TÜRKİYE BİLİŞİM DERNEĞİ

Kamu Bilişim Merkezleri Yöneticileri Birliği

Kamu Bilişim Platformu 17

Siber Güvenlik ve Kritik Altyapı Güvenliği Çalışma Grubu

Nihai Rapor

Sürüm 1.0

http://www.tbd.org.tr

5 Ekim 2015

TBD Kamu-BİB

Kamu Bilişim Platformu 17

1. ÇALIŞMA GRUBU

Bu rapor, TBD Kamu Bilisim Merkezleri Yöneticileri Birliği (TBD Kamu-BİB)'nin **onyedinci dönem** çalışmaları kapsamında, 1**. Çalışma Grubu (ÇG1)** tarafından hazırlanmıştır.

Yayını Hazırlayanlar;

Başkan

Ali YAZICI	Bilgi Güvenliği Derneği/ASELSAN

Kamu-BİB YK Temsilcisi

Mariye Umay AKKAYA	Türk Standartları Enstitüsü

Grup Üyeleri

Mehmet Ali İNCEEFE	Bilgi Güvenliği Derneği
Önder ÖZDEMİR	Türkiye Bilişim Derneği
Murat DEMİRKOL	ICTERRA
Harun DEMİR	Bilim Sanayi ve Teknoloji Bakanlığı

Belge No : TBD/Kamu-BIB/2015-ÇG1

Tarihi : 5 Ekim 2015

Durumu : Nihai Rapor – Sürüm 1.0

İçindekiler

YÖNETİCİ ÖZETİ

Siber Güvenlik Konusu tüm ülkeyi, ülkenin kurum ve kuruluşlarını ve toplumun tüm kesimlerini ilgilendiren ve genel anlamda bir koordinasyon içerisinde yürütülmesi gereken bir konudur.

Bugün bilgisayar, akıllı telefon, tablet bilgisayar gibi herhangi bir cihaz kullanan kişiler ve bu altyapıya sahip ve/veya kullanan kurumlar artık siber güvenlik sorunlarının muhataplarından birine dönüşmüş durumdadır. Güvenlik Zafiyetleri, Zararlı Yazılımlar, E-Posta Tehditleri - Spam, Phishing, Siber Casusluk ve Sürekli Tehditler (*APT*) ile Mobil ve Sosyal Medya Tehditleri siber dünyadaki varlığımızı, güvenliğimizi hedef almaktadır.

Türkiye dünya genelinde siber saldırıya uğrayan ve siber saldırı başlatan ülkeler arasında ilk sıralarda yer almaktadır. Siber saldırı başlatma istatistikleri, genel kanının aksine parlak bir gösterge değildir. Zira siber saldırıları başlatan bilgisayarların çoğu uzak kullanıcılar tarafından köleleştirilmiş (*botnet/zombi*) bilgisayarların yine uzaktan kontrolü ile gerçekleştirilen saldırılardır.

Bu veriler tarafından ortaya çıkan durum, gerek kamu, gerek kurum ve kişilerin siber güvenlik açısından gerekli özeni gösterip, gerekli tedbirleri almaktan uzak olduğudur.

Diğer yandan, farkındalığın ötesinde siber güvenlik tedbirleri için gerekli donanım ve yazılımın çok büyük bir bölümü ise yabancı kaynaklı olup, arka kapı gibi kasıtlı güvenlik açık ve zafiyetlerini de içermektedir.

Ülkemizde yapılması hızla gereken işlerden biri de kamu ve özel sektör işbirliğinde yerli siber güvenlik ekosisteminin oluşturulmasıdır.

SİBER DEVLET MEVZUATI

Ülkemizde Siber Güvenlik konusunu bütün yönleriyle ele alarak, bu alanda gerekli olan tüm düzenleme ve denetlemeleri yapacak, ülke adına politika ve strateji geliştirecek bir kurum ve kuruluş bulunmamaktadır. Bu konuyla ilgili faaliyet yürüten kurumlar arasında da bir uyum, eşgüdüm ve koordinasyon da bulunmamaktadır.

Tüm bu alanları düzenleyen kapsamlı bir çerçeve yasanın önemi ve gerekliliği açıktır.

Geçmişte hazırlanan "*Siber Devlet Yasası*" taslağının gündeme alınması ve yasalaştırılması en acil konulardan ve en büyük önceliklerinden biridir.

SİBER GÜVENLİK KURULU

Bakanlar Kurulu'nun 11.06.2012 tarihli ve 2012/3842 sayılı kararı oluşturulan Siber Güvenlik Kurulu, esasen siber güvenlikle ilgili olarak alınacak önlemleri belirlemek,

hazırlanan strateji ve planları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamakla, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı(UDHB) ise onaylanan strateji ve planların uygulanması ile görevli kılınmıştır.

Siber Güvenlik Kurulu tarafından yürütülen faaliyetlerin etkinleştirilmesi ve sürdürülebilir kılınmasına ihtiyaç duyulmaktadır.

SİBER GÜVENLİK EYLEM PLANLARI

Siber güvenlik alanında ülkemizde atılan en büyük adımlardan biri kuşkusuz 20.12.2012 tarihinde Ulusal Siber Güvenlik Strateji Belgesi'nin yayımlamasıdır. Bunun ardından Ulusal Siber Güvenlik Koordinasyon Kurulu'nun oluşturularak Siber Güvenlik Eylem Planı (2013-2014) hazırlanması, UDHB'nın Koordinasyon Makamı olarak belirlenmesi ve Siber Olaylara Müdahale Ekiplerinin (SOME) oluşturulması Türkiye'de devletin ve kurumların siber güvenlik algısını ve yaklaşımını tamamen değiştirmiştir.

2015 yılında UDHB, 2015-2017 Siber Güvenlik Eylem Planını çok daha geniş katılımlı çalıştaylar ile daha etkin ve verimli bir sürece taşımıştır.

Bu Eylem Planı'nın en çarpıcı yanlarından biri ise, Eylem Planı kalemlerinden bazılarının TBD ve BGD gibi STK'ların sorumluluğuna verilmesi yaklaşımıdır.

ULUSAL SİBER GÜVENLİK SEKTÖRÜ

Türkiye siber suçlar ve saldırılar açısından hedef ilk 10 ülke arasındadır. Türkiye aynı zamanda siber saldırı yapan ülkeler arasında ilk sıralarda gözükmektedir.

Başta kamu kurumları olmak üzere kurumsal ve bireysel düzeyde siber güvenlik açısından yeterli farkındalık, bilinç ve bilgi seviyesine henüz ulaşılamamıştır. 2013-14 döneminde 9 banka, 13 sigorta şirketi, 2 telekomünikasyon şirketi, 27 üniversite, 30 kamu kurumu saldırıya uğramıştır.

Yerli siber güvenlik çözümlerinin geliştirilmesi ve kullanımının teşvik edilmesinin bu alanda gelişimimize katkı sağlayacağı değerlendirilmektedir. Kullanılan çözümlerin %97'si yabancı (ithal) olup bunların %55'i İsrail, %35'i ise ABD kökenlidir.

Türkiye'de çoğu küçük ölçekli 40 civarında firma bu alanda faaliyet göstermekte olup bunlar arasında bir sinerji ve güç birliği mevcut değildir. Aynı zamanda bu firmalar bir ulusal strateji doğrultusunda değil dağınık bir yaklaşım ile iş yapmaya çalışmaktadır.

Gerek yerli geliştirilen ve gerekse ithal edilen siber güvenlik çözümleri milli bir sertifikasyon sürecinden geçmeden ve yeterince güvenli olup olmadıkları bilinmeden kullanıma sokulmaktadır.

SİBER GÜVENLİK STANDARTLARI ve ÜRÜN SERTİFİKASYONU

Siber güvenlikte en önemli konu standartlara uyumdur. Siber güvenlik standartları, kullanılan güvenlik sistem ve/veya ürünlerine yönelik oluşabilecek risklerin belirlenmesi ve gerekli olan risk analizlerinin sağlıklı ve maliyet etkin olarak yapılabilmesine olanak sağlamaktadır.

Siber güvenlik konusunda ilgili STK ve sektörün de katılımıyla daha üst güvenlik seviyelerinde ürün veya hizmetlere yönelik olarak asgari güvenlik isterleri tanımlanmalıdır.

SİBER GÜVENLİK EĞİTİMLERİ ve UZMANLAR

Yüksek seviyede bir siber güvenliğin sağlanması için her seviyede farkındalığa ve farkındalığın oluşturulmasına ihtiyaç vardır. Bunun ilk ve orta öğretimden başlamak üzere her seviyede eğitim kurumlarında verilmesi gereklidir. Özellikle siber güvenlik farkındalık eğitimlerinin üniversite müfredatına eklenmesi, yüksek lisans ve doktora programlarının daha fazla açılması, Ar-Ge laboratuarlarının desteklenmesi, test merkezlerinin açılması orta ve uzun dönemli başarı için temel şartlardan bir kaçıdır.

Siber güvenlik strateji belgesi ve eylem planı kapsamında, ülkemizde bu alanda yetişmiş insan gücü açığını kapatmaya yönelik çalışmalar yürütülmesi, belirli hedefler koyarak konuyla ilgili uzman yetiştirilmesi ise oldukça kritik bir konudur.

1. Giriş

Her şeyin sayısallaştığı günümüzde, artık bilişim teknolojilerinin kullanımı birey, sektör ve kamu kurum ve kuruluşları için bir seçenek olmaktan çıkmış zaruret haline dönüşmüştür. Sayısal uzay hiç beklenmedik şekilde genişlemiş ve günlük yaşantımızın, iş hayatımızın ve kamu kurumlarından aldığımız hizmetlerin ayrılmaz bir parçası olmuştur. Dünyada bilgi ve iletişim teknolojilerinin hızlı gelişimi ve yaygın olarak kullanımı sayesinde siber uzaydan yapılan saldırıların niteliğinde ve niceliğinde de önemli artışlar gözlenmektedir.

Siber saldırılar bireyleri, kurum ve kuruluşları hatta devletleri hedef almaktadır. Ülkeler siber güvenliklerini sağlamak amacıyla idari yapılanmalar gerçekleştirmekte, teknik önemler almakta ve hukuki altyapılar hazırlamaktadır. Bu düzenlenmelere dayanak olması amacıyla siber güvenlik stratejisi belgesi birçok ülke tarafından yayımlamış bulunmaktadır. Söz konusu strateji belgelerinde siber saldırılara karşı koymanın yanı sıra bilgi ve iletişim ağlarının siyasi otoriteye, ulusal menfaatlere ve kritik altyapılara karşı kullanılmasının engellenmesine yönelik strateji ve politikaların geliştirilmesi de kapsanmaktadır.

Türkiye'de de konunun önemine binaen Siber Güvenlik Kurulu kurulmuş ve bu kurul tarafından hazırlanan "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" 20/06/2012 tarihinde Bakanlar Kurulu Kararı olarak yayımlanmıştır.

Siber Güvenlik Konusu tüm ülkeyi, ülkenin kurum ve kuruluşlarını ve toplumun tüm kesimlerini ilgilendiren ve genel anlamda bir koordinasyon içerisinde yürütülmesi gereken bir konudur. Ülkemizde Siber Güvenlik konusunu bütün yönleriyle ele alarak, bu alanda gerekli olan tüm düzenleme ve denetlemeleri yapacak, ülke adına politika ve strateji geliştirecek tek bir kurum ve/veya kuruluş bulunmadığından söz konusu faaliyetler farklı kurum ve/veya kuruluşlar tarafından yürütülmekte ve bu kurum ve/veya kuruluşlar arasında da bir uyum, eşgüdüm ve koordinasyon bulunmamaktadır.

Siber saldırıların yaygınlık ve etkisinin kamuoyunda gündeme geldiğinden ve bilinirliliğinden çok daha yüksek olduğu tahmin edilmektedir. Siber saldırıların çok düşük bir oranı mağdur tarafından fark edilip bildirilmekte, büyük çoğunluğu ise ya fark edilememekte veya ekonomik / politik kaygılar ile açıklanmamaktadır. Dolayısıyla siber tehditlerin oluşturduğu tehlikenin algımızdaki boyutu ile gerçekteki boyutu arasında ciddi uçurumlar bulunmaktadır.

Siber saldırılar istemli veya istem dışı, etkin veya edilgen olabilmektedir. Siber saldırıların amacı ise yetkisiz olarak bilgiye ulaşmak dolayısıyla değiştirmek silmek veya ifşa

etmek ve hizmetlerin engellenmesi olarak iki ana grupta toplanır. Siber güvenlik ile ilgili temel tanımlar aşağıda verilmiştir.

Siber Uzay	İnternet veya başka bir bilgisayar ve iletişim ağı üzerinden kullanılabilir olan tüm bilişim sistemlerinin tamamı.
Siber Saldırı	Hedef seçilen kişi, şirket, kurum veya devletin bilgi sistemlerinin işleyişinin engellenmesi, bozulması veya değiştirilmesi yoluyla; iş, idare veya toplumsal hayat üzerinde olumsuz etki oluşturulması.
Siber Güvenlik	Siber uzayda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünü.
Kritik Altyapı	Zarar görmesi veya yok olması durumunda toplumsal düzenin ve kamu hizmetlerinin devamlılığının sağlanmasında güçlük yaratacak; işlevlerini kısmen veya tamamen yerine getiremediğinde vatandaşların sağlığına emniyetine, güvenliğine ve ekonomik faaliyetler veya devletin etkin ve verimli işleyişine olumsuz etki edecek yapılar. Kritik altyapılar ülkeden ülkeye farklılıklar gösterebilir.
Hizmetin Engellenmesi	Sistem kaynaklarına erişimin engellenmesi ya da zamana bağımlı kritik operasyonların geciktirilmesi.
Açıklık Analizi	Sistemlerin güvenlik açısından yeterliliğini belirlemek amacıyla sistematik inceleme ile mevcut güvenlik önlemleri ve onun eksikliklerini belirlemek, bununla ilgili veri sağlayarak sistemlerin güvenliğini artırmaya yönelik analiz yöntemi.

2. Mevcut Durum

Siber güvenlik alanında ülkemizde atılan en büyük adımlardan biri kuşkusuz 20.12.2012 tarihinde Ulusal Siber Güvenlik Strateji Belgesi'nin yayımlanmasıdır. Bunun

ardından Ulusal Siber Güvenlik Koordinasyon Kurulu'nun oluşturularak Siber Güvenlik Eylem Planı (2013-2014) hazırlanması, UDHB'nın Koordinasyon Makamı olarak belirlenmesi ve Siber Olaylara Müdahale Ekiplerinin (SOME) oluşturulması Türkiye'de devletin ve kurumların siber güvenlik algısını ve yaklaşımını tamamen değiştirmiştir.

2015 yılında UDHB, 2015-2017 Siber Güvenlik Eylem Planını çok daha geniş katılımlı çalıştaylar ile daha etkin ve verimli bir sürece taşımıştır.

Bu Eylem Planı'nın en çarpıcı yanlarından biri ise, Eylem Planı kalemlerinden bazılarının TBD ve BGD gibi STK'ların sorumluluğuna verilmesi yaklaşımıdır.

2.1 UDHB-Siber Güvenlik Eylem Planı 2013-2014 (29 Madde)

Siber Güvenlik Kurulunun 20.12.2012 tarihinde gerçekleştirdiği toplantıda onaylanan "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" 20.062013 tarih ve 2013/4890 sayılı bakanlar kurulu kararı olarak Resmi Gazetede yayımlanarak yürürlülüğe girmiştir. Eylem planı toplam 29 adet ana eylem ve 95 adet alt eylem maddesinden oluşmaktadır. Söz konusu eylem planının 14 maddesi ulusal siber güvenlik altyapısının güçlendirilmesi, 4 maddesi ise siber güvenlikte yerli teknolojilerin geliştirilmesi ve teşvik edilmesi ve bu ürünlerin kamu kurumları ile kritik altyapılarda kullanımının yaygınlaştırılması ile ilgilidir. Söz konusu 29 ana eylem maddesinin detaylı kırılımı aşağıda yer almaktadır;

- Siber güvenlik konusunda yasal düzenlemelerin yapılması için 2,
- Uluslararası hukuktan kaynaklanan hakların kullanılması için 1,
- Ulusal Siber olaylara müdahale organizasyonu oluşturulması için 1,
- Ulusal siber güvenlik altyapısının güçlendirilmesi için 14,
- Siber güvenlik alanında insan kaynağının yetiştirilmesi için 6,
- Siber güvenlikte yerli teknolojilerin geliştirilmesi için 4,
- Ulusal Güvenlik Mekanizmalarının Kapsamının Genişletilmesi için 1.

Söz konusu eylem planı kapsamında temel görevi koordinasyon ve işbirliği olan Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurularak, 27.05.2013 tarihinde faaliyetlerine başlamıştır.

Yine söz konusu eylem planı çerçevesinde kamu kurum ve kuruluşları bünyesinde Siber Olaylara Müdahale Ekiplerinin (Kurumsal SOME) oluşturulması öngörülmüştür. UDHB tarafından hazırlanan Siber Olaylara Müdahale Ekiplerinin, kuruluş, görev ve çalışmalarına dair usul ve esaslar hakkında tebliğ, 11.11.2013 tarih ve 28818 sayılı Resmi gazetede yayımlanmıştır.

2.2 UDHB-Siber Güvenlik Eylem Planı 2015-2017

Gelişen teknolojiler, değişen güvenlik gereksinimleri ve 2013-2014 eylem planından edinilen geri beslemeler doğrultusunda UDHB tarafından 2015-2017 dönemini kapsayan eylem planı taslak olarak hazırlanmıştır. Henüz Resmi Gazete'de yayımlanmayan söz konusu eylem planı, ilgili kamu kurum ve kuruluşları ile yapılan toplantılar ve kamu kurumları, kritik altyapı işletmecileri, bilişim sektörü, üniversiteler ve sivil toplum kurumlarını temsilen 73 kurum ve kuruluştan toplam 126 uzmanın katılımı ile gerçekleştirilen Ortak Akıl Platformu sonucunda nihai hale getirilmiştir.

2015-2017 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında olası siber güvenlik riskleri göz önünde bulundurulmuş ve stratejik amaçlara ulaşmak için gerçekleştirilecek eylemler beş stratejik eylem başlığı altında toplanmıştır. Söz konusu stratejik eylem başlıkları eylemlere ayrılmış, planlanan bitirilme tarihleri, sorumlu ve ilgili kuruluşlar belirlenmiştir. 2015-2017 döneminde gerçekleştirilmesi planlanan toplam 39 adet stratejik eylem maddesi aşağıdaki başlıklar altında gruplanmıştır;

- Siber Savunmanın Güçlendirilmesi
- Siber Suçlarla Mücadele
- Farkındalık ve İnsan Kaynağı Geliştirme
- Siber Güvenlik Ekosisteminin Geliştirilmesi
- Siber Güvenliğin Milli Güvenliğe Entegrasyonu

Söz konusu taslak eylem planında ilk defa STK'lara da görevler atanmış olup; Siber güvenlik alanında faaliyet gösteren firma envanterinin çıkartılmasından BGD, Siber güvenlik sözlüğünün hazırlanmasından ise TBD sorumlu kuruluş olarak belirlenmiştir.

2.3 Bilim, Sanayi ve Teknoloji Bakanlığı - Siber Güvenlik Çalışmaları

2.3.1 Bilim Teknoloji Yüksek Kurulu(BTYK) Çalışmaları

BTYK tarafından 2013/103 sayılı kararda ‘’ e-Devlet Uygulamaları Hizmet Alımları için Firma Belgelendirme Sistemi Oluşturulması’’ başlığı altında;

a) e-Devlet ihalelerine kabul edilecek firmalara yönelik Bilim, Sanayi ve Teknoloji Bakanlığı tarafından belgelendirme sistemi oluşturulmasına,

b) e-Devlet uygulamaları kapsamındaki hizmet alımlarının firma belgelendirme sistemi doğrultusunda yapılabilmesi için -mevzuat değişikliğine ihtiyaç olması halinde- önerilerin hazırlanmasına ve BTYK’nın 26. toplantısına sunulmasına karar verilmiştir.

Şeklinde kararlar alınmıştır.

Bu kapsamda Bilim, Sanayi ve Teknoloji Bakanlığı önderliğinde TSE, TÜBİTAK ve ilgili diğer kurumların katkılarıyla Eylül 2014’den bu yana birçok toplantı yapılmış, çalıştaylar düzenlenmiş, ilgili sektör temsilcileri ve kamu kurumları ile toplantılar yapılmıştır. Aktif çalışmalar halen devam etmektedir. Amaç Bilişim firmalarının güvenli ve kaliteli bilişim ürünü/sistemi ve yazılımı üretmelerini sağlarken, Belgelendirme desteği için fon sağlamak ve özellikle de Kamu kurumlarının güvenli ve kaliteli yazılım/bilişim ürünü ve/veya sistemlerini kullanmalarını sağlamaktır.

2.3.2 Ulusal Yazılım Sektörü Stratejisi ve Eylem Planı Çalışmaları

Türkiye Yazılım Sektörü Stratejisi ve Eylem Planı (2016-2019) Taslak Belgesi; Bilim, Sanayi ve Teknoloji Bakanlığı eşgüdümünde ilgili paydaşlarla birlikte hazırlanmıştır. Taslak Belgenin hazırlıkları kapsamında çalıştaylar gerçekleştirilmiştir. Çalıştaya konu ile ilgili kamu kurum ve kuruluşları, özel sektör, üniversiteler, enstitüler, odalar, dernekler ve vakıflardan yönetici ve uzmanlardan katılım sağlanmıştır. Çalıştayda sektörün mevcut durumunun analizi yapılarak, ortaya konulan fırsatlar ve tehditler doğrultusunda sektöre ilişkin hedefler ve eylem planı önerileri alınmıştır. Bu çalıştaya ilişkin ortaya çıkan sonuçlar, ilgili kurum ve kuruluşların görüşleri doğrultusunda düzenlenerek taslak Belge oluşturulmuştur. İlgili taslak belgede yazılım güvenliği ve Siber Güvenlik ile de ilgili eylem maddeleri yer almaktadır.

2.4 Telekomünikasyon İletişim Başkanlığı(TİB) –Bilgi Teknolojileri ve İletişim Kurumu(BTK) Siber Güvenlik Faaliyetleri

2.4.1 BTK Siber Güvenlik Faaliyetleri

2.4.1.1 Siber Güvenlik Tatbikatları

BTK tarafından yürütülen siber güvenlik ile ilgili çalışmaların arasında siber güvenlik tatbikatları yer almaktadır.

Siber güvenlik tatbikatlarının amacı;

- Katılımcıların siber saldırılara karşı koyma yeteneklerini geliştirmek,
- Katılımcıların siber saldırılara karşı kurum içi ve kurumlar arası koordinasyonlarını geliştirmek
- Siber güvenlik konusunda ulusal farkındalık seviyesini arttırmaktır.

Nisan 2015 itibari ile 3 ulusal ve 1 uluslararası siber tatbikat düzenlemiştir. Bu tatbikatlarda UDHB ile koordinasyon konularında, TÜBİTAK, TİB ve ITU-IMPACT ile teknik konularda işbirliği gerçekleştirilmiştir.

2.4.1.2 Sektörel SOME Çalışmaları

BTK bünyesinde elektronik haberleşme sektöründeki koordinasyonu sağlamak üzere 10.09.2014 tarihinde Sektörel SOME kurulmuştur. Diğer taraftan Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği ile işletmecilerin;

- Siber saldırılara yönelik tedbirler alması,
- Kurumsal SOME kurması ve Sektörel SOME koordinesinde çalışması,
- DoS/DDoS saldırıları, zararlı yazılım yayılması ve benzeri siber saldırılara karşı, USOM'un koordinesinde gerekli tüm tedbirleri alması,
- Sunucular, yönlendiriciler ve diğer şebeke elemanlarının DoS/DDoS saldırıları, zararlı yazılım yayılması gibi siber saldırılara karşı korunması amacıyla, elektronik haberleşme hizmetinin tipi de dikkate alınarak, IP adreslerinde, haberleşme portlarında ve uygulama protokollerinde; sinyal işleme kontrolü, kullanıcı doğrulama ve erişim kontrolleri gibi mekanizmalar kurması ve talep edilmesi halinde siber saldırılara karşı koruma hizmeti sunması

zorunlu hale getirilmiştir.

2.4.1.3 Farkındalık Çalışmaları

Siber güvenlik konusunda bireysel, kurumsal ve ulusal farkındalığın arttırılması amacıyla BTK tarafından çeşitli çalışmalar yürütmektedir.

BTK, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının 23. maddesi kapsamında ve kurumların talepleri doğrultusunda siber güvenlik konusunda farkındalığın arttırılması amacıyla sunumlar yapılmaktadır.

Söz konusu sunumlarda;

- Bilgi güvenliği ve siber güvenliğe yönelik tehditler, genel güvenlik önlemleri, farkındalığı artırma, kurumsal bilgi güvenliği politikaları, sosyal medya ve mobil cihazların siber güvenliği konularında bilgilendirmeler yapılmakta,
- BTK'nın düzenleme ve denetleme yetkisinde olan elektronik haberleşme sektörüne yönelik siber güvenlik mevzuat çalışmaları ve tedbirleri hakkında bilgilendirme yapılmakta,
- Siber güvenlik mevzuatı ve organizasyonu hakkında bilgilendirmeler yapılmaktadır.

2.4.2 TİB Siber Güvenlik Faaliyetleri

2.4.2.1 USOM

Ülkemizin siber güvenliğine karşı siber ortamda ortaya çıkan tehditlerin belirlenmesi, muhtemel saldırı ve olayların etkilerini azaltılması veya ortadan kaldırılmasına yönelik önlemlerin geliştirilmesi ve belirlenen aktörlerle paylaşılması için ulusal ve uluslararası düzeyde çalışmak üzere TİB bünyesinde Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) oluşturulmuştur.

Başkanlık bünyesinde kurulan USOM, ulusal ve uluslararası seviyede siber ortamda ortaya çıkan tehditler ile ilgili kendisine ulaştırılan ihbarları da değerlendirerek, söz konusu tehditlerin tespit ve bertaraf edilmesi için Kamu Kurumları ve özel kişiler ile koordinasyonunu sağlamaktadır. Bu itibarla gelen ihbar ilk aşamadan başlanarak, çözüm sürecine kadar takip edilerek değerlendirilmektedir.

Diğer taraftan ulusal ve uluslararası siber güvenlik tatbikatları düzenlenerek kamu kurum ve kuruluşlarının siber saldırılara karşı farkındalığının ve hazırlığının arttırılması faaliyetleri ile bilinçlendirme ve yönlendirme faaliyetleri hâlihazırda devam etmektedir.

2.5 TÜBİTAK

2010 yılında TÜBİTAK'ın bünyesinde kurulan Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM); bilgi güvenliği, kriptoloji ve haberleşme teknolojileri alanında hizmet vermektedir. Siber güvenlik faaliyetleri ise BİLGEM'in altında yer alan Siber Güvenlik Enstitüsü (SGE) tarafından yürütülmektedir. Bu faaliyetlere örnek olarak; sızma testleri ve güvenlik denetlemeleri, bilgi güvenliği yönetimi, Bilgisayar

Olaylarına Müdahale Ekibi (BOME), bilgi güvenliği eğitimleri ve BTK ile birlikte düzenlenen ulusal güvenlik tatbikatlar gösterilebilir. Ayrıca TÜBİTAK BİLGEM Ortak Kriterler Test Merkezi (OKTEM) aracılığıyla, bilişim teknolojileri ürünlerinin güvenlik değerlendirmeleri uluslararası Ortak Kriterler-ISO/IEC 15408 ve ISO/IEC 18045 standartlarına uygun olarak gerçekleştirilmektedir. Sertifikasyon Makamları tarafından verilen Ortak Kriterler sertifikaları CCRA (Ortak Kriterler Tanıma Anlaşması) gereği 26 ülkede tanınır olmaktadır. Böylece, bahsekonu değerlendirme sonrasında TSE tarafından sertifikalandırılan yerli Bilişim ürünlerimizin ihracat şansı da yüksek oranda artmaktadır.

Yukarıda belirtilen hizmetlere ek olarak BİLGEM tarafından; Siber Tehditleri Algılama Merkezi Sistemi (STAMPS), Siber Ortam Tuzak Sistemi (SORT), Veri Kaçağı Önleme Sistemi (VKÖS) ve benzeri bazı siber güvenlik çözümleri sunulmaktadır.

2.6 TSE Siber Güvenlik Standartları ve Belgelendirmeleri

Bilişim Teknolojileri ve Siber Güvenlik ile ilgili çalışmaları 2003 yılında başlatan TSE; Bilişim Teknolojileri Test ve Belgelendirme Daire Başkanlığı bünyesinde, bu sektöre yönelik belgelendirme ve test hizmetleri vermekte, siber güvenlik alanında yapılan çalışmalara aktif katılmakta ve öncülük etmektedir.

2013-2014 Siber Güvenlik Eylem Planı 12. maddesini gerçekleştirebilmek için TSE Bilişim Teknolojileri Test ve Belgelendirme Daire Başkanlığı uhdesinde, 11 ve 18.04.2013 tarihli Yönetim Kurulu kararlarıyla bağımsız "Siber Güvenlik Özel Komitesi" kurulmuştur. TSE'nin koordinasyonunda kurulmuş olan bu komite üniversiteler, kamu ve özel sektörden konularıyla ilgili 55 kadar teknik uzmandan oluşmuş olup, ülkemiz ihtiyaçları doğrultusunda BT alanında asgari güvenlik kriterlerinin belirlenmesine yönelik 25 adet Siber Güvenlik Ar-Ge projesi yapmış ve ülkemiz Bilgi güvenliği ihtiyaçları doğrultusunda aşağıdaki 24 adet Güvenlik Kriteri/Standart/Koruma Profilini çıkartmıştır:

1. Güvenli Elektronik Belge Yönetim Sistemi(EBYS) Koruma Profili ve Belgelendirmesi
2. Kart Erişim Cihazları(KEC) ve Elektronik Kimlik Doğrulama Sistemi(EKDS) Belgelendirmesi
3. Güvenli Coğrafi Bilgi Sistemleri(CBS) Koruma Profili ve Belgelendirmesi
4. Akıllı Sayaçlar Koruma Profili ve Güvenlik Belgelendirmesi
5. IP Tabanlı Yazar Kasa Koruma Profili ve Güvenlik Belgelendirmesi
6. Yazılım Testçiler Kriterleri ve Belgelendirmesi
7. Güvenli Bulut Bilişim Kriterleri ve Belgelendirmesi
8. TS 13638: Sızma Testi yapan kişi "Beyaz Şapkalı Hacker" ve firma kriterleri ve Belgelendirmesi SSL kriterleri ve Belgelendirmesi

9. SSL kriterleri ve Belgelendirmesi
10. Biyometrik Ürünler için Koruma Profili ve Güvenlik Belgelendirmesi
11. Güvenli Web Servisleri Koruma Profili ve Güvenlik Belgelendirmesi
12. Güvenli Web Uygulamaları Koruma Profili ve Güvenlik Belgelendirmesi
13. Veri Merkezleri-Sistem Odaları Güvenlik Kriterleri ve Belgelendirmesi
14. Bankacılık Sektörü Güvenlik Kriterleri ve Belgelendirmesi
15. Mobil Uygulamalar Koruma Profili ve Güvenlik Belgelendirmesi
16. BT Ürünleri Zayıflık Veritabanı Kütüphanesi
17. Sızma Testi Teknik Kriterleri ve Belgelendirmesi
18. Güvenli E-Ticaret Koruma Profili ve Belgelendirmesi
19. Güvenli Çip Koruma Profili
20. Gömülü İşletim Sistemleri Koruma Profili
21. E-Pasaport Koruma Profili
22. Sağlık Bilgi Sistemleri Güvenlik kriterleri ve Belgelendirmesi.
23. Adli Bilişim Güvenlik Kriterleri ve Uzmanı Belgelendirmesi
24. Pardus Göç Uzmanı Kriterleri ve Belgelendirmesi

Bilişim Teknolojileri Test ve Belgelendirme Daire Başkanlığı Siber Güvenlik Belgelendirme Müdürlüğü ve Bilişim Teknolojileri Belgelendirme Müdürlükleri bünyelerinde bilgi güvenliği hususunda önem taşıyan:

- TS ISO/IEC 15408: BT ürün güvenliği-Common Criteria (Ortak Kriterler)
- TS ISO/IEC 27001: Bilgi Güvenliği Yönetim Sistemi
- TS ISO/IEC 27031: Bilgi Teknolojileri için İş Sürekliliği
- TS ISO/IEC 19790, 24759: Kriptografik Modül/ Algoritma Sertifikasyonu
- Temel Seviye Güvenlik Belgelendirmesi
- Saha Güvenlik Belgelendirmesi
- TS 13638: Bilgi Teknolojileri-Güvenlik Teknikleri-Sızma Testi Yapan Personel ve Firma Belgelendirmesi

gibi birçok önemli hizmet gerçekleştirilmektedir.

Ayrıca TSE Bilişim Teknolojileri Test ve Belgelendirme Daire Başkanlığı tarafından siber güvenlikle ilgili alınacak önlemleri belirlemek ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla Siber Güvenlik çalıştayları ve siber güvenlik alanındaki bilgi ve tecrübelerini paylaşmak amacıyla farkındalık konferansları, seminerleri, eğitimleri ve çalıştayları düzenlenmektedir. Özellikle geleneksel hale gelen Bilişim Teknolojileri Standartları Konferansı sektörden çok ilgi görmektedir.

Önümüzdeki süreçte siber güvenlik konusunda TSE`nin yeni projelerinin arasında; Bilişim Teknolojileri Test Müdürlüğü bünyesinde BT Ürün Güvenliği TS ISO/IEC 15408-Ortak Kriterler Standardı kapsamında uluslararası "Ortak Kriterler Test Laboratuvarı"nın kurulması vardır. TSE Bilişim Teknolojileri Test ve Belgelendirme Dairesi Başkanlığının kuracağı bu laboratuar siber güvenlik ve yazılım ürünlerinin güvenlik fonksiyonlarını test ederek, ülkemizin milli bilgi güvenlik sektörüne ve ekonomisine büyük katkılar sağlaması beklenmektedir.

3. Siber Güvenlik Stratejisi ve Eylem Planı

2012 yılına kadar, devlet siber güvenlik konusuna yakın bir ilgi göstermemiştir. Özellikle siber tehdit ve saldırılar açısından ilk sıralarda yer alan ülkemiz, bu konudaki ilk ciddi adımını 20.12.2012 tarihinde Ulusal Siber Güvenlik Strateji Belgesi'nin yayınlayarak atmıştır.

Bu strateji belgesinin gereği Ulusal Siber Güvenlik Koordinasyon Kurulu kurulmuş ve UDHB Koordinasyon Makamı olarak belirlenmiştir.

Ardından da Siber Güvenlik Eylem Planı (2013-2014) hazırlanarak yürürlüğe konulması Türkiye'de devletin siber güvenlik algısının kurumsallaşması açısından çok önemli bir adım olmuştur.

2015 yılında ise, bir önceki Eylem Planının olumlu/olumsuz çıktılarını da göz önüne alınarak, 2015-2017 Eylem Planı geniş katılımlı çalışmalar hazırlanmıştır.

3.1 Siber Güvenlik Farkındalık Yaratma

Kamu kurum ve kuruluşlarında yönetici personel ve bilgi işlem personelleri başta olmak üzere tüm personelde siber güvenlik farkındalığı oluşturulmasına yönelik bir programın oluşturulması ve bu programın pilot seçilen kamu kurum ve kuruluşlarında acilen uygulanmasına başlanması bu sorunun çözümü için önemli bir kilometre taşı olacaktır.

Ayrıca; Kısa, orta ve uzun vadeli uzman yetiştirme programları kapsamında Kurumsal ve Sektörel SOME'ler başta olmak üzere Siber güvenlik sektöründeki nitelikli insan kaynağının arttırılmasına yönelik programların düzenlenmesinin gerekli olduğu değerlendirilmektedir. Bu programlar kapsamında eğitilen nitelikli insan kaynağının sertifikalandırılması ve kayıt altına alınması önem arzetmektedir. Bu kapsamda gerekli olan düzenlemelerin UDHB tarafından; BTK, TSE ve STK (BGD ve TBD) işbirliği ile yapılması uygun olacaktır.

Toplumun her kesiminde siber güvenlik bilincinin oluşturulması amacıyla eğitim kurumlarının çalışmalarına ilave olarak yazılı ve görsel medyada farkındalık çalışmalarının yapılmasının önemli olacağı değerlendirilmektedir.

Bu kapsamda yapılabilecek belli başlı faaliyetler aşağıda özetlenmiştir;

- İlk ve orta öğretimde bilişim teknolojilerinin (sosyal medya, internet vb.) güvenli kullanımı konusunda farkındalık eğitimlerinin verilmesi,

- Öğretmen ve ebeveynlere siber güvenlik farkındalığı konusunda eğitim programlarının düzenlenmesi,
- Üniversitelerde ilgili bölümlerin müfredatlarına siber güvenlik ile ilgili olarak dersler konulması, proje çalışmaları yapılması, yaz okulları açılması
- Siber güvenlik ve savunma konusunda konferanslar, çalıştaylar, seminerler ve sertifika programları yapılması
- Üniversitelerde mevcut potansiyeli arttırmak için konuya yakın Öğretim elemanlarının kendilerini geliştirecek ortamlar oluşturulması ve
- Üniversitelerin alan uzmanlığı konusunda ihtisaslaşacağı yapılar oluşturulmasıdır.

3.2 Yerli ve Sertifikalı Siber Güvenlik Ürünü Kullanılması

Türkiye siber suçlar ve saldırılar açısından hedef ilk 10 ülke arasındadır. Türkiye aynı zamanda siber saldırı yapan ülkeler arsında ilk sıralarda gözükmektedir.

Başta Kamu kurumları olmak üzere kurumsal ve bireysel düzeyde siber güvenlik açısından yeterli farkındalık, bilinç ve bilgi seviyesine henüz ulaşılamamıştır. 2013-14 döneminde 9 banka, 13 sigorta şirketi, 2 telekomünikasyon şirketi, 27 üniversite, 30 kamu kurumu saldırıya uğramıştır.

Yerli siber güvenlik çözümlerinin geliştirilmesi ve kullanımının teşvik edilmesinin bu alanda gelişimimize katkı sağlayacağı değerlendirilmektedir. Kullanılan çözümlerin %97'si yabancı (ithal) olup bunların %55'i İsrail, %35'i ise ABD kökenlidir.

Türkiye'de çoğu küçük ölçekli 40 civarında firma bu alanda faaliyet göstermekte olup bunlar arasında bir sinerji ve güç birliği mevcut değildir. Aynı zamanda bu firmalar bir ulusal strateji doğrultusunda değil dağınık bir yaklaşım ile iş yapmaya çalışmaktadır.

Gerek yerli geliştirilen ve gerekse ithal edilen siber güvenlik çözümleri milli bir sertifikasyona sürecinden geçmeden ve yeterince güvenli olup olmadıkları bilinmeden kullanıma sokulmaktadır.

Yerli ürün ve teknoloji eksikliğinin ulusal sevide siber güvenlik zafiyeti yarattığı açıktır. Başta kritik altyapılar olmak üzere güvenlik sertifikasına sahip yerli siber güvenlik teknoloji, çözüm ve ürünlerinin yaygın olarak kullanılmasını destekleyen teşvik ve zorunlulukların getirilmesinin gerekli olduğunu değerlendiriyoruz.

Öncelikli güvenlik gereksinimleri belirlenerek bu konularda üretimin yönlendirilmesi, gerekli alt yapının hazırlanması (*Teşvikler, öncelikli alan listesi, üniversite-sanayi işbirliği, test ve ölçüm laboratuarları, vb.*) yeterli sayıda ve nitelikte ürünün geliştirilmesini olanak sağlayacaktır.

Yerli sertifikaya sahip çözümlerin kullanımını zorunlu hale getirilmelisi amacıyla KİK mevzuatı başta olmak üzere gerekli düzenlemeler yapılmalıdır.

3.3 Siber Güvenlik Ekosisteminin Kurulması

Ulusal seviyede siber güvenliğin etkin ve sürdürülebilir olarak sağlanması amacıyla kapasite planlaması ve yetenek kazanımı yapılması ile mevcut yeteneklerin bir hedef doğrultusunda arttırılabilmesi ancak ulusal siber güvenlik ekosisteminin oluşturulması ile sağlanabilir. Bu ekosistemde yer alacak olan Kamu, Özel Sektör, STK ve diğer paydaşların koordineli katkılarıyla mevzuattan teknolojiye kadar gereksinimlerin gerçekçi olarak belirlenmesine ve uygulamaya yönelik eylemlerin gerçekleştirilmesine katkı sağlanacaktır.

Ekosistemin en önemli unsuru nitelikli insan kaynağıdır. Bu nedenle tüm uzmanlık alanlarında siber güvenlik elemanları yetiştirilmesi önemli kazanımlar sağlayacaktır. Türkiye'deki saygın üniversiteler siber güvenlik alanında uzman hale getirilmeli ve çalışmalar nitelikli öğretim elemanları ve yeterli altyapı oluşturularak yürütülmelidir. Üniversiteler tarafından yürütülen lisansüstü eğitim programlarında tez konuları Kamu ihtiyaçları ile BT ve siber güvenlik sektörü faaliyet alanları göz önünde bulundurularak belirlenmelidir.

Ekosistemin güçlendirilmesi ve yaygın etkisinin arttırılmasına yönelik gerekli kaynak planlamalarının yapılması ve destek mekanizmalarının oluşturulması önemli katkılar sağlayacaktır.

Ulusal Siber güvenlik ekosistemi içinde iyi örneklerin yaygınlaştırılması, danışmanlık hizmetlerinin verilmesi, açıklık, tehdit ve faydalı uygulamaların paylaşılması önemli kazanımlar sağlayacaktır.

3.4 Gerçekleştirilen Eylem Planlarının Yaygın Etkisinin Ölçümü

Gerçekleştirilen eylem planlarının etkisinin ölçülmesi ve raporlanmasının objektif olarak gerçekleştirilmesi çok önemlidir. Kamunun çalışma anlayışı ve yapısı nedeniyle bu henüz başarılabilir görülmemektedir. En azından bazı güçlü kurumlar bilgi paylaşmada istekli davranmamaktadırlar.

Diğer yandan, mevcut yapıda gerçekleştirilen eylemler sadece nicelik bakımından değerlendirilmektedir. Bunun sonucunda gerçekleştirilen eylem ile hedeflenen isterlerin karşılanıp karşılanmadığı ve sürdürülebilir yaygın etkisi ölçülememektedir. Bu amaçla STK ve üniversitelerdeki yetkin ve uzman personellerden oluşan bir değerlendirme kurulunun oluşturularak periyodik olarak rapor hazırlanması önemli bir kazanım sağlayacaktır. Somut ve gerçekçi veri alınabilecek bir mekanizma kurulmalıdır.

3.5 Ulusal Siber Güvenlik Makamının Güçlendirilmesi

Bakanlar Kurulu'nun 11.06.2012 tarihli ve 2012/3842 sayılı kararı oluşturulan Siber Güvenlik Kurulu, esasen siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan strateji ve planları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamakla, UDHB ise onaylanan strateji ve planların uygulanması ile görevli kılınmıştır.

Siber Güvenlik Kurulu tarafından yürütülen faaliyetlerin etkinleştirilmesi ve sürdürülebilir kılınmasına ihtiyaç duyulmaktadır. Bu nedenle; Ulusal Siber Güvenlik Makamının, Kamu, özel sektör, üniversiteler ve sivil toplum kuruluşları ile koordinasyon ve eşgüdümü sağlayacak şekilde yeniden tanımlanmasının ve güçlü bir merkezi yapıya dönüştürülmesinin gerekli olduğu değerlendirilmektedir.

Siber Güvenlik Kurulu'nun belirtilen görevleri daha etkin ve sürdürülebilir olarak yerine getirebilmesi amacıyla, bu kurulu destekleyen Siber güvenlik alanında uzman kişilerden (STK, Üniversite ve Sektör temsilcileri) oluşan "Siber Güvenlik Teknik Çalışma Grubu" kurulmasının faydalı olacağı öngörülmektedir. Bu çalışma grubu tarafından aşağıda belirtilen faaliyetlerin yürütülmesi gerçekleştirilecektir;

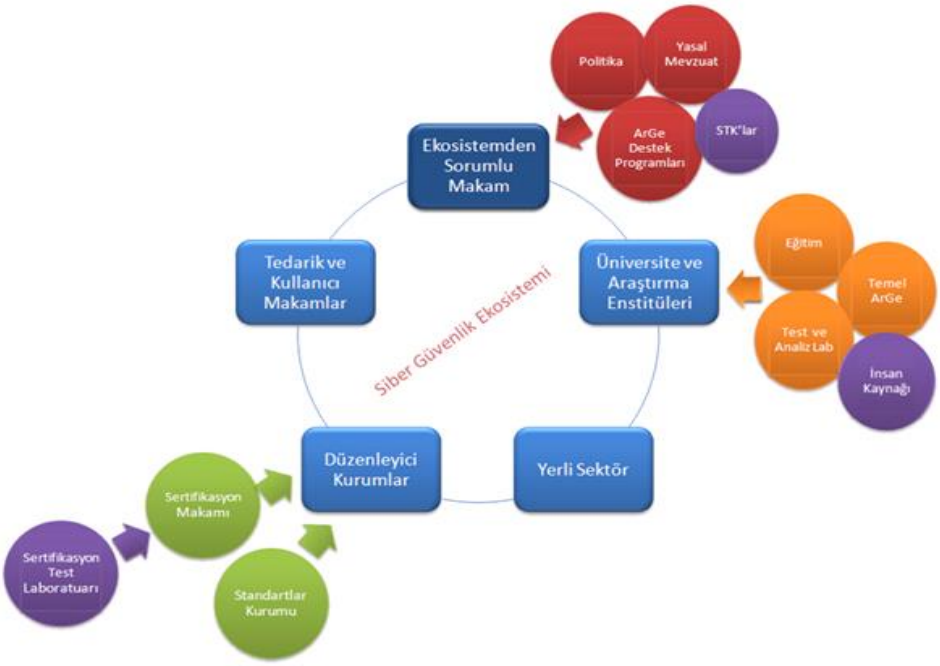
- Hangi "Siber Güvenlik Teknolojileri"nin yerli olarak geliştirilmesi gerektiğinin belirlenmesi ve önceliklendirilmesi,
- Kritik altyapılarda ne tür önlem alınmasına gerek olduğunun analiz edilmesi ve belirlenmesi,
- Lisan ve lisan üstü eğitimlerle araştırılması ve geliştirilmesi hedeflenen siber güvenlik alanlarının belirlenmesi ve önceliklendirilmesi,
- Siber güvenlik strateji ve planlarının hazırlanmasına teknik destek verilmesi,
- Eylem planlarının hazırlanmasına teknik destek verilmesi ve
- Gerçekleştirilen eylem planlarının etkisinin ölçülmesi ve raporlanması.

Kurumsal ve Sektörel SOME'lerin etkinliğinin arttırılması amacıyla, mali düzenlemelerin yapılması, yetkin personel ihtiyacının karşılanmasına ve ulusal siber olaylara müdahale organizasyonu kapsamında bilgi paylaşımının geliştirilmesine yönelik mevzuat desteğinin sağlanması gereklidir.

4. Ekosistemde Sektörün Beklentileri ve Uluslararası İşbirliği

Bilişim Teknolojileri çok hızlı gelişmektedir. Bugün için alınacak siber güvenlik önlemleri yarınlarımızın güvenli olacağını garanti altına alamamaktadır. Sürdürülebilir siber güvenlik ancak yeni nesil teknolojiler ile mümkün olabilmektedir. Yeni nesil ve yenilikçi teknolojilerin satınalma yolu ile yurtdışından tedarik edilmesi mümkün değildir. Ayrıca yurtdışından tedarik edilecek siber güvenlik teknolojilerinin arka kapı ve/veya truva atı gibi zararlı yazılımlar içermediğinin bilinmesi veya belirlenebilmesi de mümkün değildir. Bu neden ile yeni nesil, yenilikçi ve akıllı teknolojilerin yakından takip edilmesi, yerli ve özgün olarak geliştirilmesi ve üretilmesi çok önemlidir.

Ülke çapında güvenilir, yüksek güvenlik seviyesine sahip, maliyet etkin ve sürdürülebilir bir siber güvenlik kalkanının gerçekleştirilebilmesi ancak yerli siber güvenlik ekosisteminin oluşturulması ile sağlanabilir. Bu ekosistem içerisinde; müşteriler, tedarikçiler ile teknoloji, ürün ve hizmetlerin geliştirilmesine katkı sağlayan kilit paydaşlar, standardizasyon ve sertifikasyon kuruluşları, akreditasyon ve eğitim tesisleri, üniversiteler ve STK'lar başta olmak üzere tüm paydaşlar yer almalıdır. Sözkonusu ekosistem içerisinde ekosistemin politika ve stratejilerini belirleyen bir makam olmalıdır. Bu kapsamda Ar-Ge Destek programları ve Yasal mevzuatlar STK'lar ile işbirliği yapılarak oluşturulmalıdır. Bu makam tarafından geri besleme ve edinilen tecrübelerle ekosistemin politika ve stratejileri periyodik olarak güncellenmelidir. Siber Güvenlik Ekosisteminin mimari yapısı genel olarak Şekil-1'de verilmiştir.



Şekil-1. Siber Güvenlik Ekosistem Mimari yapısı

Ekosistemde Üniversite ve Araştırma Enstitülerinin fonksiyonları temel araştırmaların gerçekleştirilmesi, Test ve analiz laboratuarlarının kurulması, lisans ve lisansüstü eğitimin verilmesi ile nitelikli insan kaynağının yetiştirilmesi programlarına destek olarak özetlenebilir. Yerli sektörün sorumlulukları ise ürüne yönelik araştırma ve geliştirme faaliyetlerini yürütmek, siber güvenliğe yönelik özgün ürün ve sistemlerin yerli olarak geliştirilmesi ve üretilmesi ile ihtiyaç duyulan siber güvenlik hizmetlerin sağlanması olarak tanımlanabilir. Ekosistemde yer alan yerli sektör firma envanteri faaliyet alanı ve yetkinlik baz alınarak oluşturulmalıdır. Standardizasyon kurumu yerli olarak geliştirilecek siber güvenlik ürün, sistem ve hizmetlerinin uyulması gereken ulusal ve uluslararası standartları sektör girdilerine uyumlu olarak oluşturarak ve/veya belirleyerek yüksek performansa sahip siber güvenlik ürün, sistem ve hizmetlerinin yerli olarak geliştirilmesine ve ihracatına katkı sağlamalıdır. Sertifikasyon Makamı ise siber güvenlik ürün, sistem ve hizmetlerin sağlaması gerektiği asgari güvenlik seviyelerini belirleyerek sektöre bildirim/geribildirimlerde bulunmalıdır. Ayrıca kamu ve kuruluşları ile kritik altyapılarda kullanılan ve/veya kullanılacak olan tüm siber güvenlik ürün, sistem ve hizmetlerine ait güvenlik testlerinin sertifikasyon test laboratuarlarında gerçekleştirmesinin koordinasyonundan ve sertifikasyon sürecinin onaylanmasından sorumlu olacaktır.

4.1 Dünyadan Örnekler

Siber Güvenlik Ekosisteminin ulusal seviyede maliyet etkin olarak sağlanması amacıyla Avrupa ve İsrail'deki ekosistemler incelenmiş ve konu ile ilgili açıklamalar aşağıda belirtilmiştir.

4.1.1 İsrail

Milli araştırma ve geliştirme imkânlarıyla geliştirilmiş bir koruma kalkanının ulusal seviyede tesis edilebilmesi amacıyla Siber Güvenlik ekosistemi oluşturulmuştur. Siber Güvenlik ekosisteminde yer alan yerli üreticilerin teşvik edilmesi ve Üniversite ile İsrail Ordusu arasında Ar-Ge konularında işbirliğinin arttırılması konuları devlet politikası olarak hedeflenmektedir.

4.1.2 Birleşik Krallık

Birleşik Krallık Siber Güvenlik ekosisteminde yer alan yerli sektörün güçlendirilmesine ve uluslararası rekabet gününün arttırılmasına yönelik olarak yürütülen devlet politikası aşağıda belirtilmiştir;

- Siber İstihbarat toplama ve siber saldırılara karşı koyma konularında ilgili devlet ve sektör kuruluşları arasında işbirliği yapılması,
- Birleşik Krallık siber güvenlik endüstrisinin geliştirilmesi amacıyla destek mekanizmalarının oluşturulması ve yurtdışında sözkonusu endüstrinin desteklenmesi,
- Birleşik Krallık siber güvenlik endüstrisinin mevcut yetkinliklerinin uluslararası alanda desteklenebilmesi için pazarlama stratejisinin geliştirilmesi.

4.2 Sektörün Kamudan Beklentileri

Ankara ve İstanbul'da yapılan çeşitli incelemeler sonucunda büyük çoğunluğu küçük ölçekli işletme (KOBİ) olmak üzere yaklaşık 40-60 firmanın siber güvenlik alanında faaliyet gösterdiği belirlenmiştir. Firmaların büyük çoğunluğu Ankara'da ODTÜ, Bilkent, Hacettepe ve Gazi Üniversitesi Teknokent yerleşkelerinde faaliyet göstermektedir. 7.07.2015 tarihinde ODTÜ Teknokent'te Bilgi Güvenliği Derneği (BGD) tarafından siber güvenlik alanında faaliyet gösteren firmaların yetenek ve yetkinliklerinin belirlenmesi, ihtiyaç ve sorunlarının neler olduğu konusunda bilgi toplanması amacıyla "Siber Güvenlikte Yerli Çözümler Çalıştayı" düzenlenmiştir. Bu çalıştaya 18 firmadan toplam 26 firma temsilcisi katılım sağlamıştır. Yapılan sözkonusu çalıştayda;

- Firmaların faaliyetlerini siber güvenlik strateji belgesi ve eylem planlarından habersiz olarak kendi iş planlarına ve/veya öngörülerine göre yürüttükleri,
- Firmalar arasında sinerji ve işbirliği bulunmadığı bu nedenle yürütülen Ar-Ge faaliyetlerinde mükerrerlikler olduğu,
- Ürün ve Müşteri odaklı olmayan daha çok Ar-Ge destek programlarından faydalanmaya odaklı projelerin yürütüldüğü,

görülmüş ve yürütülen siber güvenlik faaliyetlerinin Ulusal kapasitenin oluşturulmasına ve/veya arttırılmasına beklenen olumlu katkıyı sağlayamadığı gözlemlenmiştir.

Siber güvenlik sektöründe yer alan firmalar tarafından yürütülen faaliyetlerin belirlenen hedeflere doğru ve etkin olarak erişebilmeleri ancak müşteri ve kullanıcı makamların yönlendirmeleriyle gerçekleştirilebilir. Bu nedenle Kamu kurum ve kuruluşları ile kritik altyapılara ait siber güvenlik gereksinimlerinin ve tedarik planlarının sektör ile paylaşılması gerekmektedir. Bu kapsamda sektörün kamudan beklentileri aşağıda belirtilmiştir;

- Siber Güvenlik Ekosisteminin devlet destekli olarak kurulması ve sözkonusu ekosistemi destekleyen teşvik ve zorunlulukların getirilmesi,

- Firmaların yetenek ve yetkinliklerine uygun olarak Ekosistem Firma Envanterinin hazırlanması ve Siber Güvenlik ile ilgili İhaleler ve/veya Ar-Ge Destek programlarında bu envanterin kullanılmasının sağlanması,
- Yerli olarak geliştirilecek siber güvenlik teknoloji ve/veya çözümlerinin belirlenmesi ve önceliklendirilmesi amacıyla ulusal bir stratejinin oluşturulması,
- Ulusal stratejinin oluşturulmasında sektörün yetkinliğinin gözönünde bulundurulmasının sağlanması.
- "Kritik Altyapı"larda kullanılacak siber güvenlik çözümlerinin güvenlik seviyesi ve uygunluğu yerli sertifikasyon süreçleri ile doğrulanması,
- Rekabet ortamına açık maliyet etkin sertifikasyon süreçlerinin oluşturulması (özel sektöre ve/veya üniversitelere ait akredite test laboratuarlarının oluşturulması ve sayılarının arttırılması),
- Kamu kurum ve kuruluşları ile kritik altyapılarda yerli ve sertifikalı siber güvenlik çözümlerinin kullanılmasına yönelik KİK'nda gerekli düzenlemelerin yapılması.

4.3 Ekosistem Amacıyla Yapılması Gereken Eylemler

Ulusal Siber Güvenlik Endüstrisinin güçlendirilmesi ve gelişimi açısından, tüm paydaşların yer aldığı ulusal seviyede bir ekosistemin kurulması ve idame ettirilmesi önemli bir konudur. Teknolojik derinlik, yetenek ve altyapı konularında ileri seviyede olan lider şirketlerin yanı sıra sadece belirli konularda bilgi ve tecrübeye sahip KOBİ şirketleride ekosistemde yer almalıdır. Sözkonusu altyüklenici firmaların belli alanlarda bilgi ve tecrübe edinmeleri ve gelişimlerini sürdürebilmeleri sözkonusu ekosistemde lokomotif görevi gören lider şirketler tarafından sağlanmalıdır. Sürdürülebilir bir siber güvenlik ekosisteminin ulusal seviyede maliyet etkin olarak sağlanabilmesi amacıyla ülkemizde yapılması gereken eylem planı aşağıda belirtilmiştir;

- Ekosistemin yönetiminden sorumlu makamın belirlenmesi ve gerekli politika ve stratejilerin oluşturulması,
- Ekosistem içinde yer alan kurum ve kuruluşların rol ve sorumluluklarının net olarak belirlenmesi,
- BT ve Siber Güvenlik ürünlerinin sağlaması gereken performans ve uyumluluk değerlerini tanımlayan yerli standartların oluşturulması ve yayınlanması,
- BT ve Siber Güvenlik ürünlerine ait sertifikasyon süreçlerinin oluşturulması ve gerekli yasal mevzuatın düzenlenmesi,
- BT ve Siber Güvenlik ürünlerinin asgari sağlaması gerek güvenlik seviyelerinin belirlenmesi ve bağımsız akredite test laboratuarlarının oluşturulması,

- Nitelikli insangücü istihdamına yönelik insan kaynağı yetiştirme programı yapılması,
- Kısa, orta ve uzun vadeli hedeflerin belirlenmesi ve bu hedeflere ulaşılması amacıyla gerekli eylem planlarının hazırlanması ve
- Kamu, özel sektör, üniversite ve STK'lar arasında işbirliği ve eşgüdümün sağlanmasıdır.

5. Kritik Altyapıların Güvenliği

Son yıllarda meydana gelen ve her gün kapsamı ve etkisi artan siber saldırı ve olaylar sonucunda ülkelerin güvenliği ve vatandaşların refahının korunması açısından sahip oldukları önemli yani kritik altyapıların belirlenmesi ve korunmasının gerekliliği konusunda ciddi bir görüş birliği oluşmuştur. "*Kritik Altyapı*" kavramı son yıllarda dünyanın hemen her yerinde yaygın olarak kullanılmakla birlikte üzerinde uzlaşılan bir tanımı henüz bulunmamaktadır. Ülkeden ülkeye değişen tanımlar kullanılmaktadır.

Örneğin ABD'de "*ABD için hayati fiziksel veya sanal sistemler ve varlıklar öyle ki böyle sistemlerin ve varlıkların kapasitesiz bırakılması veya yok edilmesi güvenlik, ulusal ekonomik güvenlik, ulusal kamu sağlığı veya emniyeti veya bütün bu sayılanların bir birleşimi üzerinde zayıflatıcı etkiye sahip olacaktır*." şeklinde tanımlanmaktadır.

AB'de ise *"... insanların hayati sosyal fonksiyonlarının, sağlıklarının, emniyetlerinin, güvenliklerinin, ekonomik ve toplumsal refahlarının devamı için gerekli olan ve aksama veya yok edilmesi bu fonksiyonları sürdürmede yetersiz kalma sonucunda bir üye ülkede belirgin etki gösterecek varlık, sistem veya ilgili parçaları*" olarak tanımlanır.

Bu tanımlardan giderek kritik altyapıları, devre dış kalmaları halinde can ve mal kaybına, halkın huzur ve sükûnunun bozulmasına veya ulusal güvenliğin sekteye uğramasına neden olan sistemler olarak tanımlayabiliriz. Kritik altyapılar ülkeden ülkeye farklılıklar gösterse de toplum ve günlük yaşamımızın vazgeçilmezi olan iletişim, ulaştırma, enerji, finans, sağlık, gıda, su kaynakları vb. örnek olarak gösterilebilir. Belirtilen bu kritik altyapılar, temel olarak bilgi sistemleri ve/veya bilgi sistemleri aracılığıyla çalışan sistemlerden oluşmaktadır. Hem kurumsal ağa, hem de internete operasyonel gerekçelerle bağlanabilen bu altyapıların siber saldırılara açık ve korunmasız oldukları da bilinmektedir.

5.1 Kritik Altyapıların Tanımlanması

Kritik Altyapı tanım ve envanterinin sağlıklı bir biçimde yönetilebilmesi, ancak süreklilik arz eden bir belirleme ve değerlendirme süreç döngüsü ile mümkündür. Bu süreç,

sektörler üstü koordinasyonu sağlayacak bir kurum öncülüğünde, kritik sektörlerin sorumlu bakanlık ve düzenleyici otoriteleri ile birlikte kamuya ve özel sektöre ait kuruluş temsilcileri tarafından yürütülmelidir. Periyodik olarak yapılacak değerlendirme çalışmalarıyla, zaman içerisinde Kritik Altyapı vasfını kaybeden veya yeni kazanan unsurlar da tespit edilerek güncel bir Ulusal Kritik Altyapı Envanteri oluşturulmalıdır.

Bu konudaki yabancı kaynaklarda en çok göze çarpan ortak nokta, sürecin başarıyla yürütülmesi için, ISO 31000 belgelerinde tanımlanan şekilde bir risk analiz ve yönetimi metodolojisi uygulanması gerekliliğidir. Kritik altyapı tanımlamasının yapılması ve öncelik seviyelerinin belirlenmesi gereklidir. Bu kapsamda; ulusal kritik altyapı envanterinin oluşturulması, kritik altyapıların güvenlik gereksinimlerinin belirlenmesi ve bu kritik altyapıların bağlı oldukları düzenleyici kurumlar tarafından öncelikli olarak izlenmesi sağlanmalıdır. Buna göre, bir kritik altyapı bileşeninin değeri, aşağıdaki üç parametre göz önüne alınarak tespit edilmelidir:

- Devre dışı kalması halinde oluşacak zararın büyüklüğü,
- Bu zarara yol açması muhtemel açıklıklar ve
- Bu açıklıkları kullanabilecek tehditlerin gerçekleşme olasılığı.

Kritik altyapılarda kullanılacak olan Risk analizi metodolojisinin belirlenmesi önemli bir kazanım olacaktır.

Bu değerlendirme temel alınarak oluşturulacak envanterde, oluşan zararın büyüklüğünün, açıklık miktarının ve tehdit olasılıklarının en aza indirgenmesi amacıyla uygulanacak risk hafifletme planları oluşturulmalı, bu planların başarısı ve uygulanması yakından takip edilmesi gerekmektedir.

Kamu kurum ve kuruluşları ile kritik altyapılarda bulunan verilerin kişisel veri, kritik altyapı verisi ve gizli veri olarak sınıflandırılması ve gizlilik seviyelerine uygun olarak bu verilerin saklanması ve paylaşılması gerçekleştirilmesi sağlanmalıdır.

5.2 Dünyadan Kritik Altyapı Güvenliği Yönetimi

Kritik altyapı güvenliği yönetimi konusunda ulusal seviyede gerekli altyapının oluşturulabilmesi ile güvenlik seviyelerinin maliyet etkin olarak belirlenebilmesi ve sağlanabilmesi amacıyla Avrupa ve Amerika'daki altyapı ve uygulamaların incelenmesi gerçekleştirilmiş ve aşağıdaki bölümlerde detaylı olarak anlatılmıştır.

5.2.1 Avrupa Birliği

Avrupa Kritik Altyapılarının Belirlenmesi ve Güvenliklerinin İyileştirilme Gereksiniminin Değerlendirilmesine İlişkin 2008/114/AB Konsey Direktifi ile "*Kritik Altyapı*"

kavramının yansıra "*Avrupa Kritik Altyapısı*" tanımı da yapılmıştır. Buna göre, Avrupa Kritik Altyapısı envanterini oluşturmak için kullanılan yaklaşım aşağıda belirtilmiştir;

- Sektörlerin kendine özgü kriterleri göz önüne alındığında kritik altyapı olarak tanımlanabilecek sistem veya süreçler nelerdir? (*Kritik Sektörler*)
- Belirlenen bu süreçlerden hangilerinin kaybı veya devre dışı kalması halinde topluma sunulan hizmetlerde, ekonomi, emniyet ve sosyal hayatta kayda değer zarara neden olunur? (*Kritik Altyapılar*)
- Birden fazla AB ülkesini etkileyebilecek olanlar hangileridir? (*Avrupa Kritik Altyapıları*)
- Meydana gelebilecek zararların can kaybı, ekonomik kayıp, toplumsal ve çevresel etkilerinin büyüklüğü nedir? (*Avrupa Kritik Altyapı Envanteri*)

Kritik altyapı unsurlarının belli başlı zafiyetleri ve olası tehdit senaryolarının etki tahmini, bunlara karşı alınacak tedbirlerin belirlenmesi ve önceliklendirilmesi aşamalarını kapsayan risk analizlerinin yapılmasında kullanılacak kriter ve eşik değerleri tanımlayan rehber dokümanlar AB Komisyonu tarafından hazırlanarak üye ülkelerin kullanımına sunulacaktır.

Komisyonun 2012 yılında yayınladığı değerlendirmede, alternatif yaklaşım olarak, öncelikle toplumun karşılaşabileceği büyük ölçekli olumsuz senaryoların belirlenmesi, sonrasında da bunların etkilerinin takip edilerek belirlenmesi biçiminde bir "yukarıdan aşağı" yaklaşımı önerilmiş, bu şekilde farklı sektörlerdeki kritik altyapıların birbirleriyle ilişkisinin daha sağlıklı biçimde tespit edilebileceği öngörülmüştür.

5.2.2 Amerika Birleşik Devletleri

ABD'de Anayurt Güvenliği Teşkilatı (*Department of Homeland Security - DHS*) kritik altyapıların ve önemli kaynakların (*Critical Infrastructure and Key Resources - CIKR*) korunması çalışmalarının koordinasyonundan sorumlu kurumdur. 2002 tarihli Yurt Güvenliği Yasası (*Patriot Act*) ile kurulmuş olan sözkonusu teşkilatın sorumlulukları aşağıda belirtilmiştir;

- Kritik altyapılar hakkında kapsamlı zafiyet ve risk analizleri yapmak
- İlgili bilgileri, analizleri ve zafiyet değerlendirmelerini bütünleştirerek koruyucu ve destekleyici önlemlerin önceliklerini belirlemek,
- Bu görevleri yerine getirmek için gerekli bilgilere etkin ve zamanında erişimin sağlanması konusunda gerekli tedbirleri almak,
- Kritik altyapıların korunması için kapsamlı bir Ulusal Plan hazırlamak,

- Diğer federal kurumlar, Eyalet ve Yerel yöneticiler, ajanslar ve özel sektörle koordineli bir şekilde kritik altyapıların korunması için gerekli tedbirleri önermek,

ABD Anayurt Güvenliği Bakanlığı tarafından ilk olarak 2009 yılında yayınlanan ve 2013 yılında güncellenen "Ulusal Altyapı Koruma Planı"nda, başarılı bir kritik altyapı risk yönetiminin fiziksel güvenlik, siber güvenlik ve insan faktörünün bir arada değerlendirilmesi ile yapılabileceği vurgulanmaktadır. Kritik altyapıların tanımlanması, tehditlerin belirlenip bertaraf edilmesi, açıklıkların kapatılması ve muhtemel senaryoların kritik altyapılar üzerindeki etkisinin değerlendirilmesinin, federal yönetim, eyalet ve bölge yönetimleri, kritik altyapı operatörleri, sivil toplum örgütleri ve akademinin ortak ve etkileşimli olarak yürüteceği faaliyetler ile gerçekleştirilebileceği ifade edilmektedir. Sözkonusu plana göre, kritik altyapı güvenliği çalışmaları;

- Genel ve sektörlere özel güvenlik hedeflerinin belirlenmesi
- Kritik altyapı bileşenlerinin ve birbirleriyle ilişkilerinin belirlenmesi
- Kritik altyapı bileşenleri üzerindeki tehdit, açıklık ve bunların etkilerinin belirlenmesi
- Risk yönetimi faaliyetlerinin belirlenmesi ve uygulanması
- Faaliyetlerin etkisinin ölçüm ve değerlendirilmesi

adımlardan oluşmaktadır:

ABD'de Kritik altyapı olarak belirlenen sektörler aşağıdaki listelenmiştir:

- Tarım ve gıda
- Temel Savunma Sanayi
- Enerji
- Halk sağlığı ve sağlık hizmetleri
- Bankacılık ve Finans
- Su
- Kimya
- Ticari tesisler
- Kritik üretim
- Barajlar
- Acil hizmetler
- Nükleer reaktör, yakıt ve atıklar
- Bilgi teknolojileri ve iletişim
- Ulaştırma sistemleri
- Devlete ait tesisler

5.2.3 Almanya

Almanya'da Bilgi Güvenliği Federal Ofisi (*German Federal Office for Information Security-BSI*) kritik altyapıların korunması çalışmalarının koordinasyonundan sorumlu kurumdur. Almanya'da Siber Güvenlik Strateji Belgesi ve Siber Güvenlik Yasası ile kritik altyapı işletmecileri ve hizmet sağlayıcıları tarafından kritik altyapılarda zorunlu olarak uygulamaları gereken asgari BT güvenlik standartları tanımlanmaktadır. Bunlar;

- Kritik altyapıların işlevselliği için gerekli olan BT sistem, bileşen ve süreçlerinin korunması amacıyla yapısal ve teknik önlemlerin iki yıl içerisinde uygulanması,
- Güvenlik denetimlerinin en az iki senede bir olmak üzere düzenli olarak yapılması ve bulguların Bilgi Güvenliği Federal Ofisine iletilmesi ve
- Kritik altyapılarda gözlenen BT güvenlik olaylarının Bilgi Güvenliği Federal Ofisine raporlanmasıdır.

Almanya başta olmak üzere AB'de Kritik altyapı olarak belirlenen sektörler aşağıdaki listelenmiştir:

- Su
- Enerji
- Ulaştırma sistemleri
- Tarım ve gıda
- Kolluk Hizmetleri
- Bilgi teknolojileri ve iletişim
- Bankacılık ve Finans
- Bayındırlık Hizmetleri
- Federal ve Yerel Hizmetler
- Acil Hizmetler (*Sağlık, İtfaiye vb*)

5.3 Kritik Altyapı Güvenliği Konusunda Yapılması Gerekenler

Ulusal seviyede Kritik Altyapı Güvenliğinin sağlanabilmesi amacıyla ülkemizde yapılması gereken eylem planı aşağıda belirtilmiştir;

- Kritik Altyapı tanım ve envanterinin yapılması,
- Kritik altyapılarda uygulanacak asgari güvenlik seviyelerinin her sektör için belirlenmesi,
- Kritik altyapılarda kullanılacak BT ve Siber Güvenlik ürün ve sistemlerinin sertifikalı ürün olmasının sağlanması,

- Kritik altyapılarda çalışacak personelin alması gereken eğitimlerin belirlenmesi ve bu eğitimlerin periyodik olarak verilmesi,
- Kritik altyapılarda periyodik olarak uygulanacak açıklık analizi, sızma testi ve güvenlik testlerinin belirlenmesi ve uygulanması ve
- Kritik altyapılarda bulunan verilerin sınıflandırılması ve gizlilik seviyelerine uygun olarak bu verilerin saklanması ve paylaşılmasının sağlanmasıdır.

6. Değerlendirmeler

Kritik altyapıların korunması başta olmak üzere siber güvenliğin sağlanmasında gerek devlete gerek özel sektör kuruluşlarına gerekse de bireylere büyük sorumluluklar düşmektedir. Ülkemizde siber saldırılara karşı gerekli koruma önlemlerinin alınması ve uygulanmasında özel sektör daha proaktif bir yaklaşım sergilerken, devlet sektörü genel olarak özel sektörün gerisinde kalmaktadır. Yönetim kademelerinin yanı sıra personel seviyesinde de henüz yeterli siber güvenlik farkındalığının oluşturulamamış olması, nitelikli insan kaynağı eksikliği ve ödenek sıkıntıları nedeniyle kamu kurum ve kuruluşlarında siber güvenlik açıklıklarının ve risklerinin ortaya çıktığı bilinmektedir.

Ülkemizde Siber Güvenlik Kurulu'nun kurularak faaliyete başlaması, Siber Güvenlik Strateji Belgesi ve Eylem Planlarının Resmi Gazete yayımlanması, USOM ve SOME yapılarının oluşturulmaya başlanması çok önemli kazanımlar olmakla birlikte, Siber Güvenlik Ekosisteminin henüz kurulmamış olması sebebiyle; etkin ve sürdürülebilir bir siber güvenlik yapısının ulusal seviyede tesis edilmesi henüz sağlanamamıştır.

Hedeflenen ekosistemde kullanıcılar, tedarik makamları, teknoloji, ürün ve hizmetlerin geliştirilmesine katkı sağlayan yerli sektör paydaşları, standardizasyon ve sertifikasyon kuruluşları, akreditasyon ve eğitim tesisleri, üniversiteler ve STK'lar başta olmak üzere tüm paydaşlar yer almalıdır. Siber güvenlik ekosistemin politika ve stratejileri kısa, orta ve uzun dönem için tüm paydaşlar tarafından anlaşılır şekilde açıkça belirlenmeli ve bu kapsamda oluşturulacak teşvik mekanizmaları, Ar-Ge destek programları ve yasal mevzuatlar üniversite ve STK'lar ile işbirliği yapılarak oluşturulmalıdır.

Ekosistem içinde yer alan kurum ve kuruluşların rol ve sorumlulukları açık bir biçimde belirlenmeli, Yerli sektör tarafından geliştirilen BT ve Siber Güvenlik ürünlerinin performans, güvenlik ve uyumluluk açısından sağlaması gereken yerli standartlar ile sertifikasyon süreçleri tanımlanmalıdır. Sertifikasyon süreçlerinin maliyet etkin ve rekabetçi olabilmesi amacıyla çok sayıda bağımsız akredite test laboratuarlarının oluşturulması, var olan laboratuarların etkin bir biçimde kullanılması için gerekli planlamaların yapılması ve yasal mevzuatın oluşturulması gereklidir.

Mevcut eylem planında siber güvenlikte yerli teknolojilerin geliştirilmesi ve teşvik edilmesi ile yerli ürünlerin kamu kurumları ile kritik altyapılarda kullanımının yaygınlaştırılması yer almaktadır. Ancak, ülkemizde siber güvenlik açısından hangi teknolojilerin kritik olduğu ve yerli olarak geliştirilmesi gerektiğinin belirlenmediği, gerekli öncelendirmenin yapılmadığı, yerli standartlar ile sertifikasyon süreçlerinin tanımlanmadığı ve

Ar-Ge teşvik mekanizmaları ile yasal çerçevenin henüz oluşturulmadığı için bu eylemlerin hedeflenen amaçlara ulaşmadığı görülmektedir.

Hükümet tarafından temel politika ve önceliklerin belirlenmesi ile gerekli Ar-Ge teşvik ve destek mekanizmaları için yasal mevzuatın oluşturulmasına yönelik faaliyetlerin ivedilikle yürütülmesi gerektiği değerlendirilmektedir. Bakanlıklar, Müşteşarlıklar ve Genel Müdürlükler arasında eşgüdümün sağlanması amacıyla siber güvenlik faaliyetlerin tek bir bakanlık altında toplanması veya koordinasyonundan sorumlu bir bakanlığın belirlenmesi önemli katkılar sağlayacaktır.

Ayrıca, Ulusal Siber Güvenlik Makamının, Kamu, özel sektör, üniversiteler ve sivil toplum kuruluşları ile koordinasyon ve eşgüdümü sağlayacak şekilde genişletilmesi, Teknik Çalışma Grupları kurulması ve güçlü bir merkezi yapıya dönüştürülmesi için gerekli yasal düzenlemeleri yapılması ve finansal kaynakların sağlanmasının da en temel adımlar olduğu değerlendirilmektedir.

TBMM'de grubu bulunan partiler tarafından ulusal siber güvenlik ekosisteminin etkin ve sağlıklı yürütülmesine yönelik gerekli desteğin verilmesi ve yaygın etkisinin izlenmesine katılım sağlamaları sözkonusu faaliyetlere önemli kazanımlar ve ivme sağlayacaktır.

Türkiye'de sertifikasyona sahip yerli siber güvenlik yazılımı, donanımı veya işletim sistemi geliştiren şirketlere ve bu şirketlerin ürünlerini kullanmayı tercih eden kurumlara yönelik teşvik ve ilgili mevzuatın düzenlenmesi siber güvenlik ekosistemin gelişimine önemli katkılar sağlayacaktır.

Siber güvenlik alanında nitelikli insan gücü istihdamına yönelik insan kaynağı yetiştirme programı oluşturulmalı ve uygulanmalıdır. İlk ve orta öğretimden başlamak üzere siber güvenlik farkındalık eğitimlerinin verilmesi ve Üniversitelerin müfredatına Siber Güvenlik konusunun alınması, yüksek lisans ve doktora programlarının desteklenmesi, orta ve uzun dönemli başarılar için temel teşkil edecektir.

Eylem Planları kapsamında ülkemizdeki kamu kurumları ile kritik altyapılarda siber güvenlik alanındaki yetişmiş insan gücü açığını kapatmaya yönelik olarak kısa, orta ve uzun vadeli hedefler belirlenmeli ve bu hedeflere göre uzman açığı giderilmelidir. Siber güvenlik farkındalığının sağlanması amacıyla, ilk ve orta öğretim müfredatlarına bilişim teknolojilerinin (*sosyal medya, internet vb.*) güvenli kullanımı konusunda farkındalık eğitimleri eklenmesi, öğretmen ve ebeveynlere siber güvenlik farkındalığı konusunda eğitim programları düzenlenmesi önemli katkılar sağlayacaktır. Ayrıca, siber güvenlik farkındalığını toplumun değişik katmanlarına yaymak amacıyla; Bankalar Birliği, TOBB, TÜSİAD, TMMOB gibi Kuruluşlar ile TBD, BGD gibi STK'ların desteği alınarak basılı ve görsel medyada siber güvenlik konusunun tematik olarak güncel tutulması sağlanabilir.

Yurt dışında ve yurt içinde açılan Siber Güvenlik ile ilgili yüksek lisans ve doktora programlarına katılımın devlet tarafından desteklenmesi ya da özel sektör tarafından bu eğitimin desteklenmesi durumunda vergi muafiyeti sağlanmasının önemli olacağı tarafımızca değerlendirilmektedir.

Siber güvenlik idari ve teknik önlemleri kapsayan bütünsel bakış açısı içerisinde ulusal boyutta değerlendirilmesi gereken bir konudur. Halen yürürlükte siber güvenliğe ilişkin bir kanun metninin bulunmaması ve Kişisel Verilerin Korunması Kanunu'nun yıllardır tasarı halinde TBMM'de bekliyor olması da, ülkemizde siber saldırılara karşı verilecek mücadeleyi olumsuz yönde etkilemektedir. AB mevzuatlarında benimsenen ilkeleri esas alan bir kişisel verilerin korunması kanun metni ile siber olaylarla mücadeleye ilişkin bir düzenlemenin yürürlüğe girmesi, özellikle siber saldırılara karşı koruyucu tedbirlerin alınması açısından daha fazla zaman kaybedilmeden atılması gereken adımlardır.

Özetle, Siber Güvenlik, sadece birkaç kişi ve kurumun sorunu olmayıp, bugün yapılanların yarın yetersiz kalacağı kaygı ve endişeyle sürekli olarak akılda tutulması ve tüm paydaşları kapsayacak şekilde gerekli önlemlerin ivedilikle alınması gereken bir konudur.