı sayısındaki artıştır. 2023 yılında dünya genelinde 5 milyarın üzerinde kullanıcının olduğu görülmektedir. Araştırmalara göre; Türkiye'de internet kullanıcılarının günlük ortalama 7,5 saat internette zaman geçirmekte ve bunun yaklaşık 3 saatini sosyal medya üzerinde harcamaktadır.

Ayrıca; birbirine bağlı cihaz sayısının ve akıllı uygulamaların artması ile tüm dünyada üretilen veri miktarında da ciddi bir artış yaşanmaktadır. Üretilen bu verinin 2025 yılına kadar 180 zettabaytın üzerine çıkacağı öngörülmektedir. Veri miktarının çok büyük boyutlara ulaşması nedeniyle veri işlemeye dayalı hizmetler ve çözümler gerek iş hayatında gerekse gündelik yaşamda önemli bir yer tutmaya başlamıştır.[1][2]

Yaşanan bu gelişmeler sonucunda bir yandan artan hizmet ve çözümlerden en üst seviyede faydalanılması amaçlanırken diğer yandan da bu hizmet ve çözümlerin sunulduğu altyapıları siber risk ve tehditlerden korunması, hizmet sürekliliğinin ve veri güvenliğinin sağlanması için faaliyetler yürütülmektedir. Tüm bu çalışmaların sonucunda kamu hizmetlerinin ve kritik sektörlerde yürütülen faaliyetlerin etkin ve verimli bir şekilde sunulması, bireylerin gündelik yaşamlarını güvenli bir şekilde sürdürebilmesi hedeflenmektedir.

Siber ortamdaki kurum, kuruluş ve kullanıcıların varlıklarının korunması devletlerin ve kurumların en önemli önceliklerinden biridir. Siber saldırıların maliyetleri gerek kamu gerekse özel sektör kuruluşları için çok ciddi boyutlara ulaşabilmektedir. 2024 yılında

---

[1] https://www.guvenliweb.org.tr/dosya/HQTLP.pdf
[2] https://www.statista.com/statistics/871513/worldwide-data-created

siber suçların küresel maliyetinin yıllık 9,5 trilyon Amerikan Dolarına ulaşacağı öngörülmektedir. Siber güvenlik konusu değerlendirildiğinde sadece teknolojik tedbirlerin yeterli olmadığı, siber güvenliğin teknik bir konu olmanın ötesinde bir anlam taşıdığı, ulusal ve uluslararası güvenlik stratejilerinin bir parçası haline geldiği görülmektedir.

Siber güvenliğin sağlanmasında, teknolojik tedbirlerin yanı sıra insan faktörü de büyük önem taşımaktadır. Siber güvenlik zafiyetlerinin önemli kısmının bireysel ihmallerden kaynaklanması, siber güvenliğin insan unsurunun aktif katılımıyla oluşturulan işgücü tarafından sağlanması ve siber saldırılar sonucunda insan bileşeninin doğrudan veya dolaylı olarak ciddi zararlar görmesi; bu alanda "insan" faktörünün rolünü tüm boyutlarıyla ortaya koymaktadır.

Bunun yanında; dijital dünyada bilginin ve verinin korunmasının, siber tehdit aktörlerinin saldırılarına karşı önlemler alınmasının ve bu saldırılardan kaynaklanabilecek maddi ve itibari kayıpların önüne geçilmesinin anahtarı; ulusal çapta güçlü bir siber "savunmaya" sahip olunmasıdır.

Siber tehditlere karşı etkili siber güvenlik önlemlerinin alınması ve siber "caydırıcılığın" sağlanması amacıyla oluşturulan güvenlik politikalarında;

- Tasarımdan itibaren güvenlik ilkesi gözetilerek sıfır güven yaklaşımının benimsenmesi,
- Bilgi ve iletişim teknolojileri tasarımı ve kullanımında siber güvenliği odak noktası olarak ele alan siber hijyen anlayışının yerleştirilmesi,
- Saldırganlara karşı proaktif bir yaklaşım sergilenmesi,
- Siber güvenlik altyapılarında katmanlı ve kademeli mimarilerin kullanılması

önemli faktörlerdir.

Bu çerçevede; siber güvenliğin sağlanması için güncel ve gelişmiş teknolojilerin kullanılması, siber olaylara müdahale kabiliyetlerinin güçlendirilmesi ve bilgi ve hazırlık seviyelerinin artırılması, kritik önem taşımaktadır.

Bu bağlamda, kamu kurumları, özel sektör, akademi, sivil toplum kuruluşları ve diğer paydaşların koordineli çalışmaları ulusal siber güvenliğe önemli katkılar sağlayacaktır. Siber uzayın sınır tanımaz doğası göz önüne alındığında, ikili, bölgesel ve uluslararası iş birliklerini geliştirmek de etkili bir ulusal siber güvenlik stratejisinin temel unsurlarından biri olarak görülmektedir.

Bu doğrultuda sayıları ve nitelikleri gün geçtikçe artan siber tehditlerle 7/24 mücadele edilmesi, risklerin azaltılması ve siber güvenlik alanında uluslararası seviyede öncü konumumuzun ileriye taşınması amacıyla **Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028)** oluşturulmuştur.

2. TÜRKİYE'DE SİBER GÜVENLİK

Toplumsal hayatta, uluslararası ilişkilerde, ekonomide, sanayide, sağlıkta, eğitimde, bilgi teknolojilerinin kullanıldığı her alanda siber güvenlik vazgeçilmez bir ihtiyaçtır. Birçok Avrupa ülkesinden daha fazla nüfusa sahip olan, stratejik bir bölgede yer alan, bütün dinamikleriyle düzgün ve kesintisiz işleyen güçlü bir devlet yapısına sahip olan ülkemizin teknolojik kazanımları, siber güvenliği de önemseyen stratejik politikalar sayesinde artarak devam etmektedir.

Ülkemiz; jeopolitik önemi, ekonomik yapısı ve teknoloji alanında özellikle son yıllarda gerçekleştirmiş olduğu hamleleri nedenleriyle siber tehdit aktörleri için cazibe alanı oluşturmaktadır. Bu bilinçle ülkemiz, siber güvenlik alanında gerçekleştirdiği özverili çalışmalarla, geçmişten elde ettiği tecrübeleri günümüz teknolojik imkanlarıyla birlikte mümkün olan en üst seviyede değerlendirerek, yurt içindeki ve yurt dışındaki paydaşları ile iş birliğini geliştirerek siber uzay kaynaklı tüm olumsuz etkileri asgariye indirme yönünde önemli adımlar atmaktadır.

Nitelikli insan kaynağına yatırım yapılmasına, güncel teknolojilerden yerli ve millî imkanlarla en üst seviyede faydalanılmasına, bireyleri ve ulusal çıkarları gözeten politikaların uygulanmasına yönelik tüm çalışmalar sonucunda ülkemiz dijital çağın yaşandığı ve modern toplum yaşantısının hedeflendiği günümüzde elde ettiği kazanımları artırmaya devam edecektir.

Ülkemiz, ulusal siber güvenliğin sağlanmasına yönelik olarak erken dönemde aldığı tedbirler ve oluşturduğu ulusal siber güvenlik organizasyonu ile bu alanda öne çıkan ülkeler arasında yer almaktadır.

5809 sayılı Elektronik Haberleşme Kanunu kapsamında, ulusal siber güvenliğin sağlanması amacıyla politika ve stratejilerin geliştirilmesi ile eylem planlarının hazırlanması, bunlara ilişkin izleme ve değerlendirme faaliyetlerinin gerçekleştirilmesi,

koordinasyonun sağlanması görev ve sorumlulukları Ulaştırma ve Altyapı Bakanlığına verilmiştir. [3]

Kanun kapsamında ayrıca Bilgi Teknolojileri ve İletişim Kurumuna siber saldırıların engellenmesi ve caydırıcılığın sağlanması görevleri ile bu görevler kapsamında yükümlülüklerini yerine getirmeyen ilgili taraflara yaptırım uygulama yetkisi verilmiştir.[4]

Ayrıca, 1 no'lu Cumhurbaşkanlığı Kararnamesi ile Dijital Dönüşüm Ofisine (CBDDO), bilgi güvenliğinin ve siber güvenliğin artırılmasına yönelik projelerin geliştirilmesine ilişkin görev ve sorumluluklar verilmiştir.

Mezkûr kararname ile Sanayi ve Teknoloji Bakanlığına ileri teknolojiler ile büyük veri, yapay zekâ, siber güvenlik gibi kritik alanlarda bireylerin ve işletmelerin Ar-Ge ve üretim yetkinliklerinin artırılması amacıyla politika ve strateji önerileri oluşturulması, girişimlerin desteklenmesi görev ve sorumlulukları verilmiştir.

Yine 1 sayılı Cumhurbaşkanlığı Kararnamesi ile; Cumhurbaşkanı'na bağlı çalışan Güvenlik ve Dış Politikalar Kuruluna "Siber güvenlik ile ilgili politika ve strateji önerileri geliştirmek" görevi verilmiştir.

"Siber güvenliğin sağlanması, bu alanda güçlü stratejiler oluşturulmasıyla mümkündür." anlayışıyla Ulaştırma ve Altyapı Bakanlığı tarafından 2012 yılından itibaren sürdürülen

---

[3] **Bakanlığın Görev ve Yetkileri** MADDE 5 (1) h) 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.

[4] 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.

çalışmalar kapsamında hazırlanarak yayımlanan; *2013-2014*, *2016-2019* ve *2020-2023* dönemlerini kapsayan "Ulusal Siber Güvenlik Stratejileri ve Eylem Planları" ile ülkemizde bu alanda stratejik yaklaşımın geliştirilmesi ve siber güvenlik çalışmalarının ulusal seviyede hazırlanan planlamalar doğrultusunda, süreklilik içerisinde yürütülmesi sağlanmıştır.

Söz konusu eylem planlarına ilişkin izleme ve değerlendirme çalışmaları, eylemlerden sorumlu kurum ve kuruluşlarla iş birliği içerisinde Ulaştırma ve Altyapı Bakanlığı tarafından yürütülmüştür.

2013-2014 dönemini kapsayan ve ülkemizin siber güvenlik alanında ilk strateji ve eylem planı olma özelliğini taşıyan *"Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"*, 20 Haziran 2013 tarihli ve 28683 sayılı Resmî Gazete'de yayımlanmıştır.

Siber güvenlik mevzuatının geliştirilmesi, kritik altyapıların güvenliğinin sağlanması, toplumda siber güvenlik farkındalığının oluşturulması, siber tehditlerin tespiti ve önlenmesi konularında bu dönem içerisinde elde edilen kazanımlarla, stratejik seviyede ele alınan ulusal siber güvenlik çalışmalarının kazanımları elde edilmeye başlanmıştır.

Ayrıca 2013 yılında, BTK bünyesinde faaliyetlerini sürdüren Ulusal Siber Olaylara Müdahale Merkezi (USOM), ülkemizde siber güvenlik olaylarına müdahalede ulusal koordinasyonun sağlanması ve uluslararası temas noktası olarak görev yapması adına kurulmuştur. USOM; ülke genelinde siber güvenlik anlayışının geliştirilmesi, siber tehditlerin önlenmesi amacıyla alarm ve uyarıların üretilmesi ile duyuru faaliyetlerinin yürütülmesi, kritik durumlarda yerinde müdahale ekipleriyle olay kontrolünün ele alınması ve siber olaylara müdahalede ulusal koordinasyonun sağlanması amacıyla faaliyetlerini sürdürmektedir. İnternet aktörleri, kolluk güçleri, uluslararası kuruluşlar, araştırma merkezleri ve özel sektör arasındaki iletişim ve koordinasyon USOM vasıtasıyla gerçekleştirilmektedir.

Bununla birlikte 11 Kasım 2013 tarihli ve 28818 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren "Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ" ile USOM koordinasyonunda 7/24 faaliyet

gösterecek şekilde kritik altyapı sektörlerinde Sektörel Siber Olaylara Müdahale Ekiplerinin (Sektörel SOME) kurulması, kurumlar bünyesinde de Kurumsal SOME'lerin kurulması düzenlenmiş olup kurulacak olan SOME'lerin yapısı ve görevlerine yönelik düzenlemeler yapılmıştır. Böylece ülkemizde teknik seviyedeki siber güvenlik yapılanması USOM, Sektörel SOME'ler ve Kurumsal SOME'ler olarak şekillenmiştir.

2016-2019 dönemini kapsayan *"2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı"* ile birlikte bu alandaki stratejik yaklaşımın sürekli hale getirilmesine yönelik yeni bir adım atılmıştır.

Gerçekleştirilen çalışmalarla 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 millî güvenliğe entegrasyonu konularında önemli faaliyetler gerçekleştirilmiştir.

Bu çerçevede;

- Ulusal siber güvenlik kapasite inşası programı ile SOME'lerin insan kaynağının iyileştirilmesi ve siber olaylara hazırlık seviyesinin artırılması sağlanmış,
- Ülkemizin ihtiyaç duyduğu insan kaynağının yetiştirilmesine yönelik olarak eğitim, kamp ve yarışma gibi faaliyetler gerçekleştirilmiş,
- Teknolojik önlemler programı kapsamında, yapay zekâ ve makine öğrenmesi imkânlarını kullanan AVCI, AZAD ve KASIRGA gibi hızlı tespit ve erken müdahale sistemleri geliştirilmiş,
- Tehdit istihbaratı edinimi, üretimi ve paylaşımı programı kapsamında ulusal ve uluslararası paydaşlarla iki yönlü bilgi paylaşımı ve koordinasyon çalışmaları hayata geçirilmiş 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.

2020-2023 dönemini kapsayan ve günümüze dek elde edilen kazanımların daha ileriye taşınması, siber tehditlerin etkilerinin azaltılması, ulusal kapasitenin geliştirilmesi, güvenli bir siber ortamın oluşturulması ve ülkemizin siber güvenlik alanında uluslararası seviyede en üst sıralarda yer alması hedefleriyle oluşturulan *"Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023)"*; 29 Aralık 2020 tarihli ve 31349 sayılı Resmî Gazete'de, 2020/15 sayılı Cumhurbaşkanlığı Genelgesi ile yayımlanmıştır.

Strateji belgesi ile siber güvenliğe ilişkin 8 stratejik amaç belirlenmiştir. Eylem Planı çerçevesinde;

- Kritik altyapıların korunması ve mukavemetin artırılması,
- Ulusal kapasitenin geliştirilmesi,
- Organik siber güvenlik ağı oluşturulması,
- Yeni nesil teknolojilerin güvenliğinin sağlanması,
- Siber suçlarla mücadelenin geliştirilmesi,
- Yerli ve millî teknolojilerin geliştirilmesi ve desteklenmesi,
- Siber güvenliğin millî güvenliğe entegrasyonu ve
- Uluslararası iş birliğinin geliştirilmesi

konularında önemli adımlar atılmıştır. Bu kapsamda:

- Siber olaylara müdahale ekiplerinin olgunluk seviyelerinin ölçülmesine ve yükseltilmesine yönelik olarak uluslararası örneklerle uyumlu bir olgunluk modeli hazırlanarak izleme ve değerlendirme mekanizması kurulmuştur.
- Siber tehdit/olay bildiriminde kullanılmak üzere siber tehdit taksonomisi ve siber olayları kritiklik düzeyine göre derecelendirme metodolojisi oluşturulmuştur.
- Kamu kurum ve kuruluşları arasındaki veri trafiğinin güvenli olarak sağlanmasına yönelik KamuNet (Kamu Sanal Ağı) kapsamında sağlanan hizmetlerin sayısı önemli ölçüde artış göstermiş, ağın kullanımının yaygınlaşması sağlanmıştır.

- "Bilgi ve İletişim Güvenliği Tedbirleri" konulu 2019/12 sayılı Cumhurbaşkanlığı Genelgesi'nin uygulanmasına yönelik olarak 2020 yılında "Bilgi ve İletişim Güvenliği Rehberi", 2021 yılında ise "Bilgi ve İletişim Güvenliği Denetim Rehberi" yayımlanmıştır.
- Kamu kurumlarınca bilgi güvenliği yönetim sisteminin (BGYS) uygulanmasının yaygınlaştırılması yönünde çalışmalar yapılmıştır.
- Kamu kurumlarında açık kaynak kodlu yazılım kullanımını artırmak amacıyla "Kamuda Açık Kaynak Kodlu Yazılım Kullanımı" hakkında Cumhurbaşkanlığı Genelgesi 29 Temmuz 2023 tarihinde yürürlüğe girmiştir.
- TEKNOFEST kapsamında 2018 yılından bu yana düzenli olarak siber güvenlik yarışmaları düzenlenmektedir. 2023 yılında "HackMasters" adını alan yarışmalarda her yıl siber güvenliğin farklı konseptleri ele alınmaktadır.

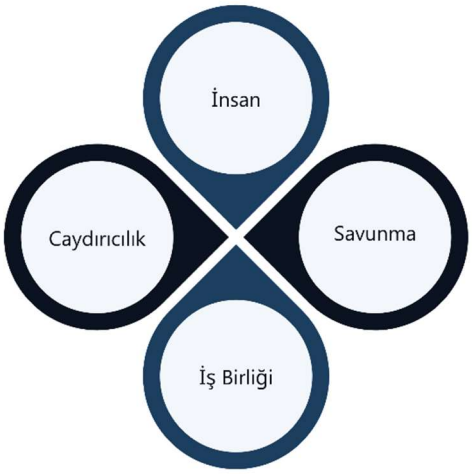
- Sektörel, ulusal ve uluslararası siber güvenlik tatbikatları ile başta kritik altyapılar olmak üzere ülkemizin siber ortamdaki varlıklarının korunmasına, siber güvenlik alanında görev yapan insan kaynağının yetkinliğinin artırılmasına, ulusal ve uluslararası paydaşlar arasındaki iş birliğinin geliştirilmesine yönelik faaliyetler gerçekleştirilmiştir.
- Çevrim içi ve laboratuvar ortamında uygulamalı siber güvenlik eğitimleri ile ülkemizde yetişmiş insan kaynağının ve yetkinlik seviyelerinin artırılmasına katkı sağlanmıştır.
- Kamu ve özel sektör kurumlarında ve kuruluşlarında, kolluk kuvvetlerinde ve adli bilişim alanında görev yapan personelin uzmanlaşmasına yönelik eğitimler verilmiş, kolluk ve adli bilişim eğitim kurumlarında da ilgili müfredat güncellenerek eğitimlerin verilmesi sağlanmıştır.
- Kuantum tabanlı güvenlik konularına ilişkin çalışmalar gerçekleştirilmiş, yapay zekâ, büyük veri, blok zincir gibi alanların siber güvenlikle etkileşimi incelenerek rehber dokümanlar oluşturulmuştur.

- Yerli ve millî ürünlerin ve teknolojilerin yaygınlaşmasına yönelik teşvik ve destek programlarının geliştirilmesi sağlanarak uluslararası pazarlarda rekabet edebilecek siber güvenlik ürünlerinin ve hizmetlerinin üretilmesine ilişkin 100'den fazla projeye destek sağlanmış, E-Turquality (Bilişimin Yıldızları) Programı kapsamında teşvikler verilmeye başlanmıştır.
- Toplumun tüm kesimlerinde siber risklere ve tehditlere karşı siber güvenlik farkındalığının artırılmasına yönelik eğitimler ve etkinlikler gerçekleştirilmiştir.
- Ülkemizde siber güvenlik alanında 4 üniversite araştırma odaklı misyon farklılaşması kapsamında ihtisas üniversitesi olarak belirlenmiş, 2 üniversite de öncelikli alanlar arasında yer alan bilgi güvenliği alanında uzmanlaşan üniversite olarak değerlendirilmiştir. Üniversitelerdeki siber güvenlik araştırma ve uygulama merkezlerinin sayısı 14'e ulaşmıştır.
- Siber güvenliğin, mesleki ve teknik eğitim kapsamında değerlendirilmesi çerçevesinde; millî eğitimde siber güvenlik konularının yer aldığı mevcut eğitim müfredatı güncellenmiştir. Bununla birlikte yalnızca siber güvenlik temelli eğitim vermek üzere Mesleki ve Teknik Anadolu Lisesi ile üniversitelerde Meslek Yüksek Okulları açılmıştır.
- Siber güvenlik alanındaki mesleklere ilişkin ulusal meslek standardı ve ulusal mesleki yeterlilikler belirlenerek yürürlüğe girmiştir.
- İlk ve orta dereceli okullarda bilgi güvenliği, siber güvenlik ve siber zorbalık gibi konuların yer aldığı müfredat güncellenerek öğrenim gören çocuklarımızın ve gençlerimizin bilgi ve bilinç düzeylerinin artırılması sağlanmıştır.
- Çocukların çevrim içi güvenliğinin sağlanmasına yönelik "Çocukların Korunmasına Yönelik Çevrim İçi Güvenlik Stratejisi (2022-2024)" yayımlanmıştır.
- USOM, MITRE-CVE (Common Vulnerabilities and Exposures) Programı'na dahil olmuş ve bu kapsamda üçüncü taraf yazılımların, donanımların veya ürünlerin güvenlik açıkları için CVE numaraları atanma çalışmalarına başlanmış, güvenlik açığı yönetim süreçlerinin koordinasyonu sağlanmıştır.

- İkili, bölgesel ve uluslararası iş birlikleri geliştirilmiş, uluslararası organizasyonların politika ve strateji belirleyici faaliyetleri ile siber olaylara müdahale merkezleri tarafından oluşturulan organizasyonlara ve etkinliklere katılım ve katkı sağlanmış, mutabakat muhtıraları imzalanmıştır.

Yapılan bu çalışmalar kapsamında son dönemde ülkemizde gerçekleştirilen siber güvenlik faaliyetlerinin bir sonucu olarak Uluslararası Telekomünikasyon Birliği (ITU) tarafından ülkelerin siber güvenlik konusundaki olgunluğunu ölçmekte kullanılan güncel *"Global Siber Güvenlik Endeksi"* verilerine göre Dünya genelinde 200'e yakın ülke arasında 2017 yılında 43'üncü ve 2018 yılında 20'nci sıradayken 2020 verilerine göre **11'inci** sıraya yükselme başarısını göstermiştir. Avrupa'da ise 2017 yılında 22'nci ve 2018 yılında 11'inci sırada yer almaktayken 2020 verilerine göre **6'ncı** sıraya yükselmiş bulunmaktadır.

3. STRATEJİ VE EYLEM PLANI BİLEŞENLERİ



"İnsan", "Savunma", "Caydırıcılık" ve ***"İş Birliği"*** temalarındaki unsurlardan yola çıkılarak hazırlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028), stratejik siber güvenlik yaklaşımının somut kazanımlara dönüştürülmesine yönelik bir yapıda planlanmıştır.

Strateji ve Eylem Planı'nın gerçekleştirilme yönteminin ana unsurlarını oluşturan 6 stratejik amaç, 18 hedef ve 61 eylem maddesine ilişkin açıklamalar aşağıda yer almaktadır:

Stratejik Amaçlar

Stratejik yaklaşım kapsamında, odak alanları belirlenmesi ve çalışmaların bu odak alanları üzerinden yürütülmesi önem taşımaktadır.

Anılan temaların, ulusal siber güvenlik çalışmalarının önemli birer bileşeni olması doğrultusunda, Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028) kapsamında 6 stratejik amaç belirlenmiştir.

Hedefler

Hedefler, stratejik amaçlarla doğrudan ilişkilendirilerek hedef bazlı gelişimin sağlanması amaçlanmıştır.

Ulusal siber güvenlik hedefleri, ülkemizin; sürdürülebilir kalkınma ve büyüme gibi büyük ölçekli önceliklerine katkı sağlayacak şekilde belirlenmiştir.

Söz konusu hedefler bütününün tamamlanması ise tespit edilen stratejik amaçlara ulaşmayı sağlayacaktır.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028) kapsamında stratejik amaçlar çerçevesinde 2028 yılına kadar ulaşılması planlanan 18 hedef belirlenmiştir.

Eylem Maddeleri

"Eylem Planı" bölümü kapsamında, stratejik amaçlar çerçevesinde gerçekleştirilecek faaliyetleri içeren eylem maddeleri ortaya konmuştur.

Her bir eylem maddesi kapsamında, gerçekleştirilecek faaliyetler belirlenmiştir. Eylem maddeleri, ulaşılması planlanan hedeflere giden yolda gerçekleştirilecek çalışmaları anlatmaktadır.

Eylem maddelerine ilişkin sorumlu kurumlar, iş birliği yapılacak kurumlar, tamamlanma tarihleri belirtilmiştir. Ayrıca, her bir eylem maddesi kapsamında yer alan açıklama kısımları içerisinde, gerçekleştirilecek çalışmaların detaylı içeriği, eylemin konusu ile ilgili hususlar, uygulama önerileri ele alınmıştır.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028) kapsamında 61 eylem maddesi yer almaktadır.

Gerçekleştirme Yaklaşımı

İzleme ve Değerlendirme

Ulusal Siber Güvenlik Stratejisi'nin tamamlayıcısı niteliğinde olan Eylem Planı'nda yer alan eylem maddeleri, belirlenen stratejik amaçlar çerçevesindeki ulusal siber güvenlik hedeflerine ulaşılmasına yönelik olarak hazırlanmıştır.

Eylem maddeleri kapsamında gerçekleştirilecek çalışmaların, somut hedeflerin işaret ettiği kazanımlara dönüşmesi amaçlanmaktadır.

Bu çerçevede Eylem Planı'nın izlenmesi ve değerlendirilmesi yöntemi; belirlenen hedeflere ulaşılması noktasında kaydedilen ilerlemelerin ortaya konması ve bu ölçekte yapılan tüm çalışmaların hedefe ulaşılıp ulaşılmadığı açısından değerlendirilmesi üzerine kurgulanmıştır.

Ulaştırma ve Altyapı Bakanlığı tarafından yapılacak izleme ve değerlendirme çalışmaları; her bir eylem maddesi için belirlenmiş olan performans kriterleri gözetilerek eylem maddelerinin gerçekleştirilmesine ilişkin yürütülen çalışmaları da içerecek şekilde, hedeflere ulaşılması kapsamında ortaya konan tüm faaliyetlere ve bu noktalardaki gelişmelere ilişkin raporlamalar temelinde, periyodik olarak, eylemlerden sorumlu ve ilgili kurum ve kuruluşlardan alınacak girdilerle sağlanacaktır.

Paydaşlar

Ulusal siber güvenlik çalışmaları; ülkemizin ortaya koyduğu vizyon doğrultusunda, siber güvenliğin ve bilgi güvenliğinin temel prensipleri dikkate alınarak tüm paydaşların katılımıyla gerçekleştirilmektedir.

Bu çerçevede, Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028), siber güvenlik alanındaki paydaşların değerli katkıları alınarak hazırlanmıştır. Paydaşlarla birlikte atılacak adımların belirlenmesi ile hedeflere birlikte ulaşılması planlanmıştır.

Hedefler ve eylem maddeleri belirlenirken mevcut durum, yürütülmesi gerekli faaliyetler, muhtemel kaynak ihtiyaçları, faaliyetlerin öngörülen gerçekleştirilme süreleri dikkate alınmış; eylemlerden sorumlu kurumlar ve kuruluşlar, iş birliği yapılabilecek kuruluşlar ve tamamlanma tarihleri bu doğrultuda belirlenmiştir.

Eylem maddeleri, sorumlu kurumların koordinatörlüklerinde ilgili kurumlarla/kuruluşlarla iş birliği halinde yürütülecek çalışmalarla gerçekleştirilmek üzere hazırlanmıştır.

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.

Güncelleme

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı; teknolojik gelişmeler, güncel koşullar, değişen ulusal ihtiyaçlar ve gereksinimler göz önünde bulundurularak ihtiyaç duyulması halinde güncellenmektedir.

Ülkemizin siber güvenlik alanındaki vizyon belgesi olan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028) kapsamında yer verilen amaçlar, hedefler ve faaliyet dönemi içerisinde tamamlanamayan eylem maddeleri; izleme ve değerlendirme çalışmaları kapsamında periyodik olarak gözden geçirilmelerinin ardından nihai değerlendirmeler sonucunda, ihtiyaç halinde bir sonraki Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'na aktarılacaktır.

4. STRATEJİK AMAÇLAR

Türkiye Yüzyılı vizyonunun gerçekleştirilmesine katkı sağlayacak olan ulusal siber güvenlik çalışmalarının sistemli bir yaklaşımla ele alınmasına, mevcut kazanımların geliştirilmesine ve yeni kazanımlar elde edilmesine yönelik olarak 12. Kalkınma Planı doğrultusunda, 2024-2028 dönemi için odaklanılan ve temalar çerçevesindeki unsurlardan yola çıkılarak belirlenen stratejik amaçlar detaylı olarak aşağıda açıklanmaktadır:

| Siber Dayanıklılık

Karmaşıklığı ve sıklığı artan siber tehditler; büyük ölçekli ekonomik zararlara, can kaybına, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına neden olabilmektedir. Siber tehditlerin olumsuz etkilerinin artmasının ve yıkıcı boyutlara ulaşmasının önüne geçilmesi için başta kritik altyapılar olmak üzere kamu ve özel sektördeki bilgi ve iletişim teknolojileri altyapılarının ve verilerin korunmasına yönelik nitelikli çalışmaların gerçekleştirilmesi gerekmektedir. Uluslararası alanda gündemde olan gelişmeler ve iyi uygulama örnekleri doğrultusunda ulusal, kurumsal ve bireysel bazda, ***iş birliği*** içerisinde alınacak tedbirler ile kurumlar, kuruluşlar ve kritik altyapı sektörlerindeki bilgi ve iletişim teknolojileri altyapılarının ve verilerinin siber risklere ve tehditlere karşı dayanıklılığının ve ***savunma*** etkinliğinin artırılması amaçlanmaktadır.

Siber dayanıklılığın sağlanması için esas olan noktalardan birisi, güvenliğe yönelik risklerin belirlendiği, değerlendirildiği, risk azaltma çalışmalarının gerçekleştirildiği ve izlendiği mekanizmalar üzerine kurgulanan risk temelli analiz yaklaşımının uygulanmasıdır. Anılan yaklaşımın acil durum ve iş sürekliliğine yönelik planlamalar ile desteklenmesi; bu anlayışın kurumsal, sektörel ve ulusal seviyede daha da ileriye taşınması ile siber tehditlerle mücadeledeki uzmanlığın, planlamalar doğrultusunda daha etkin biçimde kullanılması önemli ölçüde fayda sağlayacaktır. Bu kapsamda ulusal ve uluslararası tatbikatlar ile hazırlık seviyesinin ölçülerek siber dayanıklılığın geliştirilmesi planlanmaktadır. Siber güvenliğin millî güvenliğe entegrasyonu noktasında ise hibrit tehditlere mukabele ve mukavemetin artırılması hususundaki çalışmalara devam edilmektedir.

Ayrıca; kritik altyapı sektörlerinde siber güvenlik tedbirlerinin belirlenmesi ve uygulanması noktasında, düzenlemelere ve bu düzenlemeler üzerinden gerçekleştirilen denetlemelere dayalı siber güvenlik yaklaşımının süreklilik arz eden şekilde sağlanması elzemdir. Kurumlar ve kuruluşlar tarafından sağlanan hizmetlere ilişkin veri trafiğinin güvenli mekanizmalar üzerinden gerçekleştirilmesi ile de kamu kurumları özelinde dayanıklılığın sağlanmasına katkı verilmesi hedeflenmektedir.

| Proaktif Siber Savunma ve Caydırıcılık

Siber tehdit aktörlerinde ve saldırı vektörlerinde yaşanan artışla birlikte tehditlerin giderek karmaşık hale gelmesi, siber tehditleri de içinde barındıran hibrit tehditlerin ortaya çıkması, bu unsurlara karşı geliştirilen siber ***savunma*** anlayışının da bununla eş zamanlı ve orantılı olarak geliştirilmesi gerektiğini ortaya koymaktadır.

Siber tehditlerle mücadelede dayanıklı bilgi ve iletişim teknolojileri altyapıları inşa etmenin en etkili yöntemi; ihtiyaçlara uygun siber güvenlik çözümlerine, süreçlerine ve yetkin ***insan*** kaynağına sahip olmanın yanı sıra proaktif bir siber ***savunmanın*** geliştirilmesidir.

Siber olay öncesinin, olay esnasında ve sonrasında gerçekleştirilecek çalışmalar kadar önem taşıdığından hareketle atılacak adımlar, ülkemizde siber ***caydırıcılığın*** sağlanarak riskler ve tehditler oluşmadan önce veya erken aşamalarda iken önüne geçilmesi noktasında avantaj sağlayacaktır.

Olası siber tehditlerin analiz edilmesine ve uygun önlemlerin alınmasına yönelik oluşturulan mekanizmaların, teknolojinin getirdiği imkanlar kullanılarak daha da geliştirilmesi hedeflenmektedir. Bu kapsamda, siber güvenlik zafiyetlerinin tespitine, ilgili taraflara bildirimine ve güncel siber tehdit istihbaratı paylaşımına yönelik ulusal kapasitenin ve kabiliyetlerin artırılarak ulusal siber güvenliği tehdit edecek unsurların yapay zekâ ve büyük veri altyapılarıyla erken tespiti ve önlenmesi amaçlanmaktadır.

Düzenli izleme ve değerlendirme çalışmalarından elde edilecek çıktılar ışığında; ulusal güvenliğimizi korumak ve siber tehditlere karşı proaktif bir duruş sergileyebilmek için siber suçlarla ve tehdit aktörleri ile kapsamlı bir şekilde mücadele edilmesi, ulusal siber alanın korunmasına yönelik olarak 7/24 görev yapan Siber Olaylara Müdahale Ekiplerinin kapasitelerinin sistemli biçimde artırılması, olay müdahale kabiliyetlerinin geliştirilmesi, kurumların ve kuruluşların proaktif ***savunma*** yaklaşımına uyum sağlamaları için gereken rehberliğin sağlanması; önümüzdeki dönemde gerçekleştirilecek çalışmaların genel kapsamını oluşturmaktadır.

| İnsan Odaklı Siber Güvenlik Yaklaşımı

"Şebeke güvenliği", "bilgisayar olaylarına müdahale" ve "bilgi güvenliği" kavramlarının teknolojik ilerlemeler ve güncel gelişmeler çerçevesinde dönüşümü ile ortaya çıkan siber güvenlik konusu; teknolojik altyapı, strateji, mevzuat, eğitim, farkındalık, ***insan*** kaynağı, ulusal ve uluslararası ***iş birlikleri*** hatta suç boyutlarını bünyesinde barındıran disiplinler arası bir kavram haline gelmiştir. Bu boyutların arasında **"*insan*"**, siber güvenlik çalışmalarının odağında yer almaktadır.

Siber güvenlik zafiyetlerinin yaklaşık %80'i ***insan*** unsurunun rol oynadığı ihmallerden kaynaklanmaktadır. Siber güvenlik riskleri ve olası tehditler ile maruz kalınabilecek siber olayların etkilerine ilişkin bilgi düzeylerinin ve farkındalık seviyelerinin artırılması, siber güvenliğin sağlanmasında kritik bir rol oynamaktadır.

Siber saldırılar sonucunda bireylerin, doğrudan ve dolaylı olarak ciddi zararlar görebildiği hususu mutlaka göz önünde bulundurulmalıdır. Başta çocuklar, gençler, yaşlılar ve özel gereksinimli bireyler olmak üzere tüm kesimler, siber saldırılardan doğrudan veya dolaylı olarak etkilenmektedir. Bireylerin siber uzayın içerdiği risklerden uzak tutulması ve bilişim teknolojilerinin sunduğu imkanlardan en üst seviyede faydalanmaları maksadıyla toplumun tüm kesimlerini gözetecek çalışmalar yapılacaktır.

Siber güvenlik faaliyetlerinin, ***insan*** unsurunun aktif katılımıyla oluşturulan işgücü tarafından sağlanması, bu unsuru başka bir bakımdan daha öne çıkarmaktadır. İlk, orta ve yükseköğrenim basamaklarında siber güvenlik eğitim ve öğretiminin geliştirilerek bireylerin farkındalık ve yetkinlik seviyelerinin artırılması, bu alana ilgi duyan kişilerin siber güvenlik uzmanlığına ulaşmalarına giden yolda tüm noktalarda geliştirilen mekanizmalarla desteklenmesi; işgücümüze önemli ölçüde katkı sağlayacaktır. Ayrıca siber tehditlerle ve siber suçlarla mücadelede görev yapan profesyonellerin yetkinliklerini artırmalarına yönelik fırsatların tanınması ile yeni döneme bu alanlarda da önde başlanması hedeflenmektedir.

| Teknolojinin Güvenli Kullanımı ve Siber Güvenliğe Katkısı

Bilgi ve iletişim teknolojilerinin güvenli kullanımı, tüm dünyada artan bir gereklilik haline gelmiştir. Özellikle kritik sektörler için hayati önem taşıyan bu teknolojilerin güvenliği gün geçtikçe daha öncelikli hale gelmektedir.

Yapay zekâ ve blok zincir vb. yenilikçi ve çığır açan teknolojilerin son dönemde büyük bir hızla geliştirilerek bireylerin gündelik hayatına girmesi, hemen her konuda istenilen ve ihtiyaç duyulan bilgiye bazı yapay zekâ araçlarını kullanarak verimli ve etkin biçimde ulaşabiliyor olması dikkat çekmektedir.

Her geçen gün daha fazla kullanıcı akıllı şehir, tarım, ulaşım gibi bilgi ve iletişim teknolojileri bileşenlerine dayalı akıllı uygulamaları kullanmaktadır. 5G ve nesnelerin interneti teknolojileri ile hızla artan bağlantı sayısı, bulut bilişim kullanımı; ortaya çıkan önemli boyutlardaki verinin büyük veri araçlarıyla analiz edilmesi ve analiz sonuçlarından elde edilen öngörülerle yeni planlamalar ve uygulamalar yapılması, dijital ikiz teknolojileri ile bu planlamalara ve modellemelere katkı sağlanması; teknolojinin yönü hakkında önemli fikirler vermektedir.

Günümüzde kötü amaçlı basit bir yazılım, büyük ölçekli bir güvenlik tehdidine dönüşebilmektedir. Bu sebeple, anılan teknolojiler karşısında, *"sıfır güven (zero trust)"* anlayışıyla tedbirlerin belirlenerek güvenli bir siber ortamın ve dijital dönüşümün sağlanması, yeni teknolojilerin güvenliğine yönelik gereksinimlerin ve asgari güvenlik kriterlerinin değerlendirilmesi ve belirlenmesi, önümüzdeki dönemde gerçekleştirilecek siber ***savunma*** ve ***caydırıcılığın*** sağlanması çalışmalarının temelini oluşturmaktadır.

Ayrıca yeni teknolojilerin, siber güvenliğin sağlanmasına ilişkin çalışmalara entegre edilmesine yönelik imkanların araştırılması ve değerlendirilmesi ile ulusal siber güvenlik çalışmalarına katkı sağlanması planlanmaktadır. Özellikle yapay zekâ ve büyük veri altyapılarının bu çalışmalarda değerlendirilmesi ile önemli ölçüde ilerleme kaydedilmesi sağlanacaktır.

| Siber Tehditlerle Mücadelede Yerli ve Millî Teknolojiler

Siber güvenliğin sağlanmasına yönelik çalışmalardan elde edilen bilgiler, edinilen tehdit istihbaratları, uluslararası alanda bilgi ve iletişim teknolojilerine ilişkin tüm başlıklardaki çalışmalar; siber tehditlerin, dünyanın gündemindeki yerini koruma eğiliminde olduğunu göstermektedir.

Tüm boyutlarıyla ele alınması gereken siber tehditlerle mücadelenin ana unsurlarından biri, tehditlerin temel kaynağı olarak öne çıkan teknolojik gelişmeler ve bu gelişmelerin kötü amaçlar için kullanılmasını esas alan tehdit aktörleridir.

Tehdit aktörleri birçok farklı kaynaktan beslenmekte olduğu gibi; oluşturdukları tehditler ile siber uzayın sınırları aşan yapısı dolayısıyla farklı konumlarda yer alan farklı teknolojik bileşenleri hedef alabilmektedir.

Bu doğrultuda, ülkelerin siber uzaydaki tehditlerden korunması noktasında, *"tasarımdan itibaren güvenlik (security-by-design)"* ilkesiyle, yerli ve millî olarak üretilen teknolojiler önemli bir avantaj olarak öne çıkmaktadır. Paydaşların ***iş birliği*** ile yerli ve millî ürün projelerinin oluşturulması, sertifikasyon ve akreditasyon mekanizmalarının geliştirilmesi, bu alanda verilen teşviklerin artırılması ile siber tehditlere karşı yürütülen mücadelenin bütüncül bir yaklaşımla sürdürülmesi planlanmaktadır.

Konu tüm yönleriyle ele alındığında; yerli ve millî siber güvenlik ürünlerine ve hizmetlerine sahip olmanın ve bunların kritik altyapılarda kullanılıyor olmasının, dışa bağımlılığı azaltarak ulusal güvenliğimizin sağlanmasına ve ekonomiye katkıları önemli getiriler olarak öne çıkmaktadır.

Yerli ve millî siber güvenlik ürünleri ve hizmetleri, siber ***savunma*** ve ***caydırıcılık*** faaliyetlerinin yanı sıra ülkemizin millî teknoloji hamlesi kapsamında elde ettiği kazanımlara siber güvenlik boyutunda da katkı sağlayacaktır. Ürünlerimizin ve hizmetlerimizin dünya pazarlarındaki payının artırılarak millî güvenliğimizin yanı sıra sürdürülebilir ekonomik büyümeye ve kalkınmaya da destek verilmesi hedeflenmektedir.

| Uluslararası Alanda Türkiye Markası

Ülkemiz, siber güvenlik alanında uluslararası ölçekte güçlü bir marka olma yolunda önemli adımlar atmaktadır. Teknoloji altyapısı, yetkin ***insan*** kaynağı ve stratejik yaklaşımı; ülkemizin siber güvenlik alanında güçlü bir konumda bulunmasına imkân sağlamaktadır.

Siber uzayda, özellikle uluslararası ölçekte; *"**iş birliği**"* teması öne çıkmakla birlikte bu ***iş birliği*** yalnızca tehditlerle mücadelede operasyonel kapsamda bilgi paylaşımını değil, edinilen bilgi ve tecrübeler doğrultusunda yetkinliklerin karşılıklı olarak geliştirilmesini ve ülkemizin bu konudaki yetkinliğinin ön plana çıkarılarak bölgesel ve uluslararası paydaşlar arasında görünürlüğünün artırılmasını da esas almaktadır.

Ülkemiz, siber güvenlik alanında uluslararası ölçekte gündemin belirlendiği bölgesel ve uluslararası platformlarda aktif rol oynamaktadır. Bu kapsamdaki çalışmalarla, uluslararası seviyede belirlenen siber güvenlik tedbirlerinin ülkemizde uygulanması ve uluslararası paydaşların bu alandaki iyi uygulamalarının siber güvenlik çalışmalarında değerlendirilmesi sağlanmaktadır.

Siber güvenlik alanında Türkiye markasının etkilerinin artırılması amacı çerçevesinde ülkemizin uzmanlığının yol gösterici olarak uluslararası seviyede değerlendirilmesine ilişkin çalışmalar gerçekleştirilecektir. Bu çerçevede, bölgesel ve uluslararası paydaşlarla ikili ve çoklu ***iş birliklerinde*** değerlendirilen hususlarla uyumlu şekilde bilgi ve tecrübe paylaşımı sağlanacaktır. Ayrıca siber güvenlik alanında ülkemizin tutumunun en iyi şekilde aktarılması ve ***iş birliğinin*** geliştirilmesi kapsamında "siber diplomasi" kavramına ilişkin kabiliyetlerimizin geliştirilmesine yönelik çalışmalar gerçekleştirilecektir.

5. HEDEFLER

Hedefler; politikaların ve stratejilerin gerçekleştirilmesinde kritik rol oynamakta, motivasyonun artmasına katkı sağlamakta ve kaynakların etkin kullanılmasını sağlayarak başarı için bir yol haritası çizmektedir. Politikaların ve stratejilerin başarısı; doğru, gerçekçi, izlenebilir ve etkili hedeflerin tespit edilmesine ve bu hedeflere ilişkin gerçekleştirilecek çalışmalara bağlıdır.

Bu doğrultuda; Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028) kapsamında belirlenen hedefler, aşağıda yer almaktadır:

ULUSAL SİBER GÜVENLİK HEDEFLERİMİZ	
Siber Dayanıklılık	
H1.1	Kamu kurum ve kuruluşları ile kritik altyapı sektörlerinde, düzenleme ve denetlemeye dayalı siber güvenlik yaklaşımının geliştirilmesi.
H1.2	Kurumsal, sektörel ve ulusal bazda; risk temelli analizlere ve acil durum planlamalarına dayalı siber güvenlik yaklaşımının benimsenmesi.
H1.3	Veri paylaşımının güvenli altyapılar üzerinden gerçekleştirilmesi.
H1.4	Ulusal standardizasyon ve test mekanizmalarının geliştirilmesi.
Proaktif Siber Savunma ve Caydırıcılık	
H2.1	Siber olaylara müdahale ekiplerinin yetkinlik seviyelerinin artırılması.
H2.2	Siber risklerin ve tehditlerin tespiti ve bildirimi ile siber tehdit istihbaratı edinimi ve paylaşımına yönelik kabiliyetlerin geliştirilmesi.
H2.3	Kurum ve kuruluşlarda risklere ve tehditlere karşı iyi uygulamaların artırılması.

H2.4	Millî güvenliğin bir parçası olarak ulusal siber güvenliğe ilişkin eşgüdümün artırılması.
H2.5	Siber suçlarla mücadeleye yönelik kazanımların artırılması.
	İnsan Odaklı Siber Güvenlik Yaklaşımı
H3.1	Siber uzayın güvenle kullanılması çerçevesinde bireysel ve toplumsal farkındalığın artırılması.
H3.2	Kurumlarda ve kuruluşlarda, kurumsal siber güvenlik kültürünün yerleştirilmesi.
H3.3	İnsan kaynağının güçlendirilmesi ve yetkinliğinin artırılması.
	Teknolojinin Güvenli Kullanımı ve Siber Güvenliğe Katkısı
H4.1	Yeni teknolojilerin güvenli kullanımının sağlanması, oluşabilecek risklere yönelik önlemlerin alınması.
H4.2	Siber güvenliğin sağlanmasına ilişkin çalışmalarda yeni teknolojilerin kullanımının artırılması.
	Siber Tehditlerle Mücadelede Yerli ve Millî Teknolojiler
H5.1	Yenilikçi fikirlerin, yerli ve millî ürün ve hizmetlere dönüşümünün sağlanması.
H5.2	Ar-Ge faaliyetlerinin desteklenerek yerli ve millî siber güvenlik teknolojilerinin geliştirilmesi ve yurt içinde kullanımının yaygınlaştırılması.
	Uluslararası Alanda Türkiye Markası
H6.1	Uluslararası paydaşlarla bilgi paylaşımının ve iş birliğinin artırılması.
H6.2	Yerli ve millî siber güvenlik çözümlerinin uluslararası alanda rekabet gücünün artırılması.

Hedefler ile eylem maddeleri arasındaki ilişki, aşağıdaki tabloda yer almaktadır:

#	H1.1	H1.2	H1.3	H1.4	H2.1	H2.2	H2.3	H2.4	H2.5	H3.1	H3.2	H3.3	H4.1	H4.2	H5.1	H5.2	H6.1	H6.2
E1	X	X																
E2	X	X																
E3	X	X																
E4	X																	
E5		X						X										
E6								X										
E7		X																
E8		X																
E9					X													
E10						X												
E11						X												
E12						X						X						
E13						X												
E14						X												
E15					X			X										
E16			X															
E17			X															
E18			X															
E19	X																	
E20									X									
E21									X									
E22									X									
E23									X									
E24							X											
E25							X											
E26							X											
E27													X					
E28													X					
E29							X						X					
E30							X						X					

#	H1.1	H1.2	H1.3	H1.4	H2.1	H2.2	H2.3	H2.4	H2.5	H3.1	H3.2	H3.3	H4.1	H4.2	H5.1	H5.2	H6.1	H6.2
E31							X						X					
E32							X						X					
E33						X								X				
E34				X										X		X		
E35							X						X					
E36				X														
E37																X		
E38													X			X		
E39		X											X					
E40																		X
E41																X		X
E42															X			
E43															X			
E44																	X	
E45																	X	
E46						X												
E47																	X	
E48																	X	
E49												X						
E50					X							X						
E51											X							
E52											X							
E53												X						
E54											X							
E55												X						
E56										X		X						
E57												X						
E58										X								
E59										X								
E60										X								
E61					X													

ULUSAL SİBER GÜVENLİK EYLEM PLANI

2024-2028

Eylem Planı'nın yer aldığı 32-111 arasındaki sayfalar "Hizmete Özel" nitelikte olduğundan ilgili kurum ve kuruluşlarla paylaşılmaktadır.

T.C. ULAŞTIRMA VE
ALTYAPI BAKANLIĞI

Hakkı Turayliç Caddesi No:5 Emek
Çankaya / Ankara / TÜRKİYE