

EK-4

Türkiye 3'üncü Bilişim Şûrası

Dijital Egemenlik ve Dayanıklılık Çalışma Grubu

Alt Çalışma Grupları Kapsamındaki

Tespit ve Öneriler

(Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği ya da Bilişim Şûrası organlarının görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.)



İÇİNDEKİLER

1. Güvenli Dijital Teknolojilerin Geliştirilmesi ve Sürdürülebilirliği.....	3
1.1. Tespitler.....	3
1.2. Öneriler.....	5
2. Kritik Dijital Altyapıların Dayanıklılığı ve İş Sürekliliği.....	8
2.1. Tespitler.....	8
2.2. Öneriler.....	10
3. Veri Egemenliği Politikaları ve Kriptoloji.....	16
3.1. Tespitler.....	16
3.2. Öneriler.....	21
4. Toplumsal Dijital Dayanıklılığın Sağlanması.....	24
4.1. Tespitler.....	24
4.2. Öneriler.....	25
5. Siber Olayların ve Siber Olaylara Müdahalenin Dönüşümü.....	31
5.1. Tespitler.....	31
5.2. Öneriler.....	32
6. Ulusal Siber Güvenlik Yönetişimi.....	39
6.1. Tespitler.....	39
6.2. Öneriler.....	44

Ek-4 Tespit ve Öneriler

Ek 4-3/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

1. Güvenli Dijital Teknolojilerin Geliştirilmesi ve Sürdürülebilirliği

1.1. Tespitler

Dijital teknolojide güvenlik, siber tehditlerin büyük önem taşıdığı ve veri ihlallerinin yıkıcı sonuçlara yol açabileceği günümüzün birbirine bağlı dünyasında çok önemlidir. Dijital teknoloji, bilgisayarlar ve akıllı telefonlardan Nesnelerin İnterneti (IoT) cihazlarına ve bulut bilişim platformlarına kadar çok çeşitli sistem ve cihazları kapsar. Bu teknolojilerin güvenliğinin sağlanması, yetkisiz erişime, veri ihlallerine, kötü amaçlı yazılım saldırılarına ve diğer siber tehditlere karşı koruma sağlayacak sağlam önlemlerin uygulanmasını içerir. Buna, aktarılan ve âtıl durumdaki verileri güvence altına almak için şifreleme, kullanıcı kimliklerini doğrulamak için çok faktörlü kimlik doğrulama, ağ trafiğini şüpheli etkinliklere karşı izlemek için izinsiz giriş tespit sistemleri ve güvenlik açıklarını gidermek için düzenli güvenlik güncellemeleri ve yamalar dâhildir. Ayrıca kuruluşların, hassas bilgileri korumak ve müşteri güvenini sürdürmek için katı düzenleyici gereksinimlere ve endüstri standartlarına uyması gerekir.

Türkiye’de güvenli dijital teknoloji ekosistemi büyük ilerlemeler kaydetmektedir. Fakat hâlâ istenilen noktaya ulaşabilmiş durumda değildir. Güvenli teknolojinin sürdürülebilirliği bir bakıma millî teknolojide gelişmeyi zorunlu kılmaktadır. Ülkemizde millî teknolojik ürünlerin teşvik edilme çabalarına rağmen ön yargılar hâlâ devam etmekte ve millî ürünlerimizin kullanılması daha zorlu bir hâle gelmektedir. Bunun sebebi yerli ürünlerin yabancı ürünlerle karşılaştırıldığında kalitesinin düşük görülmesi veya güvenilirliğinin daha az olduğunun düşünülmesidir. Yerli ürün fiyatlarının uygun olmasına rağmen bu algılar nedeniyle piyasaya girmekte zorluk çekip kabul görmekte zorlanmaktadır. Bu gibi düşünceler üretici firmayı da zora sokmaktadır. Ürünün gelişiminin sağlanması için ürün kullanımına ve geri dönüşlere ihtiyaç vardır. Bu döngüye girildiğinde devlet kurumlarının müdahil olması gerekmektedir. Yerli ürünlerin faydalarını ve kalitesini öne çıkaracak planlamalar yapılması ve bu yönde bilinçlendirmeye gidilmesine ihtiyaç vardır. Bunun için kampanyalar düzenlenip firmalara da teşvikler verilebilir. Ek olarak yerli teknolojik ürünlerin kullanımına ve benimsenmesine öncelik veren, destek olan kuruluşlar veya firmalar vergi indirimi veya sübvansiyon gibi destekler alabilmelidir. Yerli ürünlerin düşük kalite algısını yıkmak için ise başarılı uygulama sergileyen girişimciler ve potansiyel kullanıcılar arasında güven ağı ve etiketleme oluşturulmalıdır.

Ek 4-4/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

Ek-4 Tespit ve Öneriler

Yerli firmalarımızın yaşadığı bir diğer zorluk ise satış ve pazarlama kısmıdır. Bu alandaki sınırlı uzmanlık ve destek hizmetlerine duyulan endişe birleştirildiğinde küresel çapta genişleme ve gelişme çabalarına engel olmaktadır. Şirketler ürünlerini uluslararası alanda kullanımının artırılması için pazarlamakta ve sürekli destek sağlamakta zorluklar yaşamaktadır. Bu durum yerli firmaların rekabet güçlerini olumsuz yönde etkilemektedir. Bunun üstesinden gelebilmek için satış ve pazarlama profesyonellerine yönelik eğitim programlarına yatırım yapılmalı ve satış sonrası destek için hizmetler geliştirilmelidir.

Ürün geliştirmeden ticarileşmeye yolculuk, yeni başlayanlar ve şirketler için özellikle finansman, bürokrasi ve devlet kurumlarının desteği açısından sayısız zorluk teşkil etmektedir. İlk satışa kadar finansman sağlamak, genellikle TÜBİTAK gibi kuruluşların desteğini gerektirdiğinden çok önemlidir. Ancak bürokratik süreçlerde gezinmek ve bakanlıklarla gerekli belgeler üzerinde çalışmak karmaşık olabilir ve ilerlemeyi engelleyebilir. Yönetimdeki değişiklikler veya kaynak yetersizliği nedeniyle projeler yarım bırakılabileceğinden, ürün geliştirmede sürdürülebilirlik başka bir endişe kaynağıdır. Bu engellerin aşılması, projelerin başarılı bir şekilde tamamlanmasını ve sürekliliğini sağlamak için etkili planlama, kaynak yönetimi ve uzun vadeli hedeflere bağlılık gerektirir. Bu zorlukların üstesinden gelmek için hem devletten hem de özel sektörden finansman ve destek şarttır, ancak süreci kolaylaştırmak için bürokrasi en aza indirilmelidir.

Yerli firmalarımız hedeflenen büyüklüğe ulaştığında veya globalleştiğinde ‘exit’ durumu meydana gelebilmektedir. Ortada bir çıkış olsun ya da olmasın kullanımdaki bir ürün için en önemli nokta ürünün hayatta kalması yani sürdürülebilirliğidir. Ürünlerin varlığının devamını sağlamak için uygun önlemler alınmazsa kaynakların israf edilmesi ve ürünün tahrip olması riski vardır. Üstelik bu süreçler üretimde aksamalara yol açarak, üretimin gelişmesini tehdit edebilir, hatta bazı pazarların tekelleşmesine bile yol açabilmektedir. Özellikle şirketlerin mevzuata uyum gereklilikleri konusunda yeterince bilgi sahibi olmaması durumunda, uluslararası patent hakları ve fikri mülkiyet ile ilgili sorunlar da ortaya çıkabilmektedir. Ayrıca, özellikle ürün kodlarının mülkiyeti veya hassas bilgilerin yabancı kuruluşlara devredilmesi durumunda veri güvenliği, gizlilik ve teknoloji aktarımıyla ilgili sorunlar yaşanabilir. Ek olarak, dikkatli bir planlama yapılmazsa, yerel işletmeler yanlışlıkla yabancı kontrolü altına girebilir ve bu da yurt içinde

Ek 4-5/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.



Ek-4 Tespit ve Öneriler

üretilen ürünlerin yabancı yatırımcılar tarafından değiştirilmesine veya durdurulmasına yol açabilir. Şirketlerin bu potansiyel sorun alanlarını proaktif olarak ele alması ve bu dönüşüm süreçlerinde riskleri azaltacak stratejiler uygulaması kritik önem taşımaktadır.

Ürünlerin sürdürülebilirliği, teknolojik gündeme ve kullanıcı ihtiyaçlarına uyum, üretici fikri mülkiyetinin ağırlığı, üreticinin yönetim olgunluğu ve finansman kabiliyeti gibi birçok başlık ile etkileşim halindedir.

1.2. Öneriler

Siber güvenlik ve teknoloji bağlamında dijital egemenlik, iş birliği, ürün geliştirme ve ekosistem desteğine ilişkin birçok kritik konu mevcuttur. Bunlardan ilki şirketler içindeki dijital egemenlik eksikliği, yetersiz iş birlikleri ve belirsiz gelecek planlamalarıdır. Şirketlerin ürün ortaya koyması ve sürdürülebilirliğini devam ettirmesi oldukça zorlu bir süreçtir. İyileştirmeler olsa da daha güçlü iş birlikleri, daha net gelecek planları ve şirketlerin ürün eksikliklerini gidermek için kamu-özel şirket güçlerini birleştirmelerinin teşvik edilmesi yönünde bir çağrı vardır.

Bunlara ek olarak yerel ürünlerin kullanımının teşvik edilmesine, zorunlu güvenlik önlemlerinin desteklenmesine ve ekosistem içindeki dernekler ve açık kaynak toplulukları arasındaki ilişkilerin geliştirilmesine vurgu yapılmaktadır. Ayrıca, yerel ürünlerin kullanımında geri bildirim eksikliğinin kalkınmayı engellediği, mevzuatın daha esnek hâle getirilmesi, pazarların açık hâle getirilmesi ve büyümeyi kolaylaştırmak için geri dönüşlerin teşvik edilmesi gerektiğine işaret ettiği vurgulanmaktadır.

Dijital teknolojilerin benimsenmesinin yarattığı zorluklara ilişkin tartışmadan bunların güvenliği sorununa geçildiğinde, bu engellerin daha geniş bir dijital güvenlik sorunuyla yakından ilişkili olduğu açıktır. Yerli ürünlere yönelik ön yargılar, satış ve globalleşmedeki zorluklar, bu ürünlerin pazara girişini engellemekle kalmamakta, aynı zamanda güvenlik ve güvenilirlik konusunda da kaygıları artırmaktadır. Dijital egemenliğe ilişkin endişeler, hassas verileri yetkisiz erişime ve dışa aktarıma karşı korumak için güçlü güvenlik önlemlerinin önemini daha da vurgulamaktadır. Yerli ürünlerin kullanımının teşvik edilmesi ve paydaşlar arasında iş birliğinin geliştirilmesi yönünde çalışmalar yapılırken, bu teknolojilerin güvenliğinin sağlanması da kritik hâle gelmektedir. Katmanlı güvenlik sistemlerine ve düzenli denetimlere duyulan ihtiyaç da dâhil

Ek 4-6/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.



Ek-4 Tespit ve Öneriler

olmak üzere siber güvenlik sorunları, siber tehdit riskini azaltmak için güvenlik açıklarını ele alma zorunluluğunu vurgulamaktadır. Ayrıca, eğitimi ve mevzuatı iyileştirmeye yönelik girişimler, profesyonelleri güvenli dijital teknolojileri geliştirmek ve sürdürmek için gerekli becerilerle donatırken aynı zamanda yenilik ve büyümeye olanak sağlayan bir ortam yaratmanın anahtarıdır. Bu nedenle, Türkiye bu zorluklarla karşı karşıya kalırken, dijital teknolojilerinin güvenliği, teknoloji sektörünün tüm potansiyelini ortaya çıkarmak ve küresel rekabet gücünü artırmak için merkezi bir husus olmaya devam etmektedir.

Ülkemizde var olan dijital teknolojilerin güvenlik tehlikesine karşı sunulan çözümlerin temeli eğitimden geçmektedir. Artan siber güvenlik tehditleri ve nitelikli siber güvenlik uzmanlarına olan talep ile mevcut iş gücü arasındaki sürekli eşitsizlik ışığında, kapsamlı eğitim ve öğretim girişimlerine öncelik vermek zorunludur. Bu, bireyleri siber riskleri etkin bir şekilde azaltmak için gerekli becerilerle donatmayı amaçlayan, güvenli kodlama uygulamalarına ve mimari perspektiflere hitap edecek şekilde uyarlanmış özel eğitim içeriğinin geliştirilmesini gerektirir. Ayrıca, çabalar, eğitim kurumlarının kalitesini artırmaya, müfredatın en son endüstri standartlarını ve uygulamalarını yansıtacak şekilde güncellenmesini sağlamaya ve öğrencilere en son teknolojilere ve pratik öğrenme fırsatlarına erişim sağlamaya odaklanmalıdır.

Güvenli kodlama uygulamalarına ve mimari perspektiflere odaklanan eğitim materyalleri oluşturmak önemlidir. Buna çevrimiçi kurslar, atölye çalışmaları, eğitimler ve çeşitli beceri düzeylerine göre uyarlanmış yazılı kılavuzlar dâhil olabilir. Güvenli kod geliştirme ve yönetişimi sağlamaya yönelik kurs ve eğitim programlarının hem lisans hem de lisansüstü düzeyde üniversite müfredatına entegre edilmesi, siber güvenlik sorunlarıyla başa çıkmak için gerekli beceri ve bilgiye sahip mezunların yetiştirilmesine yardımcı olur.

Siber güvenlik alanında eğitim kurumlarının kalitesinin artırılması hayati önem taşımaktadır. Bu, müfredatın en son endüstri standartlarını yansıtacak şekilde güncellenmesini, pratik öğrenim için en son teknolojilere erişim sağlanmasını ve siber güvenlik alanında araştırmaların teşvik edilmesini gerektirir. Ayrıca uzmanlar tarafından verilen ders ve seminerlerin düzenlenmesi, öğrencilere ve profesyonellere paha biçilemez bilgiler ve gerçek dünya deneyimleri sağlayabilir. Bu oturumlar, ortaya çıkan tehditleri, en iyi uygulamaları ve anlayışı ve farkındalığı artırmaya yönelik vaka çalışmalarını kapsayabilir.

Ek 4-7/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.



Ek-4 Tespit ve Öneriler

Yerel şirketlere iş geliştirme ve dağıtım ağları kurma konusunda eğitimler vermek, ürün ve hizmetlerinde siber güvenliğin önemini anlamalarına yardımcı olur. Bu, geliştirme yaşam döngüsü boyunca en iyi güvenlik uygulamalarının benimsenmesine yol açabilir. Özellikle Linux sistemlerine odaklanan özel eğitimler sunmak, sistem yöneticilerine altyapıyı etkili bir şekilde güvence altına almak için gereken bilgi ve becerileri kazandırır. Buna ağ güvenliği, erişim kontrolü, izinsiz giriş tespiti ve olaylara müdahale gibi konular dâhildir.

Genel olarak bu açıklamalar, siber güvenlik ve teknoloji ekosistemlerini güçlendirmek için gerekli olan, düzenleyici önlemler, iş birliği, pazar teşvikleri ve destek dâhil olmak üzere çok yönlü yaklaşımın altını çizmektedir. Bu stratejiler uygulanarak siber güvenlik uzmanlarına olan talep ile mevcut yetenek havuzu arasındaki boşluk kapatılabilir ve aynı zamanda geliştiriciler, yöneticiler ve kullanıcılar arasında siber güvenlik farkındalığı ve en iyi uygulamalar kültürü teşvik edilebilir.

Ek 4-8/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.



2. Kritik Dijital Altyapıların Dayanıklılığı ve İş Sürekliliği

2. 1. Tespitler

Türkiye'nin mevcut altyapı dayanıklılığı, sektörler arasında farklılıklar göstermekte olup, jandarma ve polis kurumlarında dikkate değer güçlü yönler bulunurken, vatandaşların ulaşım ve iletişim altyapısında uydu iletişim sistemlerinin uygulanmasını gerektiren önemli eksiklikler bulunmaktadır.

Enerji altyapıları genel dayanıklılık açısından hayati önem taşırken, altyapı kurulumları için çeşitli enerji kaynaklarından gelen çözümlere ve gelişmiş bina dayanıklılığına duyulan ihtiyaç da kabul edilmiştir. Enerji altyapılarının daha fazla dayanıklılık için güçlendirilmesi gerekirken, kritik altyapı binalarının dayanıklılık iyileştirmelerine ihtiyacı vardır. Planlamayı optimize etmek için, bölgesel risk eşitsizlikleri ve sektörler arası bağımlılıklar dikkate alınarak iletişim uyumluluk düzeyleri haritalandırılmalıdır. Projelerin tamamlandıktan sonra rafa kaldırılmaması ve sürekli değerlendirilmesi zorunludur. Yatırımlar fiziki coğrafyanın ötesine geçerek dijital altyapıda sıfır gün hazırlığına öncelik vermelidir.

Telekomünikasyon sektöründe Türkiye büyük ölçüde mevcut fiber altyapısına sahiptir ancak bunu genişletme ve çeşitlendirme yönünde artan bir zorunluluk mevcuttur. Ayrıca, özellikle İnternet altyapısı açısından düşük yörünge uydu eksikliğinin giderilmesi de büyük önem taşımaktadır. Özellikle afet senaryolarına uygun alternatif rota ve kanalların çeşitlendirilmesinin, acil durumlarda dayanıklılığın artırılması ve kesintisiz iletişimin sağlanması açısından hayati önem taşıdığı görülmektedir. Türkiye, bu girişimlerin yalnızca küresel teknolojik gelişmelere ayak uydurmak açısından değil, aynı zamanda genel telekomünikasyon altyapısının dayanıklılığını ve hazırlığını artırmak açısından da öneminin farkındadır. 6G/7G gibi teknolojik gelişmelerin gerisinde kalan Türkiye, kamu-özel sektör iş birliğinin geliştirilmesini zorunlu kılmaktadır.

Zorluklar arasında sektörel olgunluk eşitsizlikleri, altyapılar arası bağımlılık analizinin yetersiz olması ve sürekliliği engelleyen kültürel engeller yer almaktadır. Mevcut altyapı açıklarını gidermek için acil testler ve eylem planları gereklidir. Enerji, ulaştırma ve iletişim sektörleri arasında koordinasyon zorlukları devam etmekte ve depremle ilgili sorunlar daha da kötüleşmektedir. Baz istasyonlarının istikrarsız yapıların üzerine kurulması, organizasyon ve

Ek 4-9/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

Ek-4 Tespit ve Öneriler

tatbikat eksikliğinin de etkisiyle ciddi riskler oluşturmaktadır. Bireysel çabalardan ziyade verimli operatör etkileşimi ve veri paylaşımı savunulmaktadır. Çeşitli iletişim altyapılarından kaynaklanan karmaşıklık hizmet eşitsizliklerini artırmakta, felaket senaryolarına yönelik modellemede alınması gereken yol zorlukları artırmaktadır. İletişim altyapısında kamu yatırım modellerinin yetersiz oluşu ilerlemeyi engellemektedir. Ek olarak, çöken yapılar, şebeke bağımlı ve yedek gücü limitli baz istasyonu arızaları, sağlam altyapı planlamasına ve dayanıklılık önlemlerine olan ihtiyacın altını daha da çizmektedir.

2012 yılında siber güvenlik kurulunun kurulmasından bu yana ilerleme kaydedilmiş ancak hâlen alınabilecek yol vardır. Özellikle fiber ve GSM hatlarındaki iletişim altyapısı eksiklikleri 2023 depremiyle ortaya çıkmıştır. Deprem, su baskını, yangın ve yoğun kar yağışına karşı kırılganlığı göz önüne alındığında, altyapının dayanıklılığı Türkiye için çok önemlidir. Pek çok kurum önlem alırken gerçekçi afet tatbikatlarındaki eksiklikler devam etmektedir. Dirençlilik ve dijitalleşmenin vurgulanması, çeşitli krizlere uyum sağlayabilen, açık kaynak veya yerel-millî yaklaşımlara dayanan çözümleri gerektirmektedir.

2012 yılındaki düzenleyici müdahaleler sonrasında artan güvenlik farkındalığı ve kritik enerji altyapılarında hem fiziksel hem de siber kontrollerin uygulanması olumlu bir ilerlemeye işaret etmektedir. Ancak Türkiye, siber saldırılara etkili bir şekilde yanıt verme konusunda hâlâ zorluklarla karşı karşıyadır. Yetersiz kaynak tahsisi ve kritik altyapıların siber saldırılara karşı analizi endişe kaynağı olmaya devam etmektedir. Ayrıca, özellikle yer altına almanın fayda sağladığı ancak deprem onarım süreçlerini zorlaştırdığı kentsel alanlarda enerji dağıtım hatlarının dayanıklılığının sağlanması önemli bir zorluk teşkil etmektedir. Kritik altyapıların korunmasına ilişkin politika ve mevzuatın kapsamı ve etkinliği hem yerel hem de ulusal düzeyde farklılık göstermektedir. Enerji ve su gibi bazı sektörler köklü ulusal stratejilere ve düzenlemelere sahipken, sağlık sektörü gibi diğerleri, kritik önlemlerine rağmen aynı düzeyde ilgi göremeyebilmektedir. Bu politikalardaki boşlukların ele alınması, tüm temel altyapı sektörlerinin dayanıklılığının artırılması açısından önemlidir. Kritik altyapıların korunmasından sorumlu kurumlar arasında koordinasyonun ve bilgi paylaşımının geliştirilmesi büyük önem taşımaktadır. Şu anda, çeşitli kurumlar arasında parçalanmış sorumluluklar, gözetim ve müdahale yeteneklerinde boşluklara yol açabilir. Düzenlemelere ve politikalara bütünsel bir yaklaşım, çalışmalarını kolaylaştırabilir ve

Ek 4-10/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

Ek-4 Tespit ve Öneriler

düzenleyici kurumlar arasındaki iş birliğini geliştirebilir, sonuçta Türkiye'deki kritik altyapıların genel dayanıklılığını güçlendirebilir.

2. 2. Öneriler

Kritik altyapıların dayanıklılığının sağlanması için hem yerel hem de ulusal düzeyde paydaşlar arasındaki koordinasyon esastır. Bu koordinasyon, zorlukların ve zayıf noktaların etkili bir şekilde ele alınması için hem kamu hem de özel kurumları içermelidir. Kritik altyapılarda koordinasyonu ve dayanıklılığı artırmaya yönelik bazı önemli hususlar şunlardır:

- **Fiber Altyapıların Dâhil Edilmesi:** Fiber altyapıların iletişim ağlarının kritik bileşenleri olarak kabul edilmesi, korunmasına ve dayanıklılığına öncelik verilmesi. Bu, fiber optik tesislerin stabilitesini ve güvenliğini sağlamak için konum gruplarının oluşturulmasını ve önlemlerin uygulanmasını içerebilir.
- **Afet Simülasyon Tatbikatları:** Potansiyel afetleri simüle etmek ve müdahale planlarının ve prosedürlerinin etkinliğini test etmek için gerçekçi tatbikatlar yapmak.
- **Telekomünikasyon ve Fiziksel Güvenlik:** Kritik altyapıları siber saldırılar ve fiziksel sabotaj dâhil olmak üzere çeşitli tehditlere karşı korumak için hem dijital hem de fiziksel güvenlik endişelerini ele almaktadır.
- **Altyapı Sınıflandırması ve İlişki Haritalaması:** Karşılıklı bağımlılıkları ve güvenlik açıklarını daha iyi anlamak için altyapıları (ör. BT, OT) sınıflandırmak ve birbirleriyle olan ilişkilerini haritalandırmak.
- **Risk Yönetimi ve İş Sürekliliği Planlaması:** Risklerin etkin bir şekilde tanımlanması ve azaltılması için risk yönetimi süreçlerinin ve iş sürekliliği planlamasının uygulanması, temel hizmetlerin sürekliliğinin sağlanması.
- **Organizasyon Yapıları:** İlgili paydaşlar için net roller ve sorumluluklar da dâhil olmak üzere, dayanıklılık çabalarını denetlemek ve yönetmek için uygun organizasyonel yapıların oluşturulması.

Ek 4-11/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

Ek-4 Tespit ve Öneriler

- Karasal Altyapı Geliştirme: Bağlantıyı ve dayanıklılığı artırmak için fiber optik ağlar gibi karasal altyapıların geliştirilmesine, genişletilmesine ve çeşitlendirilmesine yatırım yapmak.

- Düzenleyici Çerçeveler: Kritik altyapıların olgunluğunu ve güvenliğini artırmak için denetim ve sızma testi gereklilikleri gibi mevzuat ve düzenlemeleri yürürlüğe koymak. Ayrıca dayanıklılık çabalarını desteklemek ve altyapı yönetimini geliştirmek için dijital ikizler gibi teknolojilerden yararlanılmaktadır.

- Dış Erişimin Çeşitlendirilmesi: Ağırlıkla batıya doğru yapılandırılmış ülke İnternet çıkış hatlarının doğu yönüne doğru çeşitlendirilerek dengelenmesi.

Ülkeler, bu hususları ele alarak ve paydaşlar arasındaki iş birliğini teşvik ederek, kritik altyapılarının dayanıklılığını güçlendirebilir ve çeşitli tehdit ve zorluklara daha iyi dayanabilir. Altyapının dayanıklılığını artırmak ve çok sayıda potansiyel zorluğa karşı dayanıklılığı sağlamak için, çeşitli sektörler ve kritik altyapı alanlarında kapsamlı bir dizi teknolojik çözüm ve yeniliğin uygulanması tavsiye edilmektedir.

- Güvenli Bulut Altyapılarının Yaygınlaştırılması: Krizler sırasında veri dayanıklılığını ve erişilebilirliğini sağlamak için kurumlar güvenli bulut altyapılarının benimsenmesine öncelik vermelidir.

- Yerel Hizmetleri Mikro Çözümlerle Güçlendirmek: Mobilite ve uç bilişim için mikro çözümlerin devreye alınması, yerel hizmet sunumunu destekleyerek kesintilere karşı dayanıklılığı artırabilir.

- Alternatif İletişim Altyapılarının Kurulması: Uydu iletişimi ve 5G/6G ağları gibi alternatif iletişim altyapılarının geliştirilmesi, bağlantıda yedeklilik ve esneklik sağlayabilir.

- Yedek Haberleşme Altyapısı Yatırımları: Afet anında iletişim kesintisi riskinin azaltılması için yedek haberleşme altyapısına daha fazla yatırım yapılmalıdır.

- Dijital İkizlerin Oluşturulması: Kritik altyapıların modellenmesi ve dijital ikizlerin oluşturulması, çeşitli senaryoları simüle ederek ve güvenlik açıklarını belirleyerek afete hazırlık ve müdahaleyi iyileştirebilir.

Ek 4-12/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

Ek-4 Tespit ve Öneriler

- Yerli Teknolojilerin Geliştirilmesi: Kendine güvenin sağlanması ve dışa bağımlılığın azaltılması için yerli teknolojilerin geliştirilmesine ve yaygınlaştırılmasına öncelik verilmelidir.
- Coğrafi Olarak Çeşitli Yatırımlar: Güneş enerjisi gibi yenilenebilir enerjiye yapılan yatırımlar, bölgeler arasında enerji dayanıklılığını sağlamak için coğrafi olarak çeşitlendirilmelidir.
- Altyapı İzleme Merkezlerinin Kurulması: Kritik altyapıların sürekli izlenmesi ve alarm ve anormalliklere anında müdahale edilmesi için merkezi altyapı izleme merkezlerinin hayata geçirilmesi gerekmektedir.
- Kritik Altyapının Belirlenmesi: Stratejik planlama ve yatırımı sağlamak için baz istasyonları ve fiber ağlar gibi kritik altyapılar ulusal öncelikler olarak tanımlanmalıdır.
- Uydu Tabanlı Sistemlerin Dağıtımı: Uzak veya afetten etkilenen bölgelerde güvenilir iletişim ve bağlantı sağlamak için uydu tabanlı mobil istasyonlar da dâhil olmak üzere uydu tabanlı sistemlerin dağıtımı artırılmalıdır.
- Birlikte Çalışabilirlik: Acil durumlarda kesintisiz operasyonları ve kaynak paylaşımını kolaylaştırmak için farklı altyapı sistemleri arasında birlikte çalışabilirlik sağlanmalıdır.
- Kule Tarzı Yapılar: Baz istasyonlarının çevresel tehlikelere ve fiziksel hasara karşı dayanıklılığını artırmak için bina üzeri yerine kule tarzı yapılar tercih edilmelidir.

Afetlere ve salgın hastalıklara karşı risk yönetimi stratejilerinde ve hazırlıklarda ana hatlarıyla belirtilen öncelikler, ulusal ve kurumsal düzeyde dayanıklılık ve hazırlıklılığın artırılması açısından hayati öneme sahiptir. Öncelikle belirlenen risklerin ve çözümlerin içselleştirilmesi, etkin risk yönetimi için hayati önemi haizdir. Bu, tatbikatlar ve çalıştaylar yoluyla testlerin artırılmasını, gerçekçi simülasyonlar için sanal gerçeklik gibi teknolojilerin kullanılmasını ve kritik süreçleri ele almak için yeterlilikler ve protokoller geliştirmeyi içerir.

Ulusal düzeyde birleşik bir risk yönetimi yaklaşımının benimsenmesi, çeşitli kurumlar ve özel sektör arasındaki iş birliğini teşvik etmektedir. Sıfır güven yaklaşımıyla güvenliğe öncelik

Ek 4-13/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

Ek-4 Tespit ve Öneriler

verilmesi ve acil durum planlarının AFAD gibi merkezi bir otorite altında koordine edilmesi, hazırlık ve müdahale yeteneklerini artırmaktadır. Afet ve salgın hastalıklar karşısında zafiyetlerin belirlenmesi ve iş sürekliliğinin sağlanması için risk oluşturan varlıkların kapsamlı bir envanterinin çıkarılması ve iş süreçlerinin etkin bir şekilde analiz edilmesi büyük önem taşımaktadır.

Afet ve salgın hastalıkların etkilerini azaltmak için yedekleme planlarının ve uyarı mekanizmalarının uygulamaya konulması büyük önem taşımaktadır. Bu, yedekli iletişimler, jeneratörler ve alternatif ulaşım yöntemleri oluşturma yanısıra uzaktan sistem yönetimi yeteneklerinin ve salgınlar için insan yedekleme planlarının güçlendirilmesini de içerir. Geçmişte yaşanan afet ve salgın hastalıkların kapsamlı bir şekilde analiz edilmesi, elde edilen verilere dayalı olarak alternatif planların hazırlanmasına olanak sağlamaktadır. Bu, bölgeler veya iller arasındaki desteklerin belirlenmesini, tüm senaryolara yönelik afet çalıştayları ve tatbikatlarının düzenlenmesini ve kritik bileşenlerin ve varlıkların belirlenmesini içerir.

Ulusal risk kriterlerinin tanımlanması ve kritik altyapı alanlarının önceliklendirilmesi, farklı paydaşlar arasında netlik ve koordinasyon sağlar. Siber tehditlere etkin yanıt için siber küme yapısının oluşturulması, dijital alanda korumayı ve hazırlıklılığı artırır. Karasal ve uydu ağları da dâhil olmak üzere öncelikli telekomünikasyon altyapılarının güvenliğine ve dayanıklılığına öncelik verilmesi çok önemlidir. Bu, dayanıklı baz istasyonlarının kurulmasını ve acil durumlar ve iş paylaşımı yetenekleri için yeterli uydu tabanlı mobil istasyon sağlanmasını içerir.

Afet ve salgın senaryolarında hızlı ve etkili iletişimde mevcut durumun analizi, iyileştirme ve spesifik sistemlerin geliştirilmesi gereken birçok kritik alanı ortaya çıkarmaktadır. Öncelikle baz istasyonlarının dayanıklılığının sağlanması çok önemlidir. Operatör baz istasyonlarının bulunduğu binaların, temel iletişim altyapısını korumak için afetlere karşı dayanıklı olması gerekir. İkinci olarak, mobil baz istasyonlarının yaygınlığının artırılması, afetten etkilenen bölgelerde hızlı bir şekilde esnek iletişim ağlarının kurulmasını sağlayabilir. Özellikle karasal altyapının zarar gördüğü bölgelerde uydu üzerinden alternatif İnternet erişiminin geliştirilmesi, vatandaşlara bağlantı imkânı sağlanması büyük önem taşır. Krizler sırasında dezenformasyonla mücadele etmek, bilginin doğru ve zamanında yayılmasını kolaylaştırmak için stratejik iletişim sistemlerine ihtiyaç vardır.

Ek 4-14/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.



Ek-4 Tespit ve Öneriler

Acil durum iletişim altyapısına yönelik konuşlandırılabilir yapıların bakımı, afetten etkilenen bölgelerde hızlı dağıtım ve kurulumla olanak tanır. Karasal ağların bulunmadığı uzak veya ulaşılması zor bölgelerde uydu iletişimi bir alternatif olarak değerlendirilmelidir. Omurgadan bağımsız altyapının veya dağıtılmış uygulamaların geliştirilmesi, merkezi sistemler arızalansa bile iletişim esnekliğini sağlar.

Afet ve acil durumlarda iletişim hizmetlerinin kesintisiz sağlanması için güçlü iş sürekliliği sistemleri geliştirilmelidir. Acil durumlarda daha hızlı ve etkili iletişim stratejileri için kurumlar arası koordinasyonun geliştirilmesi esastır. Afet ve salgın hastalıklarda iletişim, enerji ve ulaşım hizmetlerinin koordinasyonundan sorumlu merkezi bir iletişim koordinasyon biriminin kurulması hayati önem taşımaktadır. İletişim cihazlarının enerji sistemlerine entegrasyonu, harici güç kaynakları olmadan bile kesintisiz çalışmayı sağlar. Uydu telefonu ve İnternet gibi iletişim kanallarının çeşitlenmesi, iletişim ağlarında yedeklilik ve esneklik sağlar. WhatsApp'a benzer şekilde ulusal düzeyde sağlam ve güvenli bir iletişim altyapısının geliştirilmesi, kriz sırasında güvenilir iletişimin sağlanmasını sağlar. Baz istasyonları ve fiber altyapısının kamu risk analizine göre yapılandırılması, afetlere karşı en hassas bölgelere öncelik vermektedir. Kule bazlı iletişim sistemlerine önem verilmesi, özellikle afet riski taşıyan kentsel alanlarda kapsama alanını ve dayanıklılığı artırır.

Bu kritik alanların ele alınması ve spesifik sistemlerin geliştirilmesi, afetler ve salgın hastalıklar sırasında iletişimin etkinliğini ve dayanıklılığını önemli ölçüde artıracaktır.

Ülkeler, bu kritik alanları ele alarak ve önerilen sistemleri geliştirerek afetler ve salgın hastalıklar sırasında hızlı ve etkili iletişim kurma yeteneklerini önemli ölçüde geliştirebilir, böylece genel dayanıklılığı artırabilir ve bu tür olayların topluluklar ve altyapı üzerindeki etkisini en aza indirebilir. Bu teknolojik çözümlerin ve yeniliklerin uygulanması, Türkiye'nin altyapı direncini güçlendirerek güvenlik risklerine, afetlere ve salgın hastalıklara daha iyi dayanabilmesini sağlayacak ve krizler sırasında temel hizmetlerin ve iletişim kanallarının sürekliliğini sağlayacaktır.

Kritik altyapılara yönelik yerli ve millî çözümler geliştirmek, dışa bağımlılığı azaltarak ve altyapı güvenliği üzerinde daha iyi kontrol sağlayarak dayanıklılığı artırabilir. Açık kaynak çözümleri, kritik altyapı teknolojisi geliştirmede iş birliğini, şeffaflığı ve yeniliği teşvik ederek dayanıklılığa katkıda bulunur.

Ek 4-15/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.



Ek-4 Tespit ve Öneriler

İletişim, enerji ve ulaşım gibi kritik altyapı sektörleri arasında bütünsel değerlendirme ve koordinasyon, karşılıklı bağımlılıkları ve zayıf noktaları tespit etmek ve genel dayanıklılığı artırmak için gereklidir. Kritik altyapı tanımının sağlık ve tarım gibi sektörleri kapsayacak şekilde genişletilmesi, bunların öneminin farkına varır ve tehditlere karşı kapsamlı koruma sağlar. Tüm sektörlerde siber olgunluğun değerlendirilmesi, zayıf yönlerin belirlenmesine ve riskleri etkili bir şekilde azaltmak için siber güvenlik önlemlerine yapılan yatırımların önceliklendirilmesine yardımcı olur. Siber caydırıcılık ve egemenliğe ulaşmak, siber tehditlere karşı savunma yapmak ve düşmanlara sonuçlar dayatmak için politikalar, doktrinler ve yetenekler geliştirmeyi içerir.

Yapay zekâ, bulut bilişim ve dijital ikizler gibi teknolojik altyapılardan yararlanmak, gelişmiş simülasyonlar, tahmine dayalı analitikler ve hızlı yanıt yetenekleri aracılığıyla dayanıklılığı artırabilir. Yerli ve millî çözümlerle stratejik ürünlerin belirlenmesi ve geliştirilmesi, özgüveni artırıp dışa bağımlılığı azaltarak dayanıklılığı artırmaktadır. Dijital okuryazarlığı teşvik etmek ve IoT cihazlarıyla ilişkili riskler hakkında farkındalığı artırmak, bireylerin ve kuruluşların güvenli uygulamaları benimsemesini ve siber tehditleri etkili bir şekilde azaltmasını sağlamak için çok önemlidir. Hükümetler, kuruluşlar ve topluluklar bu sorunları kapsamlı bir şekilde ele alarak kritik altyapılardaki dayanıklılığı güçlendirebilir ve siber tehditlerden ve aksaklıklardan kaynaklanan riskleri azaltabilir.

Ek 4-16/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

3. Veri Egemenliği Politikaları ve Kriptoloji

3.1. Tespitler

Türkiye dâhil birçok ülkede, verilerin giderek daha değerli bir varlık hâline geldiği ve veriler üzerinde kontrol sahibi olmanın ulusal güvenlik, ekonomik rekabet gücü ve mahremiyetin korunması gibi çeşitli nedenlerle hayati önem taşıdığı kabul edilmektedir. Özel bir ulusal veri tabanının yokluğunda, diğer kurumların çeşitli konulara ilişkin verileri toplayıp yönetebilmesi anlaşılabilir bir durumdur. Ancak Türkiye'nin verilerinin yönetilmesinde daha aktif bir rol oynaması ve veri depolama ve işleme konusunda dış platformlara veya hizmetlere aşırı bağımlı olmamasının sağlanmasına ihtiyaç vardır.

Esneklik ve uyarlanabilirlik, dijital çağın karmaşıklıklarıyla baş etmede gerçekten çok önemlidir. Veri kullanımına ve depolamaya katı sınırlar koymak her zaman mümkün veya pratik olmasa da ülkeler, veri egemenliği ve güvenliğine ilişkin endişelerle yenilik ve iş birliği ihtiyacını dengeleyen veri yönetimi konusunda esnek yaklaşımlar benimseyebilir. Ülkeler, veri depolama ve işleme için kendi altyapılarını ve platformlarını kurarak, verileri üzerinde daha fazla kontrol sahibi olabilir ve dış sağlayıcılara olan bağımlılığı azaltabilir. Ancak ticari ortakların ve küresel şirketlerin dijital ekosistemdeki rolünün bilincinde olmak da önemlidir. Bu kuruluşlarla iş birliği teknolojik yenilik, pazarlara erişim ve ekonomik büyüme açısından önemli faydalar sağlayabilir. Veriler üzerinde ulusal egemenliğin savunulması ile ticari ortaklarla iş birliğinin teşvik edilmesi arasında bir denge bulmak, dijital çağın karmaşıklıklarıyla etkili bir şekilde baş etmenin anahtarıdır. Bu, veri yerelleştirmesini teşvik eden ve aynı zamanda güvenilir ticari kuruluşlarla iş birliğini ve ortaklığı teşvik eden politikalar ve düzenlemeler geliştirmeyi içerebilir.

Türkiye'nin veri altyapısı ve süreçleri üzerinde kontrol sahibi olması, verilerin vatandaşlarının ve milletin bütünlüğünü, güvenliğini ve refahını ön planda tutacak şekilde toplanmasını, saklanmasını, işlenmesini ve kullanılmasını sağlama ihtiyacının altını çizmektedir.

Veri egemenliği, dijital çağda ulusal egemenliğin temelidir ve ülkelere kritik bilgi varlıklarını koruma, güvenlik açıklarına karşı koruma sağlama ve ulusal güvenliğe yönelik riskleri azaltma yetkisi verir. Yalnızca veriler üzerinde kontrol sahibi olmayı değil, aynı zamanda verileri



Ek-4 Tespit ve Öneriler

etkili ve güvenli bir şekilde yönetmek için sağlam politikalar, altyapı ve yetenekler geliştirmeyi de içerir.

Verinin giderek stratejik bir varlık olarak kabul edildiği günümüzün birbirine bağlı dünyasında, Türk vatandaşlarının verilerinin korunması ve siber ortamın güvenliğinin sağlanması büyük önem taşımaktadır. Bu, veri egemenliği ilkelerini destekleyen ve Türkiye'nin dijital ortamda dirençli ve rekabetçi kalmasını sağlayan politikalar, düzenlemeler ve altyapının geliştirilmesine yönelik proaktif önlemler gerektirir.

Ayrıca veri egemenliği, veriler üzerindeki salt kontrolün ötesine geçer; harici bağımlılıklara veya yabancı varlıklara bağlı kalmadan verileri bağımsız olarak yönetme yeteneğini kapsar. Bu özgüven, Türkiye'nin gelecekteki varlığını koruması ve jeopolitik zorluklar ve gelişen dijital tehditler karşısında egemenliğini sürdürmesi açısından hayati önem taşımaktadır.

Yerileştirme ve yerelleştirme birbiriyle ilişkili kavramlardır ancak incelikli farklılıkları vardır. Her ikisi de yerel ürünlere ve çözümlere öncelik vermeyi içerse de yerli yeteneklerin teşvik edilmesi ve yabancı ithalata bağımlılığın azaltılmasının farklı yönlerine odaklanmaktadır.

Yerileştirme: Bu, daha önce ithal edilen veya dışarıdan temin edilen mal veya hizmetleri üretmek için yerli yeteneklerin geliştirilmesi sürecini ifade eder. Yurt içinde ürün üretmek veya hizmet sunmak için yerel uzmanlık, altyapı ve tedarik zincirleri oluşturmayı içerir. Yerileştirme genellikle ulusal güvenlik veya ekonomik kalkınma açısından stratejik açıdan önemli olan kritik sektörleri veya teknolojileri hedef alır.

Yerelleştirme: Yerelleştirme ise ürünlerin, hizmetlerin veya içeriğin belirli bir yerel pazarın tercihlerine, diline, kültürüne veya düzenleyici gereksinimlerine uyacak şekilde uyarlanmasını içerir. Yazılım arayüzlerinin çevrilmesini, ürün özelliklerinin yerel normlarla uyumlu olacak şekilde ayarlanmasını veya yerel düzenlemelere ve standartlara uymayı içerebilir.

Türkiye bağlamında yerelleşme vurgusunun, hem Pardus gibi yerli işletim sistemlerinin geliştirilmesi ve benimsenmesi gibi yerileştirme çabalarını hem de ithal teknolojilerin yerel ihtiyaç ve tercihlere göre uyarlanmasını içerdiği görülmektedir. Amaç, yabancı ürün ve hizmetlere bağımlılığı azaltmak, aynı zamanda yerli sanayilerin büyümesini ve rekabet gücünü teşvik etmektir.

Ek 4-18/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.



Ek-4 Tespit ve Öneriler

Pardus'un kamu sektöründe benimsenmesi ve TÜBİTAK gibi kuruluşlar tarafından özgün çözümlerin geliştirilmesi gibi Türkiye'de yerleşmeyi teşvik etme çabaları, yerli yeteneklerin geliştirilmesi ve kaynak çeşitliliğinin sağlanmasına yönelik kararlılığı yansıtmaktadır. Ancak bahsettiğiniz gibi bu hedeflerin tam olarak hayata geçirilmesinde yerli ürünlerin bulut uyumluluğuna uyarlanması, sürekli destek ve geliştirmenin sağlanması gibi zorluklar olabilir.

Önümüzdeki dönemde Türkiye'nin yerlileştirme ve yerleştirme çalışmalarına yatırım yapmaya devam etmesi kadar, veriyi değere dönüştürmeye de odaklanması gerekecektir. Bu, eyleme geçirilebilir içgörüler elde etmek, inovasyonu teşvik etmek ve veri varlıklarından ekonomik değer yaratmak için veri analitiğinden, yapay zekâdan (YZ) ve diğer teknolojilerden yararlanmayı içerebilir. Türkiye, politikaları somut eylemlerle uyumlu hâle getirerek ve veriye dayalı teknolojilerin potansiyelinden yararlanarak küresel dijital ekonomideki rekabet gücünü ve dayanıklılığını daha da artırabilir.

Türkiye'de veri işlemeyi ve analizini destekleyen politikalara ve altyapıya duyulan ihtiyacı vurgulayarak, yalnızca verileri yerleştirmenin değil, aynı zamanda verilerden değer çıkarmanın da hayati önemini vurgulamak gerekir. Bu konudaki önemli noktalar şunlardır:

- Veriden değer çıkarımı: Verinin yerleştirilmesi egemenlik ve güvenlik gibi nedenlerden dolayı önemli olsa da öncelikli amaç veriden değer elde etmek olmalıdır. Bu, içgörü elde etmek, bilinçli kararlar vermek ve yeniliği teşvik etmek için ileri teknolojilerin ve analitik tekniklerin kullanılmasını içerir.
- Veri işlemedeki zorluklar: Verilerin Türkiye'de tutulmasına yönelik çaba gösterilse de büyük veri kümelerinin işlenmesi ve analiz edilmesine yönelik altyapı ve yetenek eksikliği bulunmaktadır. Bu, toplu olarak veri bilimi olarak bilinen bulut bilişim, büyük veri analitiği, makine öğrenimi ve YZ gibi teknolojilere yatırım ihtiyacını vurgulamaktadır.
- Hükümet politikalarının rolü: Ulaştırma Bakanlığı ve buna bağlı olarak hükümet, veri bilimi teknolojilerinin geliştirilmesine ve benimsenmesine öncelik veren politikaların şekillendirilmesinde önemli bir rol oynamaktadır. Bu politikalar, şirketlerin büyük veri analitiğini denemeleri ve değer yaratmak için verilerden yararlanmaları için uygun bir ortam yaratmalıdır.

Ek 4-19/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

Ek-4 Tespit ve Öneriler

- Deney ve yenilik ihtiyacı: Büyük veri analitiğini denemek için geniş alanlara ihtiyaç vardır, bu da veri biliminde yeniliği desteklemek için özel tesislere ve kaynaklara duyulan ihtiyacı ima eder. Bu çabalar, ekonomik büyümeyi ve rekabetçiliği teşvik eden bir deneme ve yenilik kültürünü teşvik edebilir.

Özetle, odak noktasını yalnızca verileri yerelleştirmekten değer yaratmak için aktif olarak kullanmaya kaydırmanın önemini vurgulamalıyız. Bu, altyapıya yatırım yapmak, veri bilimi teknolojilerine öncelik veren politikalar geliştirmek ve deney ve yenilik için elverişli bir ortamı teşvik etmek için ortak çabalar gerektirir. Bunu yaparak Türkiye, veri varlıklarının tüm potansiyelini kullanabilir ve dijital çağda sürdürülebilir ekonomik kalkınmayı teşvik edebilir.

Veri yerelleştirmesi gerçekten de ülkeler için giderek daha önemli hâle gelmektedir. Verilerin ulusal sınırlar içinde kalmasını sağlayarak ülkeler, verilerin kullanımı ve korunması üzerinde daha fazla kontrol sahibi olabilir. Yerelleştirilmiş veriler üzerinde veri analitiği ve YZ teknolojilerinin kullanılması hem ülke hem de bireysel paydaşlar için ek değerın kilidini açabilir. Ancak verilerin ilgili teknolojilerde kullanılmasından önce anonimleştirme süreçlerine öncelik verilmesi büyük önem taşır. Bu, gizliliğin korunmasına yardımcı olur ve veri koruma düzenlemelerine uygunluğu sağlarken veri analitiğinin ve YZ sunabileceği öngörülerden ve avantajlardan yararlanmaya devam eder.

Güçlü bulut bilgi işlem hiper ölçekli altyapılarının oluşturulması, YZ ve büyük veri analitiğinin geliştirilmesi için çok önemlidir. Böyle bir altyapı olmadan YZ gelişimi durağan kalır. Özellikle eğitim ve sağlık gibi kamu sektörlerinde büyük ölçekli veri merkezlerinin oluşturulmasına öncelik verilmelidir. Ayrıca bu teknolojilerin gelişmesi için bulut bilişimin yaygın biçimde benimsenmesi gerekir. Evrensel mutabakata ve insan haklarına dayanan tekelleşme ve suiistimal düzenlemeleri bu ekosistemi olumlu yönde etkileyebilir. Ulusal yapay zekânın eğitimi, büyük verileri etkili bir şekilde yönetebilecek bulut bilişim altyapısının geliştirilmesine dayanır. Veri yerelleştirmesi, ülke içindeki teknolojilerin işlenmesini ve geliştirilmesini hızlandırarak büyük veri analitiği ve YZ sistemlerinde hızlı büyümeyi teşvik eder. Anonimleştirme teknikleri, gizliliği ve güvenliği korumak için bu teknolojilerde veri kullanımından önce gelmelidir. Sonuçta, bu alanlardaki akademik gelişimin teşvik edilmesi, ülkenin teknolojik ilerlemesi için çok önemlidir.

Ek 4-20/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.



Ek-4 Tespit ve Öneriler

Türkiye, veri egemenliğine öncelik vererek ve gerekli kaynak ve yeteneklere yatırım yaparak kendisini dijital çağda lider olarak konumlandırabilir ve gelecek nesiller için vatandaşlarının güvenliğini ve refahını sağlayabilir.

Dışa bağımlılığı azaltmak ve dayanıklılığı artırmak için yerli ve millî üretimin teşvik edilmesine güçlü bir vurgu yapılmaktadır. Yerlileştirme politikaları, özellikle teknoloji ve veri depolama gibi kritik sektörlerde yerli ürün ve çözümlere öncelik vermeyi amaçlamaktadır.

Şifreleme ve Kriptoloji Teknolojisinin Veri Güvenliği ve Mahremiyeti Üzerindeki Etkisi

Nvidia gibi şirketler, veri güvenliği de dâhil olmak üzere çeşitli endüstriler için önemli etkileri olan hızlı donanım teknolojilerinin geliştirilmesinde öncülük etmektedir. Bu gelişmeler veri koruma ve şifrelemede yeni yaklaşımlara olanak sağlar. Kuantum hesaplama, hesaplama gücü ve yeteneklerinde bir paradigma değişimini temsil eder. Karmaşık sorunları çözmek ve teknolojik yenilikleri hızlandırmak için muazzam bir potansiyel sunarken, aynı zamanda veri güvenliği açısından yeni zorluklar da ortaya çıkarmaktadır.

Ancak Türkiye'de kuantum hesaplama araştırma ve geliştirme alanında kayda değer bir uzmanlık ve yatırım eksikliği mevcut ve bu durum ülkeyi bu kritik alanda geride bırakmaktadır. Donanım teknolojileri geliştikçe veri güvenliğinin önemi giderek daha kritik hâle gelmektedir. Askerî ve ticari veriler de dâhil olmak üzere hassas bilgilerin korunması artık yalnızca hükümetlerin değil aynı zamanda işletmelerin ve bireylerin de ilgi alanıdır. Kuantum bilişimin geleneksel şifreleme yöntemlerini geçersiz kılma potansiyeli var ve bu da veri korumasına yönelik yeni yaklaşımlara yatırım yapmanın aciliyetini ortaya koymaktadır.

Veri güvenliği sorunlarını etkili bir şekilde ele almak için kuantum hesaplama gibi yeni ortaya çıkan teknolojilere yönelik daha fazla farkındalığa ve yatırıma ihtiyaç olduğu kabul edilmektedir. Amerika Birleşik Devletleri gibi ülkeler kuantum araştırmasının stratejik öneminin farkına varmış ve kaynaklarını buna göre tahsis etmiştir. Ancak Türkiye'nin bu alanda hem farkındalık hem de yatırım açısından eksik olduğu algısı, bunun ulusal güvenlik ve ekonomik rekabet gücü üzerinde önemli etkileri olabilir.

Ek 4-21/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

3. 2. Öneriler

Türkiye'nin dijital gelişiminde yerelleştirme politikaları, veri depolamanın ve sürdürülebilir uluslararası iş birliği için önemli bir başlıktır.

- Yerelleşme vurgusu: Dışa bağımlılığı azaltmak ve dayanıklılığı artırmak için yerli ve milli üretimin teşvik edilmesine güçlü bir vurgu gerekir.

- Kapsamlı politikalara duyulan ihtiyaç: Yerelleştirme çabalarında ilerleme kaydedilirken, çeşitli sektörlerde daha bütünsel ve sistematik politikalara yönelik çağrılar gereklidir. Dağınık ve bireysel çabalar toplam sistematik gelişmeyi sağlamak için yeterli olmayabilecektir.

- Veri saklamanın önemi: Veri saklama politikalarının, özellikle KVKK gibi düzenlemeler kapsamındaki kritik verilere ilişkin politikaların kapsamlı ve koruyucu olduğu düşünülmektedir. Ancak şifreleme, erişim hakları, saklanan verilerin şeffaflığı gibi alanlarda iyileştirmelere ihtiyaç vardır.

- Kamu-özel sektör iş birliğinin geliştirilmesi: Yerelleştirme çabalarını ilerletmek için kamu ve özel kuruluşlar arasında daha güçlü iş birliğine ihtiyaç olduğu kabul edilmektedir. Yurt içi yeteneklerin daha da güçlendirilmesi için kamu-özel sektör ortaklıkları ortak hedefler doğrultusunda çalışmalıdır.

- Farkındalık ve şeffaflık: Kamuoyunda veri saklama politikaları hakkında farkındalığın artırılması ve politika uygulamasında şeffaflığın artırılması yönünde bir gereksinim bulunmaktadır. Vatandaşların mahremiyet konusunda kaygıları vardır.

- İlerlemenin değerlendirilmesi: Türkiye'nin yerelleştirme politikaları ve veri depolama konusunda son on yılda kaydettiği ilerlemeye ilişkin olumlu bir değerlendirme mevcut olup, tahminler yerelleştirme oranlarında önemli artışlara işaret etmektedir. Ancak yerelleştirme ve veri egemenliğinin faydalarını tam olarak hayata geçirmek için daha fazla çabaya ihtiyaç duyulmaktadır.

Bu bilgiler, Türkiye'nin dijital altyapısını güçlendirmeye ve sürdürülebilir ekonomik kalkınmayı desteklemeye yönelik devam eden çabalara bilgi sağlayabilir. Veri güvenliği ve



Ek-4 Tespit ve Öneriler

gizliliğinin sağlanmasında şifreleme ve kriptoloji tekniklerinin kullanımı devletin farklı kurumlarında ihtiyaçtır.

Anahtar üretimi, dağıtımı ve dijital kullanım da dâhil olmak üzere şifreleme ve kriptolojinin temel yönlerini koordine etmek ve uygulamak için özel bir birimin veya ulusal otoritenin kurulması çağrısı vardır. Bu birimin ekosistemi geliştirmek ve dijital ekonominin güvenliğini sağlamak için bir yol haritası geliştirmesi gerekmektedir. Türkiye'nin şifreleme ve kriptoloji teknolojilerindeki mevcut bilgi ve kapasitesinin, özellikle kuantum hesaplama ve kuantum sonrası şifreleme gibi alanlarda yetersiz olduğu kabul edilmektedir. Buna insan kaynakları, altyapı, fikri mülkiyet, programlama ve yetenek birikimindeki eksiklikler de dâhildir.

Devlet verilerinin güvenliğinin ve gizliliğinin sağlanması, bilgi çağında hayati önem taşır. Gelişen tehditlere etkin bir şekilde müdahale edebilmeleri için bu alanda faaliyet gösteren yerli ve millî firmaların desteklenmesi ve yetkinliklerinin artırılması gerekmektedir. Ortaya çıkan güvenlik sorunlarını kapsamlı bir şekilde ele almak için kuantum hesaplama ve kriptoloji gibi alanlardaki araştırma ve geliştirme faaliyetlerine öncelik verilmesine ihtiyaç vardır. Bu, yetkinliğin artırılmasını, teşvik mekanizmalarının uygulanmasını ve denetim mekanizmalarının geliştirilmesini içermektedir.

Şifreleme ve kriptoloji teknolojileri, veri güvenliği ve gizliliği açısından vazgeçilmez kabul edilmektedir. Bu alandaki gelişmelerin desteklenmesi ve Türkiye'nin küresel rekabette rekabetçi kalmasının sağlanması büyük önem taşımaktadır. Askerî sistemlerde belirli ilerlemeler sağlanırken, şifreleme ve kriptoloji teknolojilerinin sivil uygulamalarda eksiklikleri bulunmaktadır. Bu açığı kapatmak ve her iki sektördeki yetenekleri güçlendirmek için çaba gösterilmelidir.

Sürekli gelişen dijital ortamda, yeniliği teşvik ederken veri egemenliğini ve gizliliğini korumak her şeyden önemli olmaya devam etmektedir. Dinamik veri sınıflandırması, sağlam açıklama politikaları ve sınır ötesi veri aktarımına ilişkin sıkı kontroller çok önemlidir. Merkezi bir veri kontrol merkezinin kurulması ve yazılımın yerleştirilmesine öncelik verilmesi, Türkiye'nin dijital özerkliğini koruma konusundaki kararlılığının altını çizmektedir.

Ekonomik ve politik gücün devamını sağlamak için ülkeler diğer ülkelerle stratejik ortaklıklara ve iş birliği çabalarına girişmelidir. Sınırların net olarak belirlendiği ve açıkça ilan

Ek 4-23/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.



Ek-4 Tespit ve Öneriler

edildiği bir stratejik iletişim kavramının oluşturulması hayati önem taşımaktadır. Bu, uluslararası platformda güç kullanımı ve siber suçlama gibi konulara ilişkin her ülkenin sorumluluklarının, yükümlülüklerinin ve politikalarının ana hatlarını çizmeyi içerir. Ülkeler, bu tür sınırları belirleyip uygulayarak, bu sınırları aşmaya yönelik her türlü girişimi etkili bir şekilde caydırabilir, böylece egemenliklerini koruyabilir ve küresel arenada istikrarı teşvik edebilir. Ülkeler, geleneksel pazar konumlandırma stratejilerine benzer şekilde kendilerini dijital alanda stratejik olarak konumlandırmalıdır. Bu, siber uzayı düzenleyen uluslararası yasalarla uyumlu politikaların geliştirilmesi ve uygulanması için stratejik siyasi iş birliğinin geliştirilmesini ve stratejik iletişimin teşvik edilmesini gerektirir. Siyasi ve ticari alanda etkili ülkeler gibi, gelişmiş veri işleme ve barındırma teknolojilerine sahip olanlar da hâkimiyet kuracaktır. Ulusal devletler hâkim şirketleri dikkatle izlemeli, tekelleşmeyi önlemeli ve alternatif çözümleri teşvik etmelidir.

Stratejik iletişim, veri egemenliği politikalarının ayrılmaz bir parçasıdır ve uluslararası hukukun siber alana uygulanabilirliğini vurgulamaktadır. Veri egemenliğine ulaşmak, diğer ülkelerle iş birliği ve iletişimin önemini vurgulayan uluslararası kabul gerektirir. Uluslararası düzenlemelerin oluşturulması bu alandaki ilerlemeyi hızlandırabilir ve farklı ülkelerin veri egemenliği politikaları arasında ortaya çıkabilecek çatışmaları giderebilir. Genel olarak, veri egemenliğini geniş çapta benimsemek ve standardizasyona yönelik küresel çabalara katılmak, ülkelerin uluslararası siber güvenlikteki güçlerini ortaya koymaları için hayati önem taşır.

Ek 4-24/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

4. Toplumsal Dijital Dayanıklılığın Sağlanması

4.1. Tespitler

Türkiye'nin toplumsal dijital dayanıklılığı, farklı faktörlerin etkisi altında şekillenmektedir. Günümüzde, vatandaşların psikolojik direnci ve toplumsal yardımlaşma gibi 'yumuşak' sosyal boyutlar, dijital dayanıklılığın belirleyici unsurları arasında yer almaktadır. Ancak, sosyal medyanın yoğun ve bilinçsiz kullanımı, bu dayanıklılığı olumsuz yönde etkilemektedir.

Ekrana maruz kalma süreleri çok yüksektir ve kişisel dijital bağımlılık maalesef yaygınlaşmaktadır. dünyada olduğu gibi Türkiye'de de İnternet ve medya uygulamalarının etkisiyle toplumun belirli alanlara yönlendirilebilmesi ve manipüle edilmesi kolaylaşmaktadır. Bu durum, toplumun dezenformasyona karşı hassas bir noktada olduğunu göstermektedir. Ayrıca, dijital okuryazarlık düzeyinin düşük olması, dezenformasyonla mücadelede önemli bir zorluk olarak karşımıza çıkmaktadır.

Ülkemizde, dijital dayanıklılığı olumsuz etkileyen bir diğer faktör ise farkındalık eksikliğidir. Özellikle eğitimsiz ve 50 yaş üstü bireyler arasında dijital güvenlik konusunda yeterli bilinç düzeyinin sağlanamaması, toplumsal dayanıklılığın zayıf olduğunun bir göstergesidir. Bu durum, psikoloji, tarih, sosyoloji, felsefe gibi değişik boyutlarıyla bütüncül olarak tartışılmamaktadır.

Diğer yandan, Türkiye'nin, dijital dayanıklılığını artırabilmesi için potansiyeli yüksektir. Özellikle toplumsal dayanışmanın güçlü olduğu kriz dönemlerinde gösterilen tepkiler, bu potansiyeli ortaya koymaktadır. Bununla birlikte, dijital okuryazarlık ve farkındalık düzeyinin artırılması için medya kuruluşlarının daha sorumlu içerik üretmesi ve eğitim faaliyetlerinin yaygınlaştırılması gerekmektedir.

Özetlemek gerekirse, teknolojiye erişim açısından bakıldığında Türkiye'nin durumu normal düzeylerde olmakla birlikte sabit geniş bant İnternete erişim ve kullanım ile cihaz sahipliği açısından gelişebilir alanlar olduğu anlaşılmaktadır. Vatandaşlarımızın fazlasıyla zaman geçirdiği ve iç içe bulunduğu İnternet teknolojileriyle ilgili bilgi ve beceri seviyelerinin artırılmasına dönük bir kamuoyu farkındalığı mevcuttur.



Ek-4 Tespit ve Öneriler

Bu maksatla devlet, özel sektör ve sivil toplum kuruluşları tarafından çok sayıda önemli girişim başlatılmış ve devam etmektedir. Bu girişimlerin sayı ve kalite olarak artırılması suretiyle toplumun dijital dayanıklılığına katkı sunulması için yapılması gerekenler sonraki bölümlerde ele alınmıştır.

4.2. Öneriler

Toplumsal siber dayanıklılığı güçlendirmek için dijital okuryazarlık, bu konuda bir temel oluşturması yönüyle oldukça önemlidir. Bu kapsamda öncelikle, farklı yaş gruplarına yönelik özelleştirilmiş eğitim ve bilinçlendirme programlarına odaklanmak kritiktir. Bu programlar, çocuklar için okul öncesi ve okul dönemi eğitimlerinden, yetişkinler için yaşam boyu öğrenme programlarına kadar geniş bir yelpazede olmalıdır. Ulusal medya kanallarının bu tür içerikler üretmesi ve yayınlaması, e-devlet, çevrimiçi sipariş ve alışveriş sayfaları ile diğer dijital platformlar aracılığıyla bilgilendirme sağlanması önemlidir.

Ebeveynleri de ayrıca bu sürece dâhil etmek gerekmektedir. Onlara yönelik eğitimler düzenlenmeli ve dijital dünyanın güvenli kullanımı konusunda bilinçlendirilmelidir. Ayrıca, dijital reklamlar, kamu spotları ve diğer iletişim araçları üzerinden sürekli olarak dijital okuryazarlığı artırıcı ve güvenlikle ilgili mesajlar verilmelidir. Bu çabalar, toplumun her kesiminde dijital farkındalığın artmasına yardımcı olabilir.

Toplumsal dijital dayanıklılık konusunda regülasyonların oluşturulması da önemlidir. İnternet ve diğer dijital ortamlarda güvenliği sağlamak için hukuksal düzenlemeler yapılmalı ve bu düzenlemelere uyulması sağlanmalıdır. Ayrıca, televizyon kanallarının içeriklerinin denetlenmesi ve daha nitelikli içeriklerin teşvik edilmesi gerekmektedir.

Eğitim merkezlerinde dijital okuryazarlık ve farkındalık konularının daha fazla vurgulanması ve örnek senaryolarla desteklenmesi önemlidir. Bu sayede, bireylerin dijital dünyada daha güvenli ve bilinçli bir şekilde hareket etmeleri sağlanabilir.

Psikolojik ve sosyolojik çalışmalar yapılarak toplumun mevcut dijital dayanıklılığının ortaya konulması, bilahare eksiklerin kapsamlı bir program dâhilinde tamamlanması ve vatandaşın dijital dayanıklılığı konusunda farkındalık çalışmalarının artırılması ihtiyacı bulunmaktadır.

Ek 4-26/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.



Ek-4 Tespit ve Öneriler

Dijital okuryazarlık konusunda toplumun her kesimi için ayrı ayrı çalışmalar yapılması gerekmektedir. Bu değişik şekillerde örneğin, kamu spotu, en çok kullanılan sosyal medya ya da İnternet girişinde farkındalık eğitimi, göze çarpan alanlarda bilgilendirmeler vb. yapılarak gerçekleştirilebilir.

Ekran kullanım süresinin artmasıyla birlikte dezenformasyona maruz kalma riski de artmaktadır. Bu nedenle, bilinçli olmanın yanı sıra ekran süresinin azaltılması da önemlidir. Bu amaçla, sosyologlar, psikologlar ve farklı uzmanlık alanlarından kişilerin dâhil olduğu projeler geliştirilmelidir. Bu projeler, bireylerin dezenformasyona karşı araştırma yapma alışkanlığını geliştirmelerini sağlayarak, onların bilinçlenmelerini ve sorgulamalarını teşvik etmelidir.

Yetkililer tarafından yapılan açıklamalara güven duygusunun artırılması da önemlidir. Bu güven duygusu, doğru, şeffaf ve detaylı açıklamaların zamanında yapılmasıyla sağlanabilir. Ayrıca, eğitim aracılığıyla güvenilir bilgi kaynaklarına erişimin önemi vurgulanmalı ve toplumsal bilinç oluşturulmalıdır. İnsanlara dezenformasyona karşı araştırma yapma alışkanlığının kazandırılması, uzun vadeli bir yatırım olarak görülmelidir.

Uygulamalı tatbikatların yapılması ve servis sağlayıcılarına dezenformasyonla mücadele konusunda zorunluluklar getirilmesi de etkili olabilir. Ayrıca, yaşanan olayların medya aracılığıyla doğru bir şekilde aktarılması ve eğitim müfredatına dijital okuryazarlık derslerinin eklenmesi, toplumun dezenformasyona karşı daha dirençli hâle gelmesine katkı sağlayabilir. Özetle, dezenformasyona karşı dayanıklılığın artırılması, sürekli bilgilendirme, eğitim ve bilinçlendirme çalışmalarıyla mümkün olacaktır.

Dezenformasyon ve dolandırıcılık, dijital çağın en büyük tehlikelerinden biridir ve bireyleri etkileyebilecek potansiyel riskler barındırır. Bu nedenle, her bireyin, aldığı bilgileri sorgulama, kaynağını kontrol etme ve doğrulama becerilerini geliştirmesi ve bunu âdeta refleks hâline getirmesi (eleştirel düşünme) elzemdir.

Çocuklar ve gençler için dijital dayanıklılık ve güvenlik bilincini artırmanın birkaç yolu bulunmaktadır. Öncelikle, anaokulundan üniversiteye kadar olan eğitim sürecinde müfredatta farkındalık üzerine zorunlu derslerin olması ve bu derslerin etkinliğinin ölçülmesi önemlidir. Farklı

Ek 4-27/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.



Ek-4 Tespit ve Öneriler

disiplinlerdeki derslerde konuların veya soruların içeriğine dijital dayanıklılık ile ilgili farkındalık konularının dâhil edilerek öğrencilere aktarılması faydalı olabilir.

Okul öncesi ve okul döneminde, yaş gruplarına özel animasyonlar, eğitici videolar, çizgi filmler ve derslerde içeriğe gizlenmiş bilgilendirici materyaller kullanılarak çocuklara dijital dayanıklılık ve güvenlik bilinci aşılanabilir. Gençler için ise benzer yöntemlere ek olarak, siber zorbalık ve tehditler konusunda bilgilendirme yapılmalı ve bu konuların önemi vurgulanmalıdır.

Alışkanlık kazandırılması önemlidir. Bilinçli kullanım kadar ekran süresinin azaltılması da dikkate alınmalıdır. Ayrıca, okullarda siber tatbikatların uygulanması ve öğrencilere sunulması da faydalı olabilir. Bu tatbikatlar sayesinde öğrenciler, gerçek hayatta karşılaşılabilecekleri dijital tehlikeler konusunda fikren daha hazırlıklı olurlar.

Ailelerin bu süreçte önemli bir rolü bulunmaktadır. Aile bireylerine, bilinçli bir birey nasıl yetiştirilir konusunda eğitimler verilerek, çocukların dijital dayanıklılık ve güvenlik bilinciyle donatılması sağlanabilir. Ayrıca, sosyal medyada ve okullarda düzenlenen farkındalık eğitimleri ve yarışmalarıyla da bu bilincin artırılması desteklenebilir.

Dijital eğitimin anaokulundan başlayarak verilmesi, buna karşın belli bir yaşa kadar çocukların dijital maruz kalma sürelerinin kısıtlanması gerektiği unutulmamalıdır. Bu şekilde, çocuklar ve gençler dijital dünyayı daha bilinçli ve güvenli bir şekilde kullanabilirler.

Özel sektör, sivil toplum kuruluşları ve hükümet arasında iş birliği, dijital dayanıklılığı artırmak için kritik bir öneme sahiptir. Bu iş birliği, çeşitli düzeylerde ve farklı alanlarda gerçekleşmelidir. Öncelikle, devletin liderlik rolü üstlenmesi önemlidir. Dijital dayanıklılığı artırmak için devlet tarafından ulusal stratejiler belirlenmeli ve bu stratejilerin uygulanması sağlanmalıdır. Bu stratejilerin belirlenmesinde ve uygulanmasında, özel sektör ve sivil toplum kuruluşlarının görüşleri ve katkıları gerekir. Çalıştaylar ve danışma toplantıları, paydaşların bir araya gelerek ortak stratejiler geliştirmesine olanak tanır.

Özel sektörün rolü de bu alanda oldukça önemlidir. Özel sektör, dijital dayanıklılığı artırmak için Ar-Ge faaliyetlerini yürüterek yenilikçi çözümler geliştirebilir. Hükümetin teşvik ve destekleri ile, özel sektör bu alanda daha fazla yatırım yapabilir ve ürün geliştirme süreçlerini hızlandırabilir.

Ek 4-28/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.



Ek-4 Tespit ve Öneriler

Sivil toplum kuruluşları ise toplumun farkındalığını artırmak ve eğitim faaliyetleri düzenlemek gibi önemli bir role sahiptir. Bu kuruluşlar, hükümetin belirlediği stratejilerin topluma ulaştırılmasında ve uygulanmasında aktif rol alabilirler. Ayrıca, hükümetin ve özel sektörün politika ve uygulamalarını izleyerek, toplumsal geri bildirimleri iletebilir ve bu süreçlere katkı sağlayabilirler.

Bu iş birliği modeli, dijital dayanıklılığın hem stratejik hem de operasyonel düzeyde güçlendirilmesine olanak sağlar. Özellikle, kamu-özel iş birliği projeleri ve sivil toplum kuruluşlarının katılımıyla, daha kapsamlı ve etkili çözümler geliştirilebilir. Bu sayede, dijital tehditlere karşı daha güçlü ve dayanıklı bir toplum oluşturulabilir.

Toplumsal dijital dayanıklılığın artırılmasında sosyal medya platformlarının da oynayabileceği önemli bir rolü vardır. Bu platformlar, kullanıcıların büyük bir kısmının günlük olarak vakit geçirdiği ve bilgiye eriştiği alanlar olduğu için, doğru şekilde kullanıldığında büyük bir potansiyele sahiptirler. Ancak, bazı önlemler alınmadığı takdirde dezavantajlı durumlara da yol açabilirler.

Öncelikle, sosyal medya platformları kullanıcılarına dijital okuryazarlık konusunda eğitim ve bilgilendirme sağlayabilirler. Bu, kullanıcıların yanlış bilgi ve manipülatif içerikleri daha kolay tanıyabilmesini ve doğrulanmış kaynaklara yönlendirilmesini sağlayabilir. Kullanıcılarına güvenilir bilgi kaynaklarını tanıtmak ve dezenformasyonun nasıl yayıldığını anlatmak, toplumsal dijital dayanıklılığı geliştirebilir.

Sosyal medya platformları algoritmalarını, kullanıcıların maruz kaldığı zararlı içerikleri azaltacak şekilde düzenleyebilirler. Örneğin, sahte haberlerin ve kışkırtıcı içeriklerin yayılmasını önlemek için daha etkili filtreleme ve doğrulama sistemleri geliştirebilirler. Bu, kullanıcıların daha güvenilir ve doğru bilgilere erişmesini sağlayabilir.

Sosyal medya platformları kullanıcılarına dijital güvenlik konusunda da bilgilendirme yapabilirler. Özellikle çocuklar ve gençler için çevrimiçi güvenlik ve gizlilik konularında eğitim materyalleri sunarak, onların dijital tehlikelere karşı daha bilinçli olmalarını sağlayabilirler.

Bu platformlar, kullanıcılar arasında toplumsal dayanışma ve destek ağları oluşturabilirler. Özellikle siber zorbalığa maruz kalan kullanıcılara yardım ve destek sunarak, dijital ortamda daha

Ek 4-29/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.



Ek-4 Tespit ve Öneriler

güvenli bir ortamın oluşturulmasına katkıda bulunabilirler. Bu şekilde, sosyal medya platformları toplumsal dijital dayanıklılığı artırmak için önemli bir araç hâline gelebilirler.

Dijital eğitim ve farkındalık programları, toplumun dijital güvenlik bilincinin artırılmasında kritik öneme sahiptir. Bu programlar, bireylere dijital tehditlerle nasıl başa çıkacaklarını öğretmek ve bilinçli dijital alışkanlıklar geliştirmelerine yardımcı olmak için tasarlanabilir. Ancak, bu programların sürdürülebilirliği için belirli stratejilerin benimsenmesi gerekmektedir.

Öncelikle, dijital eğitim ve farkındalık programlarının belirli aralıklarla yenilenmesi ve güncellenmesi önemlidir. Teknolojideki hızlı değişim göz önüne alındığında, programların içeriği ve sunumu sürekli olarak güncellenmelidir. Bu, kullanıcıların en son tehditlere ve güvenlik önlemlerine uygun olarak bilgilendirilmesini sağlayacaktır.

Ayrıca, dijital güvenlik bilincini artırmak maksadıyla ulusal çapta düzenli sosyal mühendislik tatbikatları yapılabilir. Bu tatbikatlar yoluyla vatandaşlarda ilk tepkinin önemine dair gerçekçi bir kalıcı izlenim oluşması sağlanır. Kullanıcılar, gerçek zamanlı senaryolara dayalı simülasyonlar aracılığıyla dijital tehditlere nasıl tepki vereceklerini uygulamalı olarak öğrenebilirler. Bu tatbikatlar, bilgiyi pekiştirerek ve pratik becerilerin geliştirilmesine yardımcı olarak, sürdürülebilir dijital alışkanlıkların oluşmasını destekleyebilir. Kısacası, alışkanlıkların sürdürülebilir olması için sanal saldırılara maruz kalma deneyiminin süresi, sıklığı ve tekrarı ihtiyaç nispetinde artırılmalıdır.

Dijital güvenlik bilincinin sürdürülebilirliği için aynı zamanda kamu spotları, sosyal medya kampanyaları ve bilgilendirme materyalleri gibi iletişim araçlarından da yararlanılabilir. Bu araçlar, geniş kitlelere ulaşarak dijital güvenlik konusundaki farkındalığı artırabilir ve sürdürülebilir alışkanlıkların teşvik edilmesine katkı sağlayabilir.

Bilinç ve farkındalık için sürekli izleme ve ölçme yapılması önemlidir. Programların etkinliğinin düzenli olarak değerlendirilmesi ve iyileştirilmesi, sürdürülebilir dijital alışkanlıkların korunmasına yardımcı olabilir. Bu şekilde, dijital güvenlik bilinci toplumun her kesimine yayılarak daha güvenli bir dijital ortam oluşturulabilir.

Siber güvenlik farkındalığı ve eğitimi, toplumun her kesimine yayılmadığı takdirde büyük riskler oluşturabilir. Bu alandaki eksikliklerin giderilmesi ve bazı noktaların geliştirilmesi

Ek 4-30/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.



Ek-4 Tespit ve Öneriler

gerekmektedir. Bunlar; her düzeydeki yöneticinin siber güvenlik stratejilerine dair farkındalığının artırılması, toplumun bilgi varlıklarının kullanımı konusunda bilinçlenmesi, gençler ve çocuklar arasında erken yaşlardan itibaren siber güvenlik eğitiminin verilmesi olarak sıralanabilir.

Tatbikatlar ve uygulamalı eğitimler, bu farkındalığın sürdürülebilir olmasını sağlar. Trafik kurallarının öğretilmesinde olduğu gibi, siber güvenlik konularının da anaokulu ve ilkökul seviyesinden itibaren eğitim programlarına dâhil edilmesi önemlidir. Tüm kesimlerin bu farkındalığı benimsememesi, ulusal güvenlik için büyük bir tehdit oluşturabilir. Bu nedenle, eğitim, tatbikat, kamu spotları ve yarışmalar gibi aktivitelerle sürekli farkındalık çalışmaları yapılmalı ve tüm kurumlar aktif bir rol oynamalıdır.

Özel sektör, devlet ve sivil toplum kuruluşlarının bir araya gelerek siber güvenlik alanında eğitim ve farkındalık programları düzenlemesi gereklidir. Siber güvenlik eğitimi vermek üzere özel eğitim programlarına ihtiyaç vardır ve bu programlar, eğitmenlerin yetiştirilmesi için genişletilmelidir. Siber güvenlik, sadece kurumları ve şirketleri değil, bireyleri de etkiler. Bu nedenle, her seviyede ve günlük yaşamda siber güvenlik bilincinin desteklenmesi gereklidir.

Ek 4-31/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

5. Siber Olayların ve Siber Olaylara Müdahalenin Dönüşümü

5.1. Tespitler

Ülkemiz dijital bağıklık kapasitesini artırmaya yönelik önemli adımlar atmakta ve ciddi mesafe almaktaysa da yeni nesil teknolojilerin siber tehdit ortamına, saldırı türlerine ve siber olayların doğasına yönelik yaratacağı dönüşüme ilişkin hâlen eksiklikler ve yapılması gerekenler bulunmaktadır.

Bu bağlamda, Türkiye'nin siber alanda artan kurumsal kapasitesi, teknik donanımı ve uluslararası kuruluşlarla olan iş birliği (NATO, AGİT) avantajlı hususlar olarak ortaya çıkarken farkındalık yetersizliği, altyapı güvenliği ve ilgili alanda yetişmiş insan gücü kıtlığı ile teknoloji geliştirme yeteneğindeki sınırlılıklar olası zorluk alanları olarak görülmektedir.

Türkiye'de siber olaylara müdahale kapasitesi sektöre ve kurumların büyüklüğüne göre farklılık göstermektedir. Kurumsal firmalar ve devlet kurumlarında farkındalık ve hazırlık seviyesi yüksek iken görece küçük kuruluşlarda daha zayıf olabilmektedir.

Ülkemiz, insan, süreç ve teknoloji anlamında gerekli gelişimi sağlıyor olmakla birlikte yetişmiş insanları ülkede tutabilme konusunda maalesef yetersiz kalınmaktadır. Siber güvenlik alanlarında istihdam edilecek personel yetiştirmek üzere lisans düzeyinde yeterince eğitim verilmemekte ve bu alana yapılan yatırım kısıtlı kalmaktadır.

Diğer bir husus ise siber olaylara ve olaylardan alınan derslere dair SOME'ler arası bilgi ve tecrübe paylaşımı ile haberleşmenin yeterli seviyede olmamasıdır. Bunun sonucunda da koordinasyon eksikliği ve iş birliği kusurları yaşanmaktadır. Bu anlamda özel sektörün, özellikle küçük ve orta boy işletmelerin olay müdahale kapasitesi oldukça sınırlı durumdadır. Bu kapasitenin bilhassa özel sektörde geliştirme ihtiyacı bulunmaktadır.

Siber olaylara müdahale konusunda politika oluşturma, süreç tanımlama ve planlama yönleriyle belirli bir olgunluk seviyesinde bulunan ülkemizde, bütçe konuları ile kontrol, denetim ve geri besleme yoluyla sürekliliğin sağlanmasına ilişkin geliştirilmesi gereken alanlar bulunmaktadır.



Siber savunma ekiplerinin hedefleri; yetişmiş personelin kurumda tutulmasına yönelik etkin bir insan kaynağı politikası yürütmek, güncel gelişmelerin yakından takip edilip, mevcut altyapıların uyumlaştırılması çalışmalarının tamamlanması olarak sıralanmaktadır.

5. 2. Öneriler

Yetişmiş personelin daha iyi şartlarda çalışma isteğiyle sık sık kurum değiştirmesi, dahası ülkeyi terk ederek yurt dışına göç etmesi, insan kaynağı eksikliği yaratması yönüyle ciddi bir sorun alanıdır.

Nitelikli personeli elde tutmak için gerekli politikalar üretmek kadar, daha az personel ile işi devam ettirebilmenin yolları da aranabilir. Bunun için iş tanımlarının sadeleştirilmesi, görev birleştirmeleri, uzman havuzları oluşturulması ve özellikle kamuda uzaktan çalışmanın yaygınlaştırılması gibi alternatifler değerlendirilebilir. Her kurumun kendi siber operasyon merkezini (SOC) kurarak işletmesi gerekli olmayabilir, doğru kaynağı doğru yere yönlendirmek suretiyle süreç daha verimli işletilebilir.

Yeni nesil teknolojik gelişmelerin siber tehditler üzerindeki etkileri oldukça kapsamlıdır. Özellikle yapay zekâ, blokzincir, IoT cihazları ve kuantum gibi teknolojiler, siber tehditlerin ölçeğini ve karmaşıklığını artırmaktadır. Bu teknolojiler, siber saldırı sathını da genişletmekte ve yöntemleri çeşitlendirmektedir. Yapay zekâ destekli saldırıları daha karmaşık hâle getirirken, IoT cihaz sayısının artması daha yüksek hacimli saldırılara yol açabilmektedir. Kuantum teknolojileri ise siber olayların öngörülebilirliğini, şiddetini ve ölçeğini karmaşıklaştırmaktadır.

Bu teknolojilerin kullanımıyla ilgili potansiyel faydalar arasında ise daha hızlı ve doğru saldırı tespiti, 7/24 koruma, yüksek miktarda verinin hızlı işlenmesi, insan hatalarının azaltılması ve otomasyonun sağlanması gibi avantajlar sıralanabilir. Bu anlamda yapay zekâ kullanımının gelecekte önemli bir rol oynaması beklenmektedir. Potansiyel kullanım alanları, anomali tespiti ve kural bazlı uygulamaların yerini alabilir ve müdahale için bilgi ve belgelerin yaygınlaştırılmasını sağlayabilir.

Ancak, bu teknolojilerin kullanımıyla beraber ciddi sınamalar da ortaya çıkmaktadır. Özellikle yapay zekâ eğitiminde veri setlerinin zehirlenmesi, yapay zekâ destekli saldırıların karmaşıklığı, IoT cihazlarının tehdit oluşturması gibi riskler bulunmaktadır.

Ek 4-33/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

Ek-4 Tespit ve Öneriler

Bu nedenle, yeni nesil dijital teknolojilerin siber tehditler üzerindeki etkileri dikkatle incelenmeli ve bu teknolojilerin kullanımıyla ilgili potansiyel faydaların yanı sıra riskler de göz önünde bulundurularak gerekli güvenlik önlemleri alınmalıdır. Eğitim ile teknik bilgi ve becerilerle donatılmış nitelikli insan kaynağının yeni nesil siber olaylara müdahale etme ve dahası alanda operatif ve taktik etki bırakma konusunda fark yaratan bir kuvvet çarpanı olacağı hususu akıldan çıkarılmamalıdır.

Siber güvenlik ekiplerinin otomasyon ve yapay zekâyı kullanması, siber olaylara müdahale süreçlerini daha hızlı ve etkin hâle getirmekte ve kaynakların verimli kullanılmasını sağlamaktadır. Otomasyon, tekrarlayan görevler ve süreçteki insan hatalarını azaltırken, yapay zekâ ise daha karmaşık ve gelişmiş saldırıları tespit ve analiz konularında önemli rol oynamaktadır. Bu noktada dijital vatanın korunması ve dayanıklılığının sağlanması için siber olayların düzgün monitör edilmesi, ağda, sunucularda ve son kullanıcılarda meydana gelen tüm olayların görünürlüğünün sağlanması kritik önem taşımaktadır.

İki ucu keskin bir kılıç gibi olan söz konusu teknolojilerin ahlaki değerler çerçevesinde, dikkatli ve sorgulayıcı bir bakış açısıyla kullanılması gerekmektedir. Potansiyel faydaları ve riskleri göz önünde bulundurarak, siber güvenlik ekiplerinin bu teknolojilere yönelik sürekli olarak güncel kalacak şekilde eğitilmeleri önemlidir.

Siber güvenlik alanındaki gelişmeler, siber tehditlerin doğasını ve karmaşıklığını değiştirmekte ve bu durum, siber güvenlik ekiplerinin müdahale kapasitesini artırmak için yeni stratejilere ihtiyaç duymalarına neden olmaktadır. Sıklıkla ifade edildiği üzere gelişmekte olan yapay zekâ, blokzincir vb. teknolojilerle yeni saldırı yüzeyleri ve yöntemleri geliştirilmiştir. Bununla eş zamanlı olarak, insan kaynağının gelişimi ve dönüşümü ile süreçlerin bu gelişmelere ayak uyduracak şekilde dinamik uyumu sayesinde siber olaylara tespit ve müdahale de daha bütünleşik ve hızlı evrilmelidir. Bu evrimin yerli ve millî teknolojilerle yapılması ve dijital bağımsızlık hedefinde bir kaldıraç olarak kullanılması hedeflenmelidir.

Yeni ortaya çıkan ve gelişmekte olan teknolojilerle birlikte siber güvenlik konusundaki yükün önemli bir kısmı sıradan vatandaşın omuzlarına yüklenecektir. Örnek vermek gerekirse, gelineen noktada, yapay zekâ sayesinde çok daha gerçekçi ve ikna edici derin sahtecilik (deep fake) yoluyla dolandırıcılığın kolaylaştığı ve bu saldırı yönteminin yaygınlaşacağı söylenebilir.

Ek 4-34/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

Ek-4 Tespit ve Öneriler

Her bir sosyal medya platformunun, dijital iletişim için kullanılan her bir temas noktasının sosyal mühendislik saldırıları için birer laboratuvara ve hatta oyun alanına dönüşeceği açıktır. Böylesi bir tehditle etkin mücadelenin sadece SOME'ler tarafından olay müdahale merkezlerinde yapılabileceği iddiası iyimser bir yaklaşım olacaktır. Dolayısıyla sıradan kullanıcının bilgi güvenliği farkındalığının artırılarak teyakkuz hâlinin üst düzeye çıkarılması, şüphe kaslarının güçlendirilmesi ve mücadele için gerekli araç gerecin kendisine sağlanması önem arz etmektedir.

Bireyin veya toplumun zararlı bilgilere ve dezenformasyona karşı direnç gösterme yeteneği, eleştirel düşünme, bilgi güvenliği ve medya okuryazarlığı gibi becerilerin üzerine inşa edilir. Bu yetenekler, dijital dünyada karşılaşılan bilgi kirliliği ve manipülasyonla başa çıkmak için önemlidir. Yüksek dijital bağışıklık, insan bağışıklığında olduğu gibi, tehdit unsurlarıyla savaşma yeteneği ile öne çıkmaktadır. Yapay zekâ ve otomasyon, gelecekte bu bağışıklığın sağlanması için önemli unsurlar olacaktır. Bu teknolojiler, büyük veri analizi ve algılama sistemleri gibi araçlarla zararlı içeriği tanımlamak ve etkili bir şekilde mücadele etmek için kullanılabilir.

İnsan faktörü bu noktada kritik öneme sahiptir; çünkü bireylerin bilinçli bir şekilde bilgiye yaklaşması ve eleştirel düşünme becerilerini kullanarak bilgiyi değerlendirmesi, dijital dünyada güvenliğin sağlanmasında temel bir rol oynamaktadır. Bu nedenle, yapay zekâ ve otomasyon gibi teknolojiler, insanların bilgi güvenliği ve dezenformasyona karşı dirençli olmalarını desteklemek için yardımcı araçlar olarak da kullanılmalıdır.

Dijital bağışıklık, modern dünyanın karmaşık ve sürekli evrilen bir gerçeği hâline gelmiştir. Bu bağlamda, maruz kalınan etkenlerle etkin bir şekilde savaşmak temel bir gerekliliktir. Süreçlerin titizlikle tanımlanması ve yürütülmesi, kurumların ve bireylerin dijital varlıklarını korumak için önemli bir adımdır.

Diğer yandan, ulusal ve uluslararası düzeyde iş birliği ve bilgi paylaşımı, tehditlerle başa çıkmak için daha güçlü ve koordineli bir yaklaşım sağlar. Varlıkların sınıflandırılması ve zafiyetlerin tespiti, dijital altyapının güvenliğini sağlamak için gereklidir. Sistemlerin sürekli olarak izlenmesi ve geliştirilmesi, tehditlerin hızla değişen doğasına uyum sağlamak açısından önem taşımaktadır. Bununla birlikte, dijital bağışıklığı tam anlamıyla sağlamak için insan faktörüne de yatırım yapılmalıdır. Bilinçli ve eğitilmiş personel, dijital tehditlere karşı daha dirençli bir organizasyon oluşturmanın anahtarıdır.

Ek 4-35/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.



Ek-4 Tespit ve Öneriler

Dijital çağın gerekliliklerine uyum sağlamak için teknolojinin yerinde ve doğru kullanılması da kritik öneme sahiptir. Yedekleme ve kurtarma süreçleri ile felaket kurtarma planları, olası risklere karşı hazırlıklı olmanın önemli bir parçasıdır.

Dijital bağışıklığın sürdürülebilirliği; sürekli izleme, analiz ve güncellemeye bağlıdır. Siber tehditlerin izlenmesi, tespiti ve önlenmesi süreci ise karmaşık ve dinamik bir yaklaşım gerektirmektedir. Teknolojideki her türlü ilerlemeye rağmen bu alanda insan sezgisine, öngörü ve sağduyusuna duyulan ihtiyaç azalmayacaktır. Bu nedenle alınacak her türlü teknik ve idari siber güvenlik önlemi, güçlü bir insan kaynağı ve sürekli eğitimle mutlaka desteklenmelidir.

Dijital bağışıklığı güçlendirmek için tespit ve önleme stratejileri hayati öneme sahiptir; bu stratejiler, olayların hızlı bir şekilde tespiti ve uygun yanıtların verilmesini sağlayarak olası zararları minimize etmeyi amaçlar. Otomasyon ve yapay zekâ gibi teknolojiler, tehditleri hızla tanımlayıp karşı önlemler almayı kolaylaştırarak bu süreci daha etkin hâle getirebilir. Aynı şekilde, yedekleme ve kurtarma süreçleri, olası veri kayıplarına karşı önleyici bir önlem olarak önemli bir rol oynar ve dijital varlıkların güvenliğini sağlamaya yardımcı olur.

Yasal ve teknolojik tedbirlerin alınması, dijital güvenliğin sağlanması için vazgeçilmezdir ve bu çerçevede, organizasyon yapılarının oluşturulması ve olgunlaştırılması tehditlere karşı daha dirençli bir yapı oluşturmak için gereklidir. Ulusal ve uluslararası düzeyde bilgi paylaşımının sağlanması için iş birliğinin geliştirilmesi, dijital tehditlerle mücadelede daha etkili bir yaklaşımı teşvik ederken hem proaktif hem de reaktif tedbirlerin alınması, tehditlere karşı sürekli bir çaba gösterilmesini sağlar. Bu stratejilerin etkin bir şekilde uygulanması, dijital bağışıklığın güçlendirilmesine yardımcı olacaktır.

Yeni nesil dijital teknolojilerin, siber olayların doğası ve karmaşıklığı üzerindeki etkisi oldukça derinlemesine incelenmelidir. Bu teknolojiler, siber tehditlerin ölçeğini ve karmaşıklığını önemli ölçüde değiştirmiştir. Özellikle kuantum ve blokzincir teknolojileri ve yapay zekânın eğitilmesi gibi alanlarda ortaya çıkan eğilimler, siber tehditlerin çok daha karmaşık ve öngörülemez hâle gelmesine katkıda bulunmaktadır.

Yapay zekânın yanlış verilerle eğitilerek zehirlenmesi ve IoT cihazlarının ilerleyen süreçte potansiyel tehdit oluşturması gibi faktörler, siber saldırıların artan bir şekilde karmaşık hâle

Ek 4-36/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.



Ek-4 Tespit ve Öneriler

gelmesine yol açmaktadır. Bu bağlamda, yapay zekânın savunma yeteneklerimize entegre edilmesi ve yapay zekâ destekli araçların kullanılması, siber güvenlik alanında önemli bir stratejik ölçek olarak öne çıkmaktadır.

Saldırı yüzeyinin artması, teknoloji çeşitliliğinin genişlemesi ve sertifikasyon ile akreditasyonun önem kazanması gibi faktörler de ayrıca dikkate alınmalıdır. Özellikle IoT cihazlarının sayısının logaritmik artışı, farklı saldırı vektörlerinin ortaya çıkmasına neden olabilir ve bu da savunmayı daha zorlaştırabilir.

Yapay zekâ, kuantum hesaplama ve otomasyon gibi alanlardaki gelişmelerin, siber olayların öngörülebilirliğini, şiddetini ve ölçeğini de karmaşıktırması, savunma stratejilerinin daha dinamik ve çok katmanlı bir yaklaşımla hazırlanması ve sürekli güncel tutulması gerektiği anlamına gelmektedir.

Siber olaylara müdahalede ulusal ve uluslararası iş birliğinin önemi, dijitalleşmenin son derece arttığı günümüz dünyasında daha da belirginleşmektedir. Türkiye'nin bu iş birliklerinde etkin bir rol oynaması ve hedefler belirlemesi önem taşımaktadır. Öncelikle, siber güvenlik ekosistemindeki birçok paydaşın katılımını gerektiren bu yapıda kamu, özel sektör, akademi, askerî kurumlar ve sivil toplum kuruluşları arasında canlı bir iş birliği ve tecrübe paylaşımı ortamı oluşturulmalıdır. Bu ortam, özellikle SOME'ler arasında çok daha etkin bir şekilde kullanılabilir.

Siber güvenlik, multidisipliner bir alan olduğundan, tek bir kurumun çabasıyla başarılamayacak kadar karmaşıklık içermektedir. Bu nedenle, ulusal seviyede birçok kurumun bir araya gelmesi ve iş birliği içinde hareket etmesi tercih değil, bir mecburiyet olarak görülmelidir. Siber olayların öncesi, olay anı ve sonrasında yapılması gerekenlerin bilinmesi ve uygulanması, alınan derslerin kaydedilmesi, tecrübe paylaşımı ve geri besleme hususları büyük önem taşımaktadır. Tehdit istihbaratı paylaşımı da siber olaylara müdahale açısından en kritik unsurdur.

Uluslararası iş birliği ise siber güvenlik anlayışının şekillendirilmesi, ulusal politikalarımızın empozesi ve bilgi alışverişinin artırılması açısından önemli bir diplomatik araçtır. Bu konuda, uluslararası seviyede iş birliği anlaşmaları ve ortak platformlar oluşturulmaktadır. Kamu kurumlarının iletişimini artırmak ve kurumlar arası iş birliğini güçlendirmek kadar küresel

Ek 4-37/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.



Ek-4 Tespit ve Öneriler

ağlarla irtibatla ve uyumlu olmak da önemlidir. Türkiye'nin ulusal düzeyde USOM gibi yapıları güçlendirmesi ve uluslararası düzeyde benzer organizasyonlarla ortaklıklarını geliştirmesi gerekmektedir. Bu şekilde, koordineli bir şekilde hareket ederek sadece uygulayan değil, aynı zamanda yön veren bir pozisyonda olunabilir.

Sonuç olarak, siber güvenlik alanındaki gelişmelerin takip edilmesi, ulusal ve uluslararası iş birliklerinin güçlendirilmesi, otomasyon ve yapay zekâ gibi yeni teknolojilerin dikkatlice kullanılması ve siber güvenlik ekiplerinin sürekli eğitilmesi, Türkiye'nin siber güvenlik alanındaki müdahale kapasitesini artırmak için atılması gereken adımlar arasında yer almaktadır.

Özetle, değişen ve gelişen teknolojiler ile beraber evrilen siber olaylara müdahale ve önleyici eylemler için de yenilikçi yaklaşımlar sergilenmesi bir mecburiyet olarak görülmektedir. Bu yaklaşımların millî bilinç ve disiplinle ele alınması ayrıca önemlidir. Derlenmiş diğer öneriler ise şu şekilde sıralanabilir:

- Yapay Zekâ, Blokzincir, Bulut Bilişim, IoT cihazları ve Kuantum teknolojileri gibi yeni teknolojilerin siber tehditlerin ölçeğini ve karmaşıklığını artırdığı göz önünde bulundurularak, siber güvenlik önlemlerinin bu gelişmelere ayak uyduracak şekilde geliştirilmesi gerekmektedir.
- Yerli ve bağımsız teknolojilere verilen destek artırılmalı ve vatandaşın bilgi güvenliği farkındalığının yükseltilmesi için çalışmalar yapılmalıdır.
- Dijital vatanın korunması ve dayanıklılığının sağlanması için siber olayların düzgün monitör edilmesi, ağda, sunucularda ve son kullanıcılarda meydana gelen tüm olayların görünürlüğünün sağlanması kritik önem taşımaktadır.
- Değişen teknolojiler ile beraber evrilen siber olaylara müdahale ve önleyici aksiyonlar için yenilikçi yaklaşımlar sergilenmeli ve bu yaklaşımların millî bir bilinç ve disiplinle ele alınması önemlidir.
- Dijital bağımsızlığın temel gerekleri olan maruz kalma ve etkenlerle baş etme yeteneğinin güçlendirilmesi için proaktif ve reaktif tedbirler alınmalı, bireylerin ve toplumun zararlı bilgilere ve dezenformasyona karşı direnç gösterme yetenekleri artırılmalıdır.

Ek 4-38/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

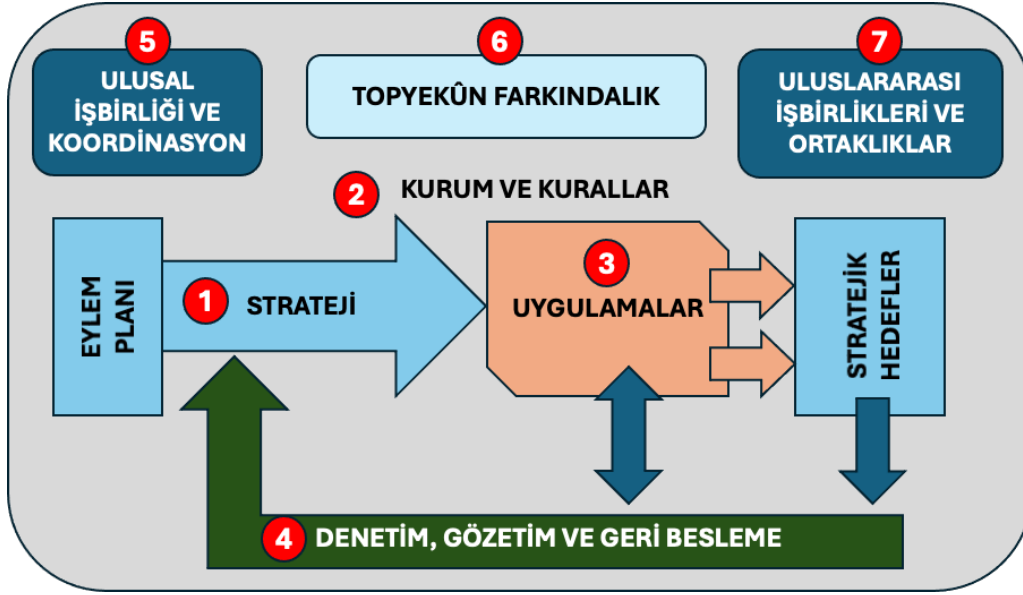
Ek-4 Tespit ve Öneriler

- Siber güvenlik ekiplerinin otomasyon ve yapay zekâ kullanımının rolü göz önünde bulundurularak, bu teknolojilerin potansiyel faydaları ve riskleri değerlendirilmeli ve dikkatlice kullanılmalıdır.
- Ulusal ve uluslararası iş birliğinin önemi vurgulanmalı ve kurumlar arası iş birliği güçlendirilmelidir. Türkiye'nin uluslararası politikalara yön veren bir konumda olması ve uluslararası iş birliklerinde aktif rol alması hedeflenmelidir.

Ek 4-39/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

6. Ulusal Siber Güvenlik Yönetişi



Şekil 1- Ulusal Siber Güvenlik Yönetişim Modeli (Örnek)

6. 1. Tespitler

Çalıştay katılımcılarının siber güvenlik kapsamındaki mevcut duruma dair değerlendirmelerine genel olarak bakıldığında, ülkemizin bu alanda önemli mesafe aldığı ancak gerek konunun dinamik doğası gerekse hızlı teknolojik gelişmeler nedeniyle önemli birtakım eksiklikler ve aksayan hususlar da olduğu yönündeki yorumun ağırlık kazandığı söylenebilir.

En uçtaki yorumlara bakıldığında ise ülkemizin siber kapasitesinin birçok gelişmiş ülke seviyesinin üzerinde olduğu bir tarafta, kritik altyapılar, siber kriz yönetimi, siber tehdit istihbaratı, siber güvenlik kapasitesinin ve ekosisteminin geliştirilmesi, yeni nesil teknolojilerin siber güvenliğe etkisi gibi hemen her alanda uluslararası camiadan geri kaldığımız görüşü diğer tarafta yer almaktadır. Şüphesiz bu iki yaklaşım da gerçeği tam olarak yansıtmamaktadır. Konunun detayına ilişkin hususlar bir önceki kısımdaki modele uygun başlıklar hâlinde aşağıda sunulmuştur.

6.1.1. Politika ve Strateji Geliştirme

Ek-4 Tespit ve Öneriler

Genel olarak strateji ve politika dokümanları ile eylem planlarının, dünyadaki gelişmelerle eş zamanlı olarak, zamanında ve yeterli kapsamla geliştirildiği ve yayınlandığı söylenebilir. Çalıştay'da bu hususta mevcut duruma ilişkin çok fazla olumsuz yorum gündeme getirilmemiştir.

Bununla beraber, ülkemizde bir strateji enflasyonu bulunduğu ve siber dünyaya dair benzer dokümanların birbirleriyle uyumlu ve koordineli bir şekilde geliştirilmesinde fayda bulunduğu yorumlarına rastlanmıştır.

Ayrıca; siber güvenlik alanında politika ve strateji geliştirirken, siber dünyada barış diye bir durum olmadığı ve sürekli sessiz savaş hâlinin yaşandığı bilinci ve bakış açısıyla olaya yaklaşmakta fayda bulunduğu belirtilmiştir.

6.1.2. Kurum ve Kurallar (Mevzuat)

Siber güvenlikle ilgili düzenlemeler ve organizasyonun mevcut durumuna ilişkin tespit ve değerlendirmeler kapsamında;

- Çok fazla regülasyona maruz kalındığı, bu durumun karışıklığa neden olduğu ve sadeleştirmeye gidilmesine ihtiyaç bulunduğu,
- Hâlihazırda yürürlükte olan muğlak regülasyonlar ve ucu açık ifadelerin, yazılan ama uygulanmayan kurallar olarak atıl kaldığı, bu kapsamda, üzerinde biraz çalışmayla güncel hâle getirilebilecek ve net ifadeler içeren düzenlemelere ihtiyaç bulunduğu,
- Siber güvenliğin çeşitli alanlarını kapsayan ikincil düzenlemelerde de eksiklikler olduğu ve görece yavaş yayımlandığı, bu konuda uluslararası camiadan geride kalındığı,
- Dijital Egemenlik kavramının çok iyi düşünülerek tanımlanması gerektiği ve bu hususta gri alanlar bulunduğu,
- Ulusal siber kriz yönetim sürecimizin tanımlı ve olgun olmadığı,
- Konuyla alakalı mevzuat geliştirme hızımızın yavaş, siber risk ve tehditlerin değişim, gelişim ve evriminin ise çok hızlı olduğu,
- Konuya ilişkin bakanlıklar üstü bir yapı olmaması ve doğrudan siber güvenlik alanını düzenleyen müstakil bir yasa bulunmamasının, pek çok sorun ve aksaklığın ana kaynağı olduğu,

Ek 4-41/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

Ek-4 Tespit ve Öneriler

- Teknik yetkinlik seviyesi güçlü bir ulusal siber güvenlik yapılanmamız olduğu ama yapının dağınık bir görüntü arz ettiği,
- Ulusal siber güvenlik yönetişiminin, hâlihazırdaki mevzuat altyapısıyla, pek çok kurumun paydaş olduğu dağınık ve görevlerin çakıştığı bir yapıda sürdürülmekte olduğu,
- AFAD'ın siber alanda bir çalışması ve yetkinliği olmadığı hususları dile getirilmiştir.

6.1.3. Siber Güvenlik Uygulamaları

Mevcut uygulamalarda tespit edilen ve katılımcılar tarafından birinci çalıştayda dile getirilen hususlar;

- Kamuda siber güvenlik yetkinliklerini artıracak yeterli insan kaynağı olmadığı, dahası, siber güvenlik alanında, hemen her sektörde ciddi bir personel eksikliği sorunu bulunduğu,
- Siber konularda tespitte iyi olmamıza rağmen müdahalede geciktığımız gerçeği,
- Tedarik süreçleri ve alımlarda normal usulden daha çok, istisna alımlar kullanıldığı ve parçalı bir yapının olduğu, bunun yabancı ürünler lehinde kullanıldığı,
- Tatbikat ve diğer hazırlıklar konusunda ülke bazında eksikler bulunduğu ve yeterli düzeyde olunmadığı,
- Yabancı menşeli ürünlerin çok yaygın olarak kullanıldığı ve herhangi bir kriz, seferberlik ve savaş durumunda bunlara erişimde sorun yaşanmasının kuvvetle muhtemel olduğu,
- Ulusal siber güvenlik stratejisinin oluşturulmasında sorun bulunmadığı ancak uygulanmasında kurumların yetersiz kaldığı,
- Ulusal siber güvenlik stratejisinin oluşturulması ve uygulanmasında farklı dinamiklerin göz önünde bulundurulmamasından dolayı birtakım zorluklarla karşılaşıldığı,
- Kamunun hizmet sunmak, özel sektörün ise doğası gereği kâr amaçlı ve hayatta kalabilmek için çalıştığı,
- Siber tehdit istihbaratı konusunda çok yeterli olunmadığı, bilgiye ve istihbarata geç ulaşıldığı,

Ek 4-42/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

Ek-4 Tespit ve Öneriler

- KOBİ'lere bütüncül bir planlamayla ücretsiz yazılımlar sunulması gerektiği, aksi takdirde büyük oyuncunun küçüğü ezdiği,
- Bazen o olgunluk seviyesinde veya o özelliklerde bir siber güvenlik ürününe ihtiyaç olmadığı hâlde yabancı menşeli ürünlerin alındığı,
- Yerli ve millî ürünlerin tercih edilip kullanılmadıkça olgunlaşmadığı, olgunlaşmadıkça da tedarik edilmediği bir kısır döngü yaşandığı,
- Yerli ürün fiyatlarının yabancı ürün fiyatlarıyla aynı düzeyde, hatta bazen daha pahalı olduğu durumlar görüldüğü,
- 'Yerli' firmaların ve ürünlerin hepsinin %100 yerli ve millî olmayabildiği, arka planda lisans ücretleri ödendiği,
- Başlangıçta yerliyen sonradan yabancıya satıldığı için Türkiye'ye teklif dahi veremez/vermez hâlde gelen örneklerin mevcut bulunduğu,
- Yerli ve millî bilgi teknolojisi ürünlerinin kullanımı konusunda 2011 yılında yayımlanmış genelgenin üzerinden 13 sene geçmiş olmasına rağmen bu konunun hâlâ tartışılıyor olmasının düşündürücü olduğu, dolayısıyla net ve keskin çözümlere ihtiyaç bulunduğu şeklinde sıralanmıştır.

6.1.4. Denetim ve Gözetim

Mevcut uygulamaların takibi, sonuçlarının ölçülmesi ve geri beslemelerin alınmasına dair dikkat çekilen noktalar kapsamında;

- Strateji ve eylem planlarının uygulanmasına yeterince eğilinmediği,
- Altyapıların, ulusal tehdit durumunda ne kadar güvenli oldukları hakkında bilgi eksikliği bulunduğu,
- AB'de sektörel SOME'ler bulunduğu, ülkemizde mevcut 14 sektörel SOME'nin, piyasa gözetim ve denetimi için yeterli olmadığı,
- Stratejik siber güvenlik eylemlerinin izlenmesi ve sonuçlarının toplumla paylaşılması gerektiği,

Ek 4-43/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

Ek-4 Tespit ve Öneriler

- Siber dayanıklılık seviyemizin ölçülemediği, bu nedenle konuya ilişkin tatbikatlar ve ölçme/değerlendirme metodolojilerinin geliştirilmesine ihtiyaç bulunduğu,
- Ulusal stratejilerin takibi ve uygulanması konusunda yapısal sorunlar olduğu, konunun sorumlularının, stratejinin oluşturulması aşamasında sürece dâhil edilmediği,
- Siber güvenlik alanının, teknoloji, bütçe ve sektörel olarak ayrıştırılarak takip edilmediği ve ölçülmediği,
- Siber güvenlik konusunda Cumhurbaşkanlığı yönetim sistemine uyumun tam olarak sağlanamadığı,
- Stratejide geçen eylem adımlarına dair sonuçların izlendiği konusunda tereddüt bulunduğu ve ne durumda olduğumuzun bilinmediği,
- Yerli ürünlerden bir kısmının çeşitli sertifikasyonlardan geçmiş olmasına rağmen güven noktasında ‘sarsıcı gözlemler’ barındırdığı,
- En kritik sistemlerde hangi ürünlerin kullanılacağını çoğu zaman el yordamı ve tecrübeyle tespit edildiği, bu nedenle çok ciddi bir şekilde Siber Güvenlik Akreditasyon Otoritesi’ne ihtiyaç bulunduğu belirtilmiştir.

6.1.5. İş birliği

Siber güvenlik konusunda iş birliği, koordinasyon ve ekosistemin canlılığına dair yapılan mevcut durum tespitleri dâhilinde;

- Sektörle bağlantıda ve kurumlar arası koordinasyon ve iletişimde eksiklikler bulunduğu,
- Ulusal siber güvenlik stratejisinin oluşturulması ve uygulanmasında paydaşlar arasında iletişim ve iş birliği sağlanmasının en çok zorlanılan konulardan biri olduğu,
- Siber Kümelenmede ciddi sayıda yerli firma bulunduğu ancak güven duyulan yazılım sayısının kısıtlı olduğu hususları dile getirilmiştir.

Bu başlık altında, tespit sayısı az olmasına rağmen aksaklığı işaret edilen konuların ciddiyetinin yüksek olması dikkat çekicidir.

Ek 4-44/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

6.1.6. Topyekûn Farkındalık

Siber güvenlik konusunda ülkemizdeki mevcut duruma ilişkin olarak;

- Toplumun geniş kesimlerinde siber güvenlik konusunda farkındalık eksikliği olduğu,
- Bu konuda çok erken yaşlardan itibaren -âdeta bir trafik eğitimi verir gibi veya çocuğa öz bakım yeterliliği kazandırır gibi- bu alışkanlıkların edinilmesi gerektiği,
- Çok sayıda eğitim verilmesine ve önemli inisiyatifler alınmış olmasına rağmen, bunların hâlâ yetersiz kaldığı,
- İnsan kaynağının ve eğiticilerin sayıca ve yetenekçe yetersiz olması nedeniyle mesleki teknik eğitimlerin nicelik, ama özellikle de nitelik konusunda yeterli seviyede olmadığı ifade edilmiştir.

6. 2. Öneriler

Ulusal siber güvenlik yönetişiminin; çağın ihtiyaçlarına, gelecek modellemelerine ve vizyonuna göre yeniden ele alınması zorunluluktur. Bu zorunluluğun hangi boyutta ve hangi bileşenlerle yerine getirileceği konusu önceki bölümde tartışılmış ve yedi ana başlıktan oluşan bir model tasvir edilmiştir.

Ulusal Siber Güvenlik Yönetişimi kapsamında 1'inci Çalıştay'da katılımcılardan alınan tespitler, ihtiyaç tanımları, eğilim ve beklentiler bu tasvire uygun olarak tasnif ve tanzim edilerek ilgili başlıklar altında sunulmuştur.

6.2.1. Vizyon, politika ve strateji geliştirilmesi kapsamında:

Ulusal siber güvenlik ve savunma başta olmak üzere yaygın ve sıklıkla kullanılan bazı tanımların netleştirilmesine ihtiyaç bulunmaktadır. Bu kapsamda sarıh bir izaha gerek duyulduğu en çok belirtilen kavramların başında yerlilik ve millilik sözcükleri gelmektedir.

Tanım ve kavramlar kapsamında ayrıca, dijital vatan için geniş bir çerçeve çizilmesi ve dijital egemenliğin artık bir bağımsızlık seviyesi olduğu hususunun ilgili dokümanlarda vurgulanarak, dijital vatan, dijital bağımsızlık ve dijital egemenlik kavramlarının net bir şekilde mutlaka bu dokümanlara ithal edilmesi gerektiği belirtilmiştir.

Ek 4-45/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.



Ek-4 Tespit ve Öneriler

Üst seviye dokümanların hazırlanmasında güncel bir yaklaşımın benimsenmesi ve dokümanlarda yerli ve millî kapasite ile dijital vatana mutlaka hükmetme ve siber güvenliğin millî güvenlik unsuru olduğu vurgusunun yer almasına ihtiyaç bulunmaktadır.

Ulusal siber güvenlik stratejisinin geliştirilmesinde, yüksek katılımı çok geniş tabanlı olarak paydaşların bir araya gelmesi, stratejinin uygulanması sürecinde ise ortak hedefler ve ortak bakış açısı ile yönetilmesi önem arz etmektedir.

Bu kapsamda paydaşların alanda üstlendikleri roller iyi belirlenmeli, sonrasında aralarında koordinasyonu sağlayacak mekanizmalar netleştirilmelidir. Ayrıca, siber güvenliğe ilişkin stratejilerin uygulanabilmesi için tüm kurumları bağlayıcı ulusal mevzuat oluşturulmalıdır.

Strateji çalışmaları tüm kurumların katılımına açık olmalı, ilan edilmeli, taslaklar kurumların görüş ve değerlendirmelerine açılmalı ve ulusal terminoloji birliği sağlanmalıdır. Gerek hazırlık gerekse uygulama süreçlerinde; akademi, özel sektör ve kamu iş birliği daha etkin oluşturulmalıdır.

Stratejik karar alma mekanizmalarının; siber güvenlik uzmanlığı olan tarafların temsil edildiği kamu, özel ve sivil toplum kuruluşlarından, standart oluşturma ve teknoloji geliştirme konularına hâkim, sivil ve askerî otoriteler ile meslek kuruluşları, ihtiyaç makamları vb. zengin bir kompozisyona sahip ve siyasi temsilin de üst seviyede olduğu bir yapı olması gereklidir.

Strateji oluşturma sürecine dâhil olduğu ölçüde aidiyet artacak ve uygulama aşamasında hedeflere ulaşmak kolaylaşacaktır. Sebep, süreç ve sonuçları kapsayan tüm safhaların şeffaf olarak kamuoyuyla paylaşılması da konuya yaklaşımdaki ciddiyet ve inandırıcılığın yerleşmesine katkı sağlayacaktır.

Stratejiler oluşturulurken, her yerde güvenlik yerine, doğru yerde güvenlik prensibiyle önceliklendirmelere gidilerek sıklet merkezi oluşturulması gerekmektedir. Bu konuda zaman kaybedildiği değerlendirilmektedir.

6.2.2. Mevzuat, organizasyonel yapı ve diğer ikincil düzenlemeler kapsamında:

Yönetim Organizasyon

Ek 4-46/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

Cumhurbaşkanlığı Yönetim sistemine geçişle birlikte haberleşme ve bilgi güvenliği konularından doğrudan sorumlu icracı bir bakanlık kurularak, yapı yeniden organize edilmelidir.

Ulusal siber savunma koordinasyon sorumluluğu ise bakanlıklar üstü tanımlanacak bir yapıda konumlanmalıdır. Bu oluşum, kurumlar üstünde bir yetkilendirme ile doğrudan Cumhurbaşkanlığına bağlı faaliyet gösterecek “merkezi” bir siber güvenlik otoritesi olmalıdır.

Tüm kamu kurumları, özel sektör ve diğer paydaşlar üzerinde bir siber otorite olarak tek elden yönetişimin ana sorumlusu olacak bu Kurul’un hayata geçmesi ile birlikte siber güvenlik alanında en üstten en alta kadar yapılaşmaya gidilmesi ve sistemin günün şartlarına uygun olarak yeniden düzenlenmesi gerekmektedir.

Mülga Siber Güvenlik Kurulu yetkilerine ve gerekli diğer yetkilere sahip, stratejiden başlayarak, taktik ve operatif seviyeye kadar, yönlendirme ve yönetim işlevlerini uhdesinde barındıran bir üst otorite makamı olarak, tüm kurumların bu merkezden yerli ve millî imkânlarla her anlamda beslenmesi ve adı geçen kurul tarafından kurumlar arası koordinasyonun tek merkezden yönetilmesi, denetim, yaptırım ve teknik faaliyetlerin yine aynı merkez aracılığı ile idare edilmesinde fayda görülmektedir.

Cumhurbaşkanlığı Hükümet sistemi ile uyumlu çatı bir koordinasyon kuruluşu, “Kurul (Board)”, olarak görev yapması beklenen bu yapı, müstakil ve kapsayıcı bir “Siber Güvenlik Yasası” ve bütünüleyici ikincil düzenlemelerle de tamamlanmalı ve desteklenmelidir.

Bilişim sektöründe herkesin kendi güvenliğini kendi sağlaması yerine güvenli alanlar yaratılmasına ihtiyaç bulunmaktadır. Bilirkişilerin bir araya getirilmesi, organize edilmesi, süreçlerin devamının sağlanması, koşulsuz uygulanması fikri değerlendirilmelidir.

Tek bir siber ordu ile bütün siber ulusu savunmanın mümkün olmadığı dünyadaki örneklerle sabittir. Bunun yerine askerî harekâtın dayandığı kritik altyapıları korumaya yönelik bir Ulusal Siber Görev Gücünün tanımlanması, barıştan itibaren planlanması, denenmesi, senaryo tabanlı faaliyet ve hazırlıkları öngörülmelidir.

Barış, Kriz, Alarm, Savaş, Seferberlik durumlarında görev ve sorumluluklar;

Ek-4 Tespit ve Öneriler

Ülke geneline uygulanacak standartlar, politikalar ve eylemlerin belirlenmesi gereklidir. Örnek olarak ulusal çapta risk yönetim çerçevesi (RMF) oluşturulabilir. Sınırları iyi belirlenmiş bir görev dağılımı yapılması gerekmektedir.

Ulusal siber alarm durumunun, normal alarm durumuyla örtüştürülmesi konusu çalışılmalıdır. Siber tehdit istihbarat ve erken tespit platformlarının hâlihazırda belli düzeyde hizmet sunması önemli olmakla birlikte geliştirilmesi gerekmektedir. Barış, kriz, gerginlik ve savaş silsilesini takip ederek adım adım planlama ve değerlendirmeye ihtiyaç bulunmaktadır.

Savaş ve seferberlik durumlarında, siber varlıkların korunmasının sağlanması ve neyin nasıl yapılacağının ezbere biliniyor olması, yetki ve sorumlulukların başta seferberlik ve savaş hâli olmak üzere netleştirilmesi, gerekirse yeniden düzenlenmesi, özetle kriz yönetme becerisi edinilmesi elzemdir.

Stratejilerin düzgün bir şekilde planlanması, uygulanabilir bir yapı kurulması, yönetim kapsamında belirlenen usuller ve standartların faydalı özellikleri bağlamında tam ve eksiksiz uygulanması için önlemler alınmalıdır.

Aktif siber savunma için güç ve kabiliyet geliştirme, organizasyon yapısını gözden geçirme ihtiyacı bulunmaktadır.

Siber alanda teknolojiyi büyük oranda özel sektör sürüklemektedir. Bu nedenle, teknolojinin gelişmesi, trendlerin yakalanabilmesi için özel sektör yeteneklerinin artırılması gerekir. Bu noktada, özel sektöre yönelik regülasyonlar önem taşımaktadır. Kamu, objektif bir düzenleme ile kontrol çerçevesi oluşturmalıdır. Kamu teşvikleri, destek paketleri, ihracat destekleri, vergi indirimleri bu kapsamda düşünülebilir.

Dijital egemenlik hedefine ulaşılabilmesi için düzenlemelerin net olduğu, hızlı, sürdürülebilir, tabiri caizse saat gibi işleyen bir yönetim yapısı gerekmektedir.

6.2.3. Uygulamalara dair ihtiyaç, beklenti ve eğilimler kapsamında:

Yerli ve Millî Konusu

Yerli ve millî siber güvenlik ürünlerinin kullanılması ve yaygınlaştırılması konusunun artık millî teknolojiler lehine nihayete erdirilmesi gerekmektedir. Bu doğrultuda dijital

Ek 4-48/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.



Ek-4 Tespit ve Öneriler

altyapılarımızın yerelleşmesi için hem teşvik hem de kanun eliyle zorlamaya ihtiyaç bulunmaktadır.

Hazır olmayan ürünlerin bir an evvel tamamlanması, kişisel bilgilerin korunması için kendi platformlarımızın hayata geçirilmesi ve dışa bağımlılığın azaltılması gerekmektedir. Yerli kaynakların kullanımının artırıldığı ölçüde güçlü ve bağımsız olunacağı hatırdan çıkarılmamalıdır.

Kurumların birincil görevi kendini korumak, ikincil olarak da yerli ürünleri korumak olmalıdır. Yerli ürünlerde kalitenin artırılması, istikrarlı ve sürdürülebilir bir sunumla ürünün cazip kılınması yoluyla yerli ürünlere/yazılımlara güven kazandırılmalıdır.

Yerli ve milliliğin tanımı yapılmalı, netleştirilmeli, gri alanlar ortadan kaldırılmalı veya olabildiğince azaltılmalıdır.

Yerli ürün kullanımında ceza yerine ödül mekanizmalarının ön plana çıkarıldığı daha keskin, net ve sonuç alıcı çözümlere ihtiyaç bulunmaktadır.

Yerli ürünlere, tedarik veya teşvik yoluyla parasal ve satın alma desteği verilmesi yanında, kullanım sürecinde geri beslemelerde bulunulması en az diğeri kadar önem taşımaktadır. Bu kapsamda somut geri bildirim mekanizmalarının oluşturulması ve bu hususun tüm kamuya yaygınlaştırılması gereklidir.

Yerli ve millî ürünlerin kullanımında ve yaygınlaştırılmasında ivme kazanmak için, üretim sürecinde odaklı işlere hızlı ve verimli gerçekleştirmelerle imza atacak teknik yetkinlik ve uzmanlaşmanın kazanılması, elde tutulması ve kurulacak iş birliği platformları ile destek ve teşvik sağlanması bir mecburiyettir. Yerli ve millî ürünlerin kullanımı yalnız kamuda değil eş zamanlı olarak tüm dijital vatan sathında ele alınmalıdır.

Yerli ürünlerin sahada rüştünü ispat edene kadar tevazu içerisinde ilerlemesi ve kendini geliştirmeye odaklanması gerekmektedir. Bu kapsamda TOGG yerli elektrikli otomobili ve çok sayıdaki savunma sanayi projesi model olarak örnek alınabilir. Üretici/kullanıcı, kamu/özel sektör birlikte geliştirme ve iyileştirme süreçleri yaygınlaştırılabilir.

Sosyokültürel Bariyerler

Ek 4-49/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.



Ek-4 Tespit ve Öneriler

Ulusal stratejilerin ciddiye alınması ve eylem planlarında tanımlanan işlemlerin titizlikle hayata geçirilerek takibinin yapılması gerekmektedir. Kural ve düzenlemelerin etrafından dolaşarak, yapılmıyormuş izlenimi yaratılması yönündeki davranış modelinin terk edilmesi için gerekli sosyolojik ve kültürel çalışmalar dâhilinde tedbir geliştirilmelidir.

Kriz Durumları

Herhangi bir nedenle yaşanan kriz ve kaos durumlarında enerji-üretim ve dağıtım zincirinin en kritik halkası olan enerji arzının sürekliliğine ilişkin tedbir alınması hayati önemi haizdir. 06 Şubat 2023 tarihinde meydana gelen deprem felaketinde yaşanan sayısız tecrübe buna çarpıcı örnek olarak verilebilir.

Siber Olay Müdahale

Ulusal tehdit modelleme metodolojisi çerçevesinde başta siber tehdit istihbaratı ve erken uyarı-ihbar sistemi olmak üzere bazı teknik çözümlerin geliştirilmesi ve zafiyet ortaya çıkmadan önce gerekli tedbirin alınması gerekmektedir.

Kamunun yeni nesil siber tehditlere karşı reaksiyon kabiliyetini, bulut bilişim gibi teknolojileri azami şekilde kullanarak geliştirmesi ve aktif siber savunma, ofansif güvenlik gibi konseptleri ve bunlarla ilişkili yetenekleri geliştirerek bünyesine dâhil etmesi gerekmektedir.

Siber olay yönetimi alanında USOM'un da üzerinde bir eşgüdüm makamı oluşturulması gerekmekte, yalnızca siber olayların sonrasında müdahalede bulunan değil, olay öncesi, olay esnası ve sonrası olmak üzere yürütülecek tüm faaliyetleri koordine edebilecek bir yapıya gereksinim duyulmaktadır.

Yeni sektörel SOME'ler oluşturulup sıkı denetimleri yapılmalı ve savunma sanayi paydaşları ayrı bir sektörel SOME olarak ele alınmalıdır.

Beyin Göçü

Zaten kısıtlı bulunan yetkin ve nitelikli insan kaynağının ülkede tutulması siber güvenlik alanında başarı için hayati önem taşımaktadır. Bunun sağlanması için gerekli yasal, idari, ekonomik ve sosyolojik tedbirler alınmalı, eldeki personelin ülkede tutulması yanında, dünyadaki yeteneklerin ülkemize çekilebilmesi için cezbedici yol ve yöntemler oluşturulmalıdır.

Ek 4-50/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.



KOBİ'lere Siber Güvenlik Desteği

Tüm şirketlerin aynı imkân ve kabiliyet düzeyinde olamayacağından hareketle, küçük ve orta boy işletmelerin siber güvenliğini sağlamak amacıyla istifade edebilecekleri güvenli alanlar oluşturulmalı, KOBİ'ler için ayrıca yazılım ve altyapı desteği sağlanmalıdır. Zira, tedarik zincirinin siber güvenliği, en alttaki sağlayıcıdan başlamakta ve en zayıf halka kadar güçlü olmaktadır.

Tedarik Süreçleri

Yenilikçi kamu tedarik süreçleri oluşturulmalı, alımlarda bütünlük sağlanmalı, bu süreçler yerli ve millî ekosistemi olgunlaştıracak şekilde kurgulanmalıdır.

6.2.4. Denetim ve Gözetim

Akreditasyon ve Onay

Hâlihazırda en kritik sistemlerde dahi hangi ürün ve sistemlerin ne şekilde kullanılacağı konusu büyük oranda el yordamı ve tecrübeyle tespit edilmektedir. Bu kapsamda çok ciddi bir şekilde Ulusal Siber Güvenlik Akreditasyon Otoritesi'ne ihtiyaç bulunmaktadır. Özellikle yabancı menşe ürün ve çözümler otoritenin akreditasyonlarına ilk önce tabi tutulmalıdır.

Denetim ve Yaptırım

Kamu kurumları ve özellikle ulusal kritik altyapılar üzerinde, piyasa gözetimi ve denetimi haricinde, savunma ve güvenlik bakış açısıyla siber güvenlik denetimi yapacak ve önlemler alabilecek bir yapıya ihtiyaç bulunmaktadır.

Siber güvenlik alanında yabancı yazılım ve donanımlara bağımlılık ülkemizi her anlamda zora sokmaktadır. Bunun çözümü için siber güvenlik konusu ayrı düzenlemelere tabi tutulmalı, yerli ürünlerin kalite ve güvenlik kontrolleri çok daha sıkı sağlanmalı, bu ürünlerin kullanımı teşvik edilmeli ve millî siber güvenlik şirketlerinin yabancı sermayeye satılması önlenmeli, alternatif yatırım yapıları oluşturulmalıdır.

Strateji belgeleri başta olmak üzere kural ve eylem dikte edici bütün düzenlemelerin uygulanması safhasında kurumları bağlayıcı tedbirler artırılmalı, etkin denetimleri yapılmalı ve önceden tanımlı yaptırımlar gerektiği durumlarda hayata geçirilmelidir.

Ek 4-51/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

Envanter Çıkarılması, Ölçme ve Değerlendirme

Sayılamayan şey ölçülemez ilkesinden hareketle, siber egemenlik için, siber envanterin bilinmesi büyük önem taşımaktadır. Bu kapsamda, başta kamu ve kritik altyapılar olmak üzere tüm sektörlerde kullanılan siber güvenlik ürün ve hizmetlerinin detaylı bir envanteri çıkarılmalıdır. Bilahare, bir plan ve önceliklendirme dâhilinde dijital altyapıların yerleştirilmesi, sektörün regüle ve teşvik edilmesi bağımsızlığa giden yolu açacaktır.

Siber dayanıklılık seviyemizi ölçebilmek ve gerçek durumumuzu bilebilmek için tatbikatlar ve ölçme/değerlendirme metodolojileri geliştirilmeli ve tüm alanlarda kullanılabilecek ortak bir düzenleme olmalıdır. (Örn. ISO 27001, Siber hijyen, KVKK vb.)

Regülasyonların uygulanma durumu ve düzeyinin sahada denetim ve takip işlemleri, çerçevesi ve standartları oluşturulmuş tutarlı bir yapıda, güçlü bir merkezi otorite ve yetkin denetçiler tarafından yapılmalıdır.

6.2.5. İş birliği ve Koordinasyon

Kamuda siber güvenlik yetkinliklerini artıracak yeterli insan kaynağı olmamasından dolayı özel sektör mutlaka ciddi bir paydaş olarak yönetim süreçlerine dâhil edilmelidir. Bu anlamda kamu ve özellikle kritik altyapıların korunmasına yönelik iş birliği gayretleri artırılmalı, hızlı iletişim ve bilgi alışverişi sağlanmalıdır. Bu birliktelik zamanla yönetimlere de güven verecektir.

Siber güvenlik yerli ekosisteminin gelişiminin hızlandırılmasına yönelik olarak sektörel bazlı üyelerin bir araya geleceği ve ortak akıl üretecekleri bir platform kurulması yönünde kararlar alınıp hızla uygulamaya geçirilmelidir.

Ulusal siber güvenlik açısından yönetim altyapısı en alt hücrelere kadar etki edecek şekilde mutlaka güçlendirilmeli, kesintisiz ve etkin bir iletişim, iş birliği ve istişare yoluyla çok paydaşlı yönetim kültürü yerleştirilmelidir.

Paylaşım, istişare ve iş birliği konusundaki tereddütleri ve kültürel menfi alışkanlıkları ortadan kaldırmak maksadıyla insanın dönüşümü için çaba sarf etmek gerekmektedir. Bu konu,



Ek-4 Tespit ve Öneriler

sadece siber güvenlik uzmanları ile sınırlı tutulamayacak ve geniş bir perspektiften ele alınarak çözüm aranacak bir problem sahasıdır.

Siber Güvenlik Kümelenmesinin faaliyetleri genişletilmeli ve kamuda yerli ürün kullanımının ödül mekanizmaları ile artırılması sağlanmalıdır. Ayrıca kritik kapsamda ürün geliştiren yerli firmaların yurt dışına satılmasının önüne geçilmesi gerekmektedir.

6.2.6. Topyekûn Farkındalık

Siber güvenlik personelinin sayıca ve yetkinlikçe yeterli hâle getirilmesinin sağlanması gerekmektedir. Bu konuda verilen eğitimler sayı, içerik ve nitelik olarak yeterli görülmemektedir. Konu, bilgi güvenliği farkındalığı kapsamında ilköğretimden başlayarak, ön lisans, lisans ve lisansüstüne kadar devam eden ve nihayetinde siber güvenlik mühendisi/teknisyeni/uzmanı yetiştirme ile neticelenecek bütüncül bir bakışla ele alınmalıdır. Söz konusu teorik öğretim süreci, beceri geliştirme eğitimleri ile desteklenmeli ve tamamlanmalıdır.

Yetiştirilen personele ilave olarak, formal eğitim süreçlerinden geçmemiş ama sahada kendini yetiştirmiş ilgili ve meraklı kişilerin tespiti ve sürece kazandırılması için yeni yetenek avcılığı mekanizmaları tanımlanmalı, varsa olanların ıslahı ve geliştirilmesi için çalışmalar yapılmalıdır.

Kamu kurumları ve kritik altyapılarda görevli sıradan kullanıcılar başta olmak üzere çalışanlarda siber güvenlik farkındalığı artırmaya yönelik çalışmalar yapılmalı, bu çalışmalar bilahare tüm sektöre yaygınlaştırılmalıdır.

Yerli yazılımların gerekliliği ve bu yazılımlara güven konusunda ilgili tüm paydaşlar nezdinde bir farkındalık kampanyasına ihtiyaç bulunmaktadır. Güven eksikliğinin varsa giderilmesi, endişe ve tereddütlerde haklılık payı varsa ürünün güvenilir hâle getirilmesi için tedbir alınmalıdır. Her iki tarafa da sorumlulukların düştüğü bu süreçte, teknolojik dönüşüm ve iyileştirmeler görece kolaysa da insanın dönüşümü ve ikna edilmesi konusunda bilimsel olarak ve titiz bir şekilde çalışılması gerekmektedir.

6.2.7. Uluslararası İş birlikleri ve Ortaklıklar

Ek 4-53/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.

Ek-4 Tespit ve Öneriler

Siber olaylara müdahale kapsamında caydırıcı birtakım yeteneklerin kazanımı ve bunların dünya kamuoyuna ilan edilmesi bir gerekliliktir. Söz konusu caydırıcı tedbirlerin nasıl alınacağı, hangi şartlarda ne şekilde kullanılacağı vb. hususlarda küresel bilinirlik, bu kabiliyetin etkisini artıracaktır. Bu kapsamda, tanımlı süreçlere dair kural ve içtihatların oluşturulduğu uluslararası yapılara düzenli ve etkili katılım, ülkemiz menfaatine uygun düzenlemeler yapılması ve dünya kamuoyunun ülkemize yaklaşımını müspet etkileyecektir.

Ek 4-54/54

Çalıştay masalarındaki katılımcı girdilerini içeren ek olup Bilgi Güvenliği Derneği görüşleri değildir. Görüş çeşitliliğinin gözlenmesi adına ayrıca ek olarak sunulmuştur.