KAMU KURUMLARINDA SİBER GÜVENLİK ve TÜRKİYE'NİN TOPLUMSAL MAHREMİYETİ 2025 DURUM RAPORU

Bu raporun amacı, Türkiye'deki kamu kurumlarının siber güvenlik durumunu değerlendirmek, mevcut tehdit ve açıkları tespit etmek, gerekli önlemleri belirlemek ve bilgi güvenliğini güçlendirmeye yönelik somut öneriler sunmaktır. Ayrıca, siber saldırıların toplumsal, ekonomik ve siyasi etkilerini analiz ederek kamu hizmetlerinin sürekliliği için stratejik bir yol haritası oluşturmayı hedeflemektedir.

EDİTÖR
PROF.DR.ÖZCAN GÜNGÖR
AR-GE ve PARTİ İÇİ EĞİTİM OKULU BAŞKANI

DURUM RAPORLARI SERİSİ
SERİ 2

A PARTİ
ANAHTAR PARTİ
AR-GE ve PARTİ İÇİ EĞİTİM OKULU BAŞKANLIĞI

Anahtar Parti Yayınları | *Anahtar Party Publications*
Hilal Mah. Rabindranath Tagore Cd. No:66, 06550 Ankara, Türkiye
Web: https://anahtarparti.org | eposta: arge@anahtarparti.org

Yayın Adı	*Publication Name*	: **Kamu Kurumlarında Siber Güvenlik ve Türkiye'nin Toplumsal Mahremiyeti** *Cyber Security in Public Institutions and Social Privacy in Türkiye*
Yayın No	*Publication Number*	: 3
Yayın Serisi	*Publication Series*	: AR-GE Durum Raporları Serisi *R&D Situation Report Series*
Seri No	*Serial Number*	: 2

Editör	*Editor*	: **Prof. Dr. Özcan Güngör**
Unvanı	*Title*	: Hacı Bayram Veli Üniversitesi Öğretim Üyesi/ Anahtar Parti Genel Başkan Yardımcısı AR-GE ve Parti İçi Eğitim Okulu Başkanı *Academic Member of the Haci Bayram Veli University/ Anahtar Party Deputy Chairperson Chair of R&D and Party Academy*
Kurumu	*Affiliation*	: Ankara Hacı Bayram Veli Üniversitesi/ Anahtar Parti Genel Merkez AR-GE Başkanlığı *Ankara Hacı Bayram Veli University/ Anahtar Party Department of R&D*

Sertifika No	*Certificate Number*	: 78848
Telif	*Copyright*	: Anahtar Parti Yayınları | *Anahtar Party Publications*
Yayım Tarihi	*Publication Date*	: 2 Ocak 2025 | *January 2nd, 2025*
Yayım Yeri	*Place of Publication*	: Ankara, TÜRKİYE
Yayın Türü	*Publication Type*	: Editoryal Rapor | *Editorial Report*
Yayın Dili	*Language*	: Türkçe | *Turkish*
Yayımlandığı Ortam	*Publishing Format*	: PDF | *PDF*
Ebat	*Dimensions*	: 15.5x23.5 cm
Baskı Sayısı	*Edition*	: 2
Sayfa Sayısı	*Page Count*	: 32
Atıf Bilgisi	*Cite as*	: Güngör, Özcan (ed.), Kamu Kurumlarında Siber Güvenlik Ve Türkiye'nin Toplumsal Mahremiyeti. Anahtar Parti Yayınları, 2025.

Kapak Tasarım	*Cover Design*	: *AG graphics design*
Dizgi ve Mizanpaj	*Typesetting and Layout*	: Burak AYTEKİN
Baskı Matbaası	*Printing Press*	:

İÇİNDEKİLER

Yönetici Özeti

Bu rapor, Türkiye'deki kamu kurumlarının siber güvenlik durumu, mevcut güvenlik açıkları, alınan önlemler ve geleceğe yönelik stratejiler üzerine kapsamlı bir değerlendirme sunmaktadır. Türkiye'nin artan dijitalleşme süreci ve siber tehditlerin çeşitliliği göz önüne alındığında, kamu kurumlarının bilgi güvenliğini sağlamak ve toplumsal güveni korumak için daha güçlü ve yenilikçi politikalar geliştirilmesi gerekmektedir.

Mevcut Durum: Kamu Kurumlarının Siber Güvenlik Durumu

Türkiye'de kamu kurumlarının siber güvenlik altyapıları hızla gelişmektedir; ancak daha karmaşık hale gelen tehditler, sistemlerde ciddi açıklar yaratmaktadır. Öne çıkan sorunlar:

Teknolojik Eksiklikler: Güncel olmayan yazılımlar, zayıf şifreleme yöntemleri ve yetersiz altyapı.

Kurumsal Zafiyetler: Çalışan farkındalığının düşük olması ve kurumlar arası güvenlik eşitsizlikleri.

Hacklenme Olayları: Kamu kurumlarına yönelik saldırılar arasında kişisel veri sızıntıları, fidye yazılımı saldırıları ve kritik altyapılara yönelik tehditler yer almaktadır.

Örnekler:

Sağlık Bakanlığı: Kişisel sağlık bilgileri hedef alınmıştır.

MERNİS ve PolNet: Kapsamlı veri sızıntıları yaşanmıştır.

Savunma Sanayi Şirketleri: AR-GE verilerinin sızdırılması hedeflenmiştir.

Mevcut Siber Güvenlik Politikaları ve Hukuki Çerçeve

Türkiye, **Kişisel Verilerin Korunması Kanunu (KVKK)** ve **ISO 27001** gibi yasal düzenlemelerle bilgi güvenliği için güçlü bir çerçeve oluşturmuştur. Ancak, bu düzenlemelerin etkinliği, uygulamadaki boşluklar nedeniyle tam anlamıyla sağlanamamaktadır. Öneriler:

1. **Yasal Uyumluluk:** Kamu kurumlarının KVKK ve uluslararası standartlara uyum düzeylerinin artırılması.
2. **Cezai Yaptırımlar:** Siber suçlara yönelik daha caydırıcı yaptırımların uygulanması.
3. **Denetim Mekanizmaları:** Siber güvenlik önlemlerinin düzenli olarak denetlenmesi.

Risk Yönetimi ve Tehdit Modelleme

Türkiye'deki kamu kurumlarına yönelik başlıca tehditler:

Hacker Grupları: Kamu hizmetlerini aksatma ve veri çalma girişimleri.

Siber Terörizm: Enerji ve sağlık gibi kritik altyapıların hedef alınması.

Devlet Destekli Saldırılar: Diplomatik ve ekonomik çıkarları hedefleyen saldırılar.

Sosyal Mühendislik: Çalışanları hedef alan kimlik avı saldırıları.

Öneriler:

Risk Analizi: ISO 27005 gibi standartlarla tehditlerin düzenli olarak değerlendirilmesi.

Tehdit İstihbaratı: Ulusal ve uluslararası işbirliğiyle tehditlerin erken tespit edilmesi.

Bilgi Güvenliği Stratejileri

Türkiye'nin bilgi güvenliğini artırmak için izlenmesi gereken stratejiler:

1. **Güvenlik Protokolleri:** Erişim kontrolü, veri şifreleme ve acil durum planlarının oluşturulması.
2. **Çalışan Eğitimi:** Kamu personelinin düzenli siber güvenlik eğitimlerine tabi tutulması.
3. **Denetim ve İzleme:** Güvenlik önlemlerinin etkinliğini artırmak için düzenli izleme ve raporlama.

Teknolojik Altyapı ve Yatırımlar

Türkiye'nin kamu kurumları, daha güçlü bir siber güvenlik altyapısına ihtiyaç duymaktadır:

Altyapı Yatırımları: Gelişmiş güvenlik duvarları, şifreleme protokolleri ve yedekleme sistemlerinin güçlendirilmesi.

Bulut Güvenliği: Veri güvenliğini sağlamak için bulut tabanlı sistemlerde şifreleme ve erişim kontrolü uygulanması.

Bütçeleme: Siber güvenlik yatırımlarına ayrılan bütçenin artırılması ve etkin kullanılmasının sağlanması.

Kriz Yönetimi ve Olay Müdahale Planları

Siber saldırı sonrası etkili bir müdahale süreci, kamu kurumlarının güvenliğini yeniden sağlamada kritik bir role sahiptir:

1. **Hızlı Tespit ve İzolasyon:** Saldırıya uğrayan sistemlerin hızla izole edilmesi.
2. **Olay Yönetimi:** Saldırıların etkilerinin analiz edilmesi ve sistemlerin geri yüklenmesi.
3. **Şeffaflık ve İletişim:** Kamuoyunun doğru bilgilendirilmesi.
4. **Felaket Kurtarma Planları:** Yedekleme ve veri kurtarma süreçlerinin hızla devreye alınması.

Ulusal ve Uluslararası İşbirlikleri

Türkiye, siber güvenlik kapasitesini artırmak için hem ulusal hem de uluslararası işbirliklerini geliştirmelidir:

Özel Sektör İşbirliği: Güçlü teknolojik altyapılar ve uluslararası standartların uygulanması.

Uluslararası İttifaklar: NATO ve diğer küresel organizasyonlarla bilgi paylaşımı ve ortak savunma stratejilerinin geliştirilmesi.

Sonuç ve Öneriler

Türkiye'nin kamu kurumlarının siber güvenlik seviyesinin artırılması için kapsamlı bir stratejiye ihtiyaç duyulmaktadır:

1. **Mevzuatın Güçlendirilmesi:** KVKK ve diğer düzenlemelerin etkin uygulanması.
2. **Altyapı Yatırımları:** Modern ve dayanıklı teknolojik altyapıların kurulması.
3. **Eğitim ve Farkındalık:** Çalışanların bilgi güvenliği bilincinin artırılması.
4. **Uluslararası İşbirlikleri:** Küresel siber tehditlere karşı ortak stratejiler geliştirilmesi.

Bu önerilerin hayata geçirilmesi, Türkiye'nin dijital dönüşümünü güvenli ve sürdürülebilir bir şekilde gerçekleştirmesine katkı sağlayacaktır.

Kamu Kurumlarında Siber Güvenlik ve Türkiye'nin Toplumsal Mahremiyeti

Giriş

Bu rapor, Türkiye'nin siber güvenlik stratejilerinin, yasal düzenlemelerinin ve alınan önlemlerinin analiz edilmesiyle, kamu kurumlarının siber güvenlik açıklarını kapatmaya yönelik somut adımlar atılmasını teşvik etmeyi amaçlamaktadır. Devletin siber güvenlik alanındaki kapasitesinin artırılması, yerel ve küresel tehditlere karşı dirençli bir yapı oluşturulmasını sağlamak için kritik öneme sahiptir.

Amaç: Bu raporun temel amacı, Türkiye'deki kamu kurumlarının siber güvenlik durumu hakkında kapsamlı bir değerlendirme yapmaktır. Özellikle son yıllarda artan siber saldırılar göz önünde bulundurularak, kamu kurumlarının mevcut siber güvenlik altyapıları, savunma stratejileri ve potansiyel zafiyetleri analiz edilecektir. Raporda, kamu kurumları için geçerli olan siber güvenlik riskleri ve bu risklere karşı alınması gereken önlemler üzerinde durulacaktır. Ayrıca, siber saldırıların toplumsal, ekonomik ve siyasi etkileri de tartışılacak ve bu bağlamda kamu hizmetlerinin sürekliliği için gerekli önlemler önerilecektir.

Kapsam: Raporda, Türkiye'deki kamu kurumları ve devlet hizmetlerinin siber güvenlik düzeylerinin değerlendirilmesi ile birlikte, devletin mevcut bilgi güvenliği politikalarının etkinliği analiz edilecektir. Özellikle kritik kamu hizmetleri sunan sektörler (örneğin sağlık, enerji, eğitim, finans) hedef alınarak, her bir sektörün karşılaştığı güvenlik tehditlerine odaklanılacaktır. Ayrıca, kamu kurumlarının mevcut güvenlik altyapıları ve süreçleri üzerinde de durulacak, kurumsal güvenlik yönetimi açısından karşılaşılan zorluklar ve boşluklar tartışılacaktır. Son olarak, kamu kurumları ve devlet hizmetlerinin siber saldırılara karşı korunmasına yönelik stratejiler geliştirilerek, bu stratejilerin nasıl daha etkili hale getirilebileceği konusunda öneriler sunulacaktır.

Türkiye'nin Siber Güvenlik Stratejileri: Hükümetin Bilgi Güvenliği Politikaları, Yasal Düzenlemeler ve Önlemler

Türkiye'de çeşitli zamanlarda korsanlar ve hacker grupları tarafından hedef alınan ve hacklenen birçok kamu kurumu ve özel sektör kuruluşu olmuştur. Bu saldırılar, genellikle kişisel verilerin sızdırılması, kritik sistemlere zarar verilmesi veya devletin iç işleyişine dair bilgiler edinilmesi amacıyla gerçekleştirilmiştir.

Yıllara göre öne çıkan saldırılar ve hedefler aşağıda sunulmaktadır:

1. 2016 ve Öncesi: DDoS Saldırılarının Yükselişi

2015 ve 2016 yıllarında kamu kurumları ve bankacılık sistemlerine yönelik yoğun **DDoS (Dağıtık Hizmet Engelleme)** saldırıları gerçekleştirilmiştir.

Amaç: Bankacılık ve kamu kurumlarını çalışamaz hale getirerek işleyişi durdurmak.

Etkiler: Birçok banka ve devlet kurumu bu saldırılar karşısında savunmasız kalarak geçici süreyle devre dışı kalmıştır.

2. 2020: Pandemi Döneminde Phishing ve Fidye Yazılımı Saldırıları

Pandemi döneminde dijital altyapının önemi artmış ve siber saldırılar da bu altyapılar üzerinden yoğunlaşmıştır.

Hedef: Sağlık ve eğitim sektörü.

Saldırı Türleri:

Phishing (Oltalama): Sahte e-postalar ve siteler üzerinden kullanıcı bilgilerinin ele geçirilmesi.

Fidye Yazılımı: Kritik sistemlerin şifrelenerek fidye talep edilmesi.

3. 2022: Phishing Saldırıları ve Veri Sızıntılarının Artışı

Bu yıl, önceki yıllara kıyasla **phishing (oltalama)** saldırılarında ve **veri sızıntısı girişimlerinde** belirgin bir artış yaşanmıştır.

USOM Verileri: 72 binden fazla oltalama girişimi engellenmiş, kritik altyapılara yönelik saldırılara karşı önlemler alınmıştır.

4. 2023: Siber Saldırılarda %30 Artış

2023 yılında siber saldırılar %30 oranında artış göstermiştir.

Hedefler: Kamu kurumları (%99), savunma sanayi şirketleri, özel bankalar ve holdingler.

Phishing Saldırıları: 105 binden fazla oltalama girişimi raporlanmıştır.

5. 2024 (İlk Çeyrek): Artan Saldırı Hacmi

USOM, 2024 yılının ilk üç ayında 37.600 siber saldırıyı engellediğini bildirmiştir.

Hedefler: Phishing saldırıları, zararlı yazılım girişimleri ve bankacılık işlemleri.

Amaç: Veri çalma, kritik sistemleri devre dışı bırakma.

En Çok Hedef Alınan Kamu Kurumları ve Saldırı Türleri

E-devlet Kapısı (turkiye.gov.tr):

Saldırı Türleri: DDoS saldırıları, kimlik avı girişimleri.

Enerji ve Tabii Kaynaklar Bakanlığı:

Saldırı Türleri: Enerji altyapılarına yönelik saldırılar.

Sağlık Bakanlığı ve Hastaneler:

Saldırı Türleri: Kimlik avı girişimleri.

Merkezi Nüfus İdaresi Sistemi (MERNİS):

Saldırı Türleri: Veri sızıntısı girişimleri.

Ulaştırma ve Altyapı Bakanlığı:

Saldırı Türleri: İnternet altyapılarına ve iletişim ağlarına yönelik saldırılar.

Millî Eğitim Bakanlığı:

Saldırı Türleri: Uzaktan eğitim platformları (EBA gibi).

Bankacılık Düzenleme ve Denetleme Kurumu (BDDK):

Saldırı Türleri: Bankacılık sistemlerini hedef alan oltalama girişimleri.

Adalet Bakanlığı ve E-adalet Sistemi:

Saldırı Türleri: Hukuki bilgi sızıntıları, kimlik avı girişimleri.

Savunma Sanayii Başkanlığı:

Saldırı Türleri: Savunma projelerine yönelik siber casusluk.

Belediyeler:

Saldırı Türleri: Su ve ulaşım sistemlerine yönelik saldırılar.

Aşağıda, Türkiye'de çeşitli hackleme olaylarına uğrayan bazı kurumlar yer almaktadır:

1. Sağlık Bakanlığı

2016: Sağlık Bakanlığı'nın bilgi sistemlerine yönelik büyük bir siber saldırı gerçekleşmiştir. Hackerlar, Türkiye'nin sağlık verilerini içeren kritik sisteme sızmış ve kişisel sağlık bilgileri ile veritabanları hedef alınmıştır.

2019: Bakanlık, bazı sistemlerinin hacker grupları tarafından ele geçirildiğini ve önemli verilerin sızdırıldığını açıklamıştır.

2. T.C. İçişleri Bakanlığı

İçişleri Bakanlığı'nın bazı alt birimlerinin veritabanları siber saldırılara uğramıştır. Bu saldırılar, çoğunlukla devletin yönetim sistemleri ve güvenlik verilerinin hedef alındığı, sistemlerdeki açıklar aracılığıyla yapılmıştır. **2024 yılında PolNet veri sızıntısı** konusunda Gazeteci İbrahim Haskoloğlu tarafından X üzerinden yapılan paylaşımda, *"Hackerlar, Emniyetin kullandığı POLNET üzerinden veri sızıntısı başlattıklarını duyurdu. Kontrol ettiğimde bu senenin başında aldığım telefon numarasından ortaokulda aldığım ilk numaraya kadar her şey çıkıyor. 3 gün önce yeni bir numara aldıysanız maalesef o bile çıkıyor."* ifadesi yer aldı.

3. Türkiye Elektrik Dağıtım A.Ş. (TEDAŞ)

TEDAŞ'a ait sistemler, 2016 yılında büyük bir siber saldırıya uğramıştır. Bu saldırı, enerji altyapısına zarar verme amacıyla gerçekleştirilmiş ve birçok kritik sistemin ele geçirilmesine yol açmıştır.

4. Millî Savunma Bakanlığı

Millî Savunma Bakanlığı'na ait çeşitli dijital sistemler de defalarca hedef olmuştur. Hacker grupları, askeri verilere ve savunma sistemlerine yönelik saldırılar gerçekleştirmiştir. Özellikle **2015 ve 2016 yıllarında** bu tür saldırılar sıkça gündeme gelmiştir.

5. Türk Telekom

2019 yılında, Türk Telekom'un bazı sistemlerine siber saldırılar yapılmış ve hackerlar tarafından bazı verilerin ele geçirildiği bildirilmiştir. Bu saldırılar, Türkiye'nin internet altyapısına yönelik tehditler oluşturmuştur.

6. TCDD (Türkiye Cumhuriyeti Devlet Demiryolları)

TCDD'nin veritabanlarına ve yolcu bilgilendirme sistemlerine yönelik çeşitli siber saldırılar gerçekleşmiştir. Bu saldırılar, sistemlere zarar verilmesi ve bazı bilgilerin ele geçirilmesi amacıyla yapılmıştır.

7. Türkiye Cumhuriyet Merkez Bankası (TCMB)

Merkez Bankası'nın sistemlerine yönelik saldırılar, siber tehditler arasında en ciddi olanlardan biri olmuştur. Bankanın finansal verilerine ve işlemlerine yönelik saldırılar gerçekleştirilmiş, bazı veriler sızdırılmıştır.

8. Yüksek Seçim Kurulu (YSK)

YSK, 2019 seçimleri öncesi, siber saldırılara maruz kalmıştır. Seçim sonuçlarıyla ilgili güvenliği sağlamak için çeşitli önlemler alınmasına rağmen, saldırılar sonuçların manipüle edilmesi ve verilerin ele geçirilmesi amaçlamıştır.

9. E-devlet Sistemi

E-devlet sistemi de hacker grupları tarafından hedef alınmış ve sistemdeki kullanıcı bilgileri ve devlet hizmetlerine erişim hakkı tehlikeye girmiştir. Türkiye'deki birçok e-devlet uygulamasının hacklenmesi, çeşitli güvenlik açıklarının ortaya çıkmasına neden olmuştur.

10. ÖSYM (Ölçme, Seçme ve Yerleştirme Merkezi)

2017 yılında ÖSYM, siber saldırılara uğramış ve bazı sınav sonuçları üzerinde değişiklik yapabilecek şekilde sistemlere giriş yapılmıştır. Bu tür saldırılar, sınav sisteminin güvenliğini tehdit eden unsurlar oluşturmuştur. 2024 yılında YKS, ALES, DGS, YÖKDİL sınavlarında alınan tüm sonuçların verileri sızdırıldı.

11. Bankacılık ve Finans Kuruluşları

Türkiye'deki birçok banka ve finansal kurum, hem iç hem de dış tehditlerle karşı karşıya kalmış, hacker grupları çeşitli zamanlarda bankaların ödeme sistemlerine saldırılar gerçekleştirmiştir. Özellikle **2017 ve 2018 yıllarında** siber saldırılar finans sektörü için önemli bir tehdit olmuştur.

12. Kamuya Ait Veri Tabanları ve Eğitim Kurumları

Türkiye'deki bazı eğitim kurumları ve kamuya ait veri tabanları, çeşitli siber saldırılara uğramış ve kritik bilgilere erişilmiştir. Bu saldırılar çoğunlukla kişisel verilerin sızdırılması, diplomaların ve akademik belgelerin manipüle edilmesi gibi sonuçlar doğurmuştur.

13. Türk Hava Yolları (THY)

THY, bazı siber saldırılara maruz kalmış ve şirketin uçuş sistemlerine yönelik saldırılar, müşteri bilgilerinin tehlikeye girmesine neden olmuştur. Bu saldırılar, hem uçuş güvenliğini hem de yolcu verilerini tehdit etmiştir.

14. Diyanet İşleri Başkanlığı

2020 yılında Diyanet İşleri Başkanlığı'nın sistemine siber saldırı yapılmış ve çeşitli veriler sızdırılmıştır. Diyanet İşleri'nin dijital sistemlerine yönelik tehditler, dini organizasyonlara ait hassas verilerin güvenliğini riske atmıştır.

Türkiye'de Siber Saldırıların Hedefi: Savunma Sanayi ve Özel Şirketler

Türkiye'de siber saldırılar, ulusal güvenlik ve ekonomik değerlerin korunması açısından stratejik öneme sahip savunma sanayi şirketleri ile özel sektör kuruluşlarını hedef almaktadır. Özellikle stratejik ürün ve teknolojik veri geliştiren şirketler, Ar-Ge verilerinin sızdırılması amacıyla sürekli saldırılara maruz kalmaktadır. Bu durum, şirket yönetimleri ve Savunma Sanayii Başkanlığı tarafından raporlanmıştır. Siber saldırılara maruz kalan kurum ve kuruluşlar aşağıda sıralanmıştır:

1. En Çok Siber Saldırıya Maruz Kalan Savunma Sanayi Şirketleri

ASELSAN

Hedef: Elektronik sistemler ve iletişim teknolojileri alanında savunma sanayisine yaptığı katkılar.

Siber Güvenlik Önlemleri: Şirket, hassas teknolojik verilerin korunması için siber güvenlik altyapısını sürekli güncellemektedir.

HAVELSAN

Hedef: Bilgi ve iletişim teknolojileri, siber güvenlik çözümleri.

Siber Güvenlik Önlemleri: Şirket, altyapısını güçlendirmek için büyük ölçekli yatırımlar yapmaktadır.

BAYKAR Teknoloji

Hedef: İHA ve SİHA teknolojilerinde lider bir üretici olması nedeniyle kritik teknolojik verileri.

Siber Güvenlik Önlemleri: Şirket, saldırılara karşı sürekli önlemler almakta ve altyapısını güncel tutmaktadır.

TAI (Türk Havacılık ve Uzay Sanayii)

Hedef: Hava platformları ve uzay teknolojileri alanındaki stratejik veriler.

Siber Güvenlik Önlemleri: Şirket, savunma sistemlerini sürekli olarak yenilemekte ve güncellemektedir.

ROKETSAN

Hedef: Füze ve roket teknolojilerinde geliştirdiği kritik veriler.

Siber Güvenlik Önlemleri: Şirket, veri koruması için siber güvenlik yatırımlarını artırmıştır.

2. En Çok Siber Saldırıya Maruz Kalan Özel Şirketler

Koç Holding

Hedef: Teknoloji iştirakleri olan KoçSistem ve KoçDigital üzerinden stratejik AR-GE çalışmaları.

Netaş

Hedef: Savunma sanayiyle ilgili AR-GE verilerinin ele geçirilmesi.

Turkcell ve Türk Telekom

Hedef: Teknolojik altyapılarında kesinti oluşturma ve iletişim sistemlerini devre dışı bırakma.

Bankacılık Sektörü (Örneğin, Ziraat Bankası ve Diğer Finans Kurumları)

Hedef: Kimlik avı (phishing) ve fidye yazılımı saldırılarıyla müşteri bilgileri ve finansal sistemler.

Perakende ve E-Ticaret Şirketleri (Trendyol, Hepsiburada, N11 vb.)

Hedef: Müşteri veri tabanlarının ele geçirilmesi ve ticari işlemler üzerinde kontrol sağlama.

Bu örnekler, Türkiye'deki birçok kamu ve özel sektör kuruluşunun, siber güvenlik açıkları nedeniyle hackerlar ve korsanlar tarafından hedef alındığını ve bu durumun ciddi toplumsal ve ekonomik etkiler yaratabileceğini göstermektedir. Türkiye'nin siber güvenlik altyapısının güçlendirilmesi ve siber tehditlere karşı daha dayanıklı bir sistemin kurulması gerekliliği, her geçen gün daha fazla önem kazanmaktadır.

1- Türkiye'nin Mevcut Siber Güvenlik Stratejileri

Türkiye, siber güvenlik alanında önemli adımlar atmış ve stratejik bir yaklaşım benimsemiştir. Ülkede siber güvenlik stratejilerinin temelini oluşturan ilkeler arasında ulusal güvenliği sağlama, ekonomik ve toplumsal süreçlerin güvenliğini temin etme ve siber tehditlerle mücadele etme yer almaktadır. Hükümet, çeşitli güvenlik önlemleriyle kamu kurumlarının siber saldırılara karşı daha güçlü hale gelmesini amaçlamaktadır. Bu stratejiler arasında, ulusal bir siber güvenlik merkezi kurma, siber güvenlik eğitimleri ve farkındalık artırma faaliyetleri ve siber kriz yönetim planları bulunmaktadır.

Bununla birlikte, Türkiye'nin siber güvenlik stratejileri büyük oranda **ulusal savunma** ve **devletin kritik altyapılarının korunması** üzerine yoğunlaşmaktadır. Türkiye'nin **Siber Güvenlik Stratejisi 2016-2019** belgesi, devletin, kamu ve özel sektörlerin işbirliği içinde siber güvenlik alanında daha sağlam bir yapı oluşturması gerektiğini vurgulamaktadır. Ayrıca, bu strateji ile Türkiye'nin **siber güvenlik kapasitesinin artırılması**, **yenilikçi siber teknolojilerin kullanılması** ve **yeni nesil tehditlere karşı etkili bir savunma sistemi oluşturulması** hedeflenmiştir. Fakat gelinen noktada alınması istenilen veya alınan tedbirlerin yeterli olmadığı görülmektedir.

Yasal Düzenlemeler ve Hukuki Çerçeve

Türkiye, siber güvenlik ve bilgi güvenliği alanında güçlü bir hukuki altyapı oluşturmayı hedeflemiş ve bu bağlamda çeşitli yasal düzenlemeler geliştirmiştir. Bunların başında, 2016 yılında yürürlüğe giren **Kişisel Verilerin Korunması Kanunu (KVKK)** yer almaktadır. Bu kanun, hem kamu kurumları hem de özel sektör için kişisel verilerin korunmasını sağlamak amacıyla güçlü bir düzenleme ortaya koymaktadır. KVKK, veri güvenliği konusunda önemli bir adım olmakla birlikte, tüm siber güvenlik politikalarının bir parçası olarak görülmelidir.

Bir diğer önemli yasal düzenleme ise **Elektronik Ticaretin Düzenlenmesi Hakkında Kanun** ve **Siber Güvenlik Yasası**dır. Bu yasalar, dijital ortamda güvenli iletişimi ve verilerin korunmasını sağlayacak bir çerçeve oluşturmuş, aynı zamanda kamu kurumlarının verilerini kötüye kullanımına karşı sağlam güvenlik önlemleri almayı zorunlu hale getirmiştir.

Ayrıca, Türkiye'nin **Siber Güvenlik Koordinasyon Kurulu** ve **Ulusal Siber Olaylara Müdahale Merkezi (USOM)** gibi kuruluşlar, devletin siber güvenlik stratejilerinin hayata geçmesi için önemli bir rol oynamaktadır. USOM, kamu kurumlarının siber güvenlik zafiyetlerini izler ve siber saldırı anında müdahale eder. Bunun dışında, Türkiye'nin NATO ve diğer uluslararası güvenlik işbirliklerine katılımı, Türkiye'nin küresel siber tehditlere karşı işbirliğini artırmaktadır.

Siber Güvenlik Önlemleri

Hükümetin siber güvenlik politikaları, sadece yasal düzenlemelerle sınırlı kalmamaktadır. Türkiye, kamu kurumları için **siber güvenlik altyapısının güçlendirilmesi** adına çeşitli teknik önlemler de almaktadır. Bu önlemler arasında, **güvenlik duvarları (firewall)**, **saldırı tespit ve engelleme sistemleri (IDS/IPS)**, **şifreleme teknikleri**, ve **kapsamlı veri güvenliği** sağlamak amacıyla uygulanan yöntemler yer almaktadır. Bunun yanı sıra, kamu kurumlarının **bilgi güvenliği yönetim sistemleri** oluşturarak, güvenlik seviyelerinin sürekli denetlenmesi sağlanmaktadır.

Türkiye, ayrıca **siber saldırılara karşı siber savunma takımlarının oluşturulması**, **siber tehdit istihbaratı paylaşımı**, ve **siber güvenlik tatbikatları** ile ulusal savunma kapasitesini güçlendirmeyi amaçlamaktadır. Bu stratejiler, Türkiye'nin bilgi güvenliği alanındaki kapasitesini artırırken, aynı zamanda devletin ve kamu kurumlarının savunma yeteneklerini sürekli olarak geliştirmeyi hedeflemektedir. Bunca önleme rağmen başarılamayan sızıntıların devam etmektedir.

2. Türkiye'deki Kamu Kurumlarının Bilgi Güvenliği Durumu

Mevcut Durum Analizi:
Kamu Kurumlarının Siber Güvenlik Altyapıları, Güvenlik Açıkları ve Önceki Hacklenme Olaylarının Analizi

Türkiye'deki kamu kurumlarının siber güvenlik altyapıları, genellikle giderek artan dijitalleşme süreçlerine paralel olarak gelişmektedir, ancak her geçen gün daha sofistike hale gelen siber tehditler karşısında bazı açıklar ve eksiklikler ortaya çıkmaktadır. Kamu kurumları, özellikle kritik altyapı sağlayan sektörlerde (sağlık, enerji, finans, kamu hizmetleri) siber güvenlik önlemlerini güçlendirme yönünde ilerlemeler kaydetmiş olsa da, daha geniş bir yaklaşım ve kapsamlı bir güvenlik politikası eksikliği gözlemlenmektedir.

Birçok kamu kurumu, veri güvenliği ve siber savunma için temel güvenlik duvarları (firewall) ve antivirüs yazılımları kullanmakta, ancak bu yöntemler günümüzün gelişmiş siber saldırıları karşısında yeterli olmayabilmektedir. Birçok kurumda siber güvenlik için yapılan yatırımlar hala sınırlıdır, siber güvenlik kültürü henüz her seviyede yerleşmemiştir ve bu durum, kurumların daha büyük saldırılara karşı savunmasız olmasına neden olmaktadır. Ayrıca, çeşitli kamu kurumlarında bilgi güvenliği uygulamaları birbiriyle tutarsızdır, bu da veri kaybı ve sistemin çökmesi gibi felakete yol açabilecek riskleri artırmaktadır.

Birçok kamu kurumu, *kapsamlı siber güvenlik yönetim sistemlerine* sahip olsa da, bunlar genellikle yeterli düzeyde güncellenmemekte ve geniş bir tehdit yelpazesine karşı etkili olamamaktadır. Ayrıca, bazı kamu kurumları daha eski altyapılara dayalı çalışmakta olup, bu durum siber tehditler karşısında ciddi zafiyetlere yol açmaktadır.

Riskler ve Zafiyetler:
Kamu Kurumlarında Karşılaşılan Bilgi Güvenliği Riskleri, Devletin ve Kamu Sektörünün Siber Tehditlere Karşı Savunmasız Noktaları

Türkiye'deki kamu kurumları, siber tehditlere karşı birçok risk ve zafiyet ile karşı karşıya kalmaktadır. Bunların başında **yazılım güncellemeleri ve yamalarının zamanında yapılmaması**, **zayıf şifreleme protokollerinin kullanımı**, **sosyal mühendislik saldırılarına karşı zayıf savunmalar**, **kurumlar arası veri paylaşımı sırasında güvenlik önlemlerinin yetersizliği** ve **insan faktörü** gibi sorunlar yer almaktadır. Kamu kurumları, kişisel verilerin korunmasına dair yasal düzenlemelere uymakta zorlanmakta ve sistematik denetim eksiklikleri yaşanmaktadır.

Veri güvenliği riskleri kamu sektöründe büyük bir tehdit oluşturuyor. Kurumlar arasındaki veri paylaşımı sırasında, verilerin şifrelenmeden iletilmesi veya depolanması, büyük ölçüde güvenlik açığına yol açmaktadır. Ayrıca, bazı kurumlarda **sistemsel zafiyetler** nedeniyle veritabanlarına izinsiz erişim mümkün olabilmektedir.

İç tehditler de siber güvenlik zafiyetlerine yol açmaktadır. Kamu kurumlarında çalışanların, özellikle de düşük güvenlik bilinci ile çalışmaları, siber güvenlik tehditlerine karşı kurumları savunmasız bırakmaktadır. Buna ek olarak, **sosyal mühendislik saldırıları** gibi teknik olmayan saldırılar, şifrelerin çalınması veya yetkisiz erişimlerin sağlanması gibi durumlara yol açabilmektedir.

Hacklenme Olayları:
Önceki Hacklenme Olaylarının Değerlendirilmesi ve Bunların Sonuçları

Son yıllarda Türkiye'de kamu kurumlarına yönelik birçok önemli hacklenme olayı yaşanmıştır. Bu saldırılar, genellikle kritik kamu hizmetlerinin felç olmasına ve büyük veri ihlallerine yol açmıştır. Özellikle **sağlık sektörüne ait verilerin** çalınması, **bankacılık sektörü ve kamu finansal işlemlerine yönelik saldırılar** ve **kamu kurumları veri tabanlarına** yönelik siber saldırılar büyük yankı uyandırmıştır.

Örneğin, **sağlık kurumlarına yönelik saldırılar**, hastaların kişisel bilgilerini hedef almış, bu bilgilerin çalınması sağlık hizmetlerinin verimli şekilde sunulmasına engel olmuştur. Bu tür saldırılar, kurumların sadece maddi kayıplar yaşamasına değil, aynı zamanda kamu güveninin sarsılmasına da yol açmaktadır.

Başka bir örnek ise **Türkiye'deki kamu bankalarına yönelik gerçekleştirilen siber saldırılardır**. Bu saldırılar, finansal sistemde güvenlik açıkları oluşturmuş ve çeşitli bankacılık hizmetlerinin askıya alınmasına sebep olmuştur. Bu tür saldırıların sonuçları, yalnızca kamu kurumlarına değil, aynı zamanda devletin genel güvenliği ve ekonomisi için de ciddi tehditler oluşturabilmektedir.

Hacklenme olaylarının sonuçları, sadece anlık veri kayıplarına yol açmakla kalmayıp, uzun vadeli **güven kaybı**, **hukuki ve düzenleyici sorunlar** ve **toplumun güvenlik algısının zedelenmesi** gibi önemli olgulara da neden olmuştur. Bu olaylar, daha güçlü ve sistematik bir siber güvenlik stratejisinin gerekliliğini bir kez daha gözler önüne sermektedir.

Kurumlar Arası Güvenlik Farklılıkları:
Farklı Kamu Kurumlarının Bilgi Güvenliği Seviyeleri ve Bu Seviyedeki Eşitsizlikler

Türkiye'deki kamu kurumları arasındaki **bilgi güvenliği seviyeleri** büyük farklılıklar göstermektedir. **Büyük ve merkezi kurumlar**, genellikle siber güvenlik altyapılarına daha fazla yatırım yapmış ve gelişmiş sistemler kullanmaktadır. Örneğin, **banka ve finans sektörü gibi kritik alanlardaki kamu kurumları**, siber güvenlik konusunda daha sofistike ve gelişmiş güvenlik önlemleri almaktadır.

Ancak, **yerel yönetimler ve küçük kamu kuruluşları** arasında bu alanda ciddi eşitsizlikler bulunmaktadır. Bu kurumlar genellikle daha az kaynak ayırmakta ve altyapılarını yeterince güncelleyememektedir. Bu durum, düşük güvenlik önlemleriyle çalışan kurumların, siber saldırılara karşı daha savunmasız olmalarına neden olmaktadır.

Ayrıca, **yasal ve düzenleyici standartlara uyum** konusunda da kurumlar arasında büyük farklılıklar bulunmaktadır. Bazı kurumlar, **KVKK** ve **siber güvenlik yasalarına** tam uyum sağlarken, diğer kurumlar bu yasaları yeterince uygulayamamaktadır. Bu durum, ulusal güvenliği tehdit edebilecek büyük bir boşluğa yol açmaktadır.

Sonuç olarak, Türkiye'deki kamu kurumlarında, siber güvenlik konusunda eşit bir güvenlik seviyesi sağlanması için acil önlemler alınması gerekmektedir. Bu önlemler arasında, **yerel yönetimlerin ve küçük kurumların** siber güvenlik altyapılarına daha fazla yatırım yapmalarını teşvik etmek, **bilgi güvenliği farkındalığını artırmak** ve **kurumlar arasında bilgi paylaşımını artırmak** büyük önem taşımaktadır.

Bu noktada, **tek tip ve merkezi bir siber güvenlik stratejisi** oluşturulması ve kurumlar arasındaki eşitsizliklerin giderilmesi, Türkiye'nin genel siber güvenlik seviyesinin güçlendirilmesine katkı sağlayacaktır.

3- Bilgi Güvenliği Risk Yönetimi

Risk Analizi ve Değerlendirme Yöntemleri:
Kamu Kurumlarında Kullanılan Risk Analiz Metodolojileri

Kamu kurumlarında bilgi güvenliği risk analizi, genel olarak çeşitli metodolojilerle gerçekleştirilmekte olup, bunlar kurumların karşılaştığı tehditler, zafiyetler ve potansiyel etkileri değerlendirmek amacıyla kullanılır. Türkiye'deki kamu kurumlarında yaygın olarak kullanılan bazı **risk analiz metodolojileri** şunlardır:

ISO 27005:

Bu, uluslararası standartlara dayalı bir risk yönetim metodolojisidir ve kurumların siber güvenlik risklerini tanımlamalarına, değerlendirmelerine ve yönetmelerine yardımcı olur. Kamu kurumları, ISO 27005 standardını kullanarak bilgi güvenliği risklerini daha sistematik ve yapılandırılmış bir şekilde analiz ederler. Bu metodoloji, riskin etkisini ve olasılığını belirleyerek, uygun güvenlik önlemleri ve stratejileri geliştirmek için kullanılır.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation):

Bu metodoloji, özellikle kurumsal ortamlar için tasarlanmış bir risk değerlendirme çerçevesidir. Kamu kurumları OCTAVE yöntemini kullanarak, kritik varlıkları tanımlar, tehditleri belirler ve güvenlik zafiyetlerini gözden geçirir. Bu model, güvenlik önlemlerini ve savunmalarını belirlemek için organizasyonel hedefleri dikkate alır.

NIST (National Institute of Standards and Technology) Risk Yönetimi Çerçevesi:

NIST'in önerdiği risk analizi metodolojisi, özellikle devlet kurumları ve kritik altyapılar için yaygın olarak kullanılır. Bu çerçeve, risk değerlendirmesinin temel adımlarını belirler ve siber tehditlerin, zafiyetlerin, olasılıkların ve potansiyel etkilerin sistematik bir şekilde analiz edilmesini sağlar.

Kamu kurumları, bu metodolojilerle elde edilen bulguları kullanarak risklerini tanımlar, önceliklendirir ve bu risklere karşı etkili stratejiler geliştirir. Ancak, her metodolojinin uygulanması sürecinde, **kurumların siber güvenlik bilincini artırması**, **düzenli denetimler yapması** ve **yeni tehditlere karşı proaktif önlemler alması** gerekmektedir.

Tehdit Modelleme:
Türkiye'deki Kamu Kurumlarını Hedef Alabilecek Olası Siber Tehditler

Türkiye'deki kamu kurumlarını hedef alabilecek çeşitli **siber tehditler** mevcuttur. Bu tehditler, teknolojinin hızla gelişmesi, siber saldırı tekniklerinin evrilmesi ve kurumsal güvenlik açıklarının artması ile giderek daha karmaşık hale gelmektedir. Türkiye'deki kamu kurumlarına yönelik olası tehditler arasında şunlar öne çıkmaktadır:

Hacker Grupları ve Siber Suçlular:

Türkiye'nin kritik altyapılarını hedef alan hacker grupları, sıklıkla **siber suç** işleme amacı güder. Özellikle kamu hizmetlerinin verimli işleyişini bozmaya yönelik saldırılar, devletin dijital varlıklarını çalmaya veya şantaj yapmaya yönelik tehditler oluşturmaktadır. **Ransomware (fidye yazılımı)** gibi saldırılar, büyük ölçekli kamu kurumlarını tehdit etmekte ve önemli verilerin şifrelenmesi yoluyla işletme süreçlerini engellemektedir.

Siber Terörizm:

Kamu kurumlarına yönelik **siber terörizm** tehdidi, özellikle kritik altyapıların hedef alınması durumunda büyük tehlike oluşturabilir. Bu tür saldırılar, kamu güvenliğini tehdit edebilir, halkı paniğe sevk edebilir ve devletin toplumsal barışını bozabilir. Kritik enerji altyapıları, ulaşım sistemleri, sağlık ve iletişim ağları gibi devletin hassas alanları, siber teröristlerin hedeflerinden biri olabilir.

Devlet Destekli Saldırılar:

Türkiye'nin siber güvenlik stratejileri, özellikle **devlet destekli siber saldırılar** ile mücadeleye odaklanmaktadır. Bu tür saldırılar genellikle, **diplomatik ilişkiler**, **stratejik çıkarlar** ve **ekonomik avantajlar** amacı güden, belirli bir ülke ya da grup tarafından desteklenen hacker grupları tarafından gerçekleştirilmektedir. Bu tür saldırılar, kamu kurumlarının işleyişini bozmaya yönelik olabileceği gibi, devletin ulusal güvenliğine zarar verebilecek doğrudan tehditler oluşturabilir.

Sosyal Mühendislik ve Phishing Saldırıları:

İnsan faktörüne dayalı saldırılar, devletin siber güvenlik zafiyetlerini artıran önemli bir tehdit oluşturmaktadır. **Phishing** (oltalama) ve **sosyal mühendislik** saldırıları, kurum içi çalışanların kimlik bilgilerini çalmak amacıyla yapılmaktadır. Bu tür saldırılar, güvenlik zafiyetlerinden yararlanarak devlet verilerine izinsiz erişim sağlanmasına yol açabilir.

Zafiyet Tespiti:
Mevcut Güvenlik Önlemlerinin Etkili Olup Olmadığının Analizi
ve Kurumlar Arası Güvenlik Boşluklarının Ortaya Konması

Türkiye'deki kamu kurumlarının mevcut **güvenlik önlemleri**, genellikle altyapı, sistem güvenliği ve çalışan eğitimi gibi temel düzeydeki ihtiyaçları karşılama noktasında kalmaktadır. Ancak, daha geniş tehditlere karşı yeterince etkili değildir. **Zafiyet tespiti**, bu açıkları ve eksiklikleri belirlemenin temel aracıdır.

Teknolojik Zafiyetler:

Kamu kurumları arasında eski yazılımlar ve güncellenmemiş sistemler yaygın bir güvenlik açığı oluşturmaktadır. Yazılım güncellemelerinin geciktirilmesi ve zayıf şifreleme yöntemlerinin kullanılması, kurumların saldırılara karşı savunmasız kalmasına neden olmaktadır. Ayrıca, bazı kurumlarda **ağ güvenliği** konusunda ciddi zafiyetler mevcut olup, **güvenlik duvarları** ve **IDS/IPS sistemleri** gibi araçlar yeterince etkin kullanılmamaktadır.

İçsel Zafiyetler:

Kurum içi çalışanlar, siber güvenlik tehditlerinin en büyük kaynağı olabilir. **Çalışan eğitimi ve farkındalık eksiklikleri**, siber saldırılara karşı zayıf bir savunma oluşturur. **İç tehditler**, dışarıdan yapılan saldırılardan daha tehlikeli olabilir. Bunun yanında, **kurumlar arası veri paylaşımı** ve **işbirlikleri** sırasında yeterli güvenlik önlemleri alınmamaktadır, bu da büyük bir risk oluşturur.

Kurumlar Arası Güvenlik Boşlukları:

Türkiye'deki kamu kurumları arasında büyük **güvenlik boşlukları** bulunmaktadır. Özellikle, **yerel yönetimler** ve **küçük ölçekli kamu kurumları**, merkezi yönetim ve büyük kurumlar kadar siber güvenlik yatırımlarına sahip değildir. Bu durum, **farklı güvenlik seviyelerine** ve **eşitsizliklere** yol açmakta, tüm kamu kurumlarının genel siber güvenlik seviyesini zayıflatmaktadır.

Türkiye'deki kamu kurumlarında güvenlik açıklarının tespiti ve bu açıkların kapatılması için kapsamlı ve sürekli bir risk yönetimi sürecinin kurulması gerekmektedir. Kamu kurumları, **siber güvenlik eğitimi**, **güncel altyapı yatırımları**, **yazılım güncellemeleri** ve **kurumlar arası işbirliği** gibi önlemlerle bu zafiyetleri minimize edebilir ve siber tehditlere karşı daha sağlam bir savunma hattı oluşturabilirler.

4- Mevcut Siber Güvenlik Politikaları ve Hukuki Çerçeve

Yasal Düzenlemeler ve Standartlar: Türkiye'deki Kamu Kurumlarının Bilgi Güvenliği İçin Mevcut Yasal Çerçeve ve Uluslararası Standartlar

Türkiye'deki kamu kurumları, bilgi güvenliği sağlamak amacıyla bir dizi yasal düzenleme ve uluslararası standartlara uymak zorundadır. Bu çerçevede, **Kişisel Verilerin Korunması Kanunu (KVKK)** ve **ISO 27001** gibi önemli düzenlemeler ve standartlar, bilgi güvenliğinin hukuki temellerini oluşturur.

Kişisel Verilerin Korunması Kanunu (KVKK):

2016 yılında kabul edilen **KVKK**, Türkiye'deki bilgi güvenliği çerçevesinin en önemli parçasıdır. KVKK, kişisel verilerin işlenmesi, saklanması ve korunması konusunda kapsamlı düzenlemeler getirmektedir. Kamu kurumlarının, kişisel verileri toplarken, saklarken ve işleme süreçlerinde bireylerin haklarına zarar vermemek için KVKK'ya tam uyumlu hareket etmeleri gerekmektedir. Kanun, kişisel verilerin korunmasına yönelik hukuki yükümlülükleri belirler ve ihlallerde belirli cezai yaptırımlar öngörür.

ISO 27001 (Bilgi Güvenliği Yönetim Sistemi):

Kamu kurumları için uluslararası kabul görmüş bir diğer önemli standart **ISO 27001**'dir. ISO 27001, bilgi güvenliği yönetim sisteminin oluşturulması, uygulanması ve sürdürülmesi için bir çerçeve sunar. Türkiye'de birçok kamu kurumu, ISO 27001 standardını benimseyerek, uluslararası seviyede kabul gören güvenlik önlemleri almayı hedeflemektedir. Bu standart, kurumların bilgi güvenliğini yönetmeleri, potansiyel tehditleri tespit etmeleri ve önlem almaları için bir yol haritası sunar.

Bilgi Güvenliği İçin Diğer Yasal Düzenlemeler:

Türkiye'deki kamu kurumları ayrıca **Elektronik Ticaretin Düzenlenmesi Hakkında Kanun**, **Siber Güvenlik Stratejisi** ve **Siber Güvenlik Yükümlülükleri** gibi yasal düzenlemelere de tabidir. Bu düzenlemeler, devletin kritik altyapılarını korumak amacıyla siber tehditleri ele alır ve kamu sektöründe bilgi güvenliği bilincini artırmayı hedefler.

Türkiye'nin **yasal düzenlemeleri**, kamu kurumlarının bilgi güvenliği için bir temel sağlarken, **uluslararası standartlar** da bu sistemlerin etkinliğini artırmak için önemli bir referans noktası oluşturur. Ancak, hukuki çerçevenin etkin bir şekilde uygulanabilmesi için devletin, özel sektörle işbirliği yaparak denetimleri sıklaştırması ve güncel tehditlere karşı sürekli yasal düzenlemeler yapması gerekmektedir.

Bilişim Suçları ve Cezai Yaptırımlar: Kamu Kurumlarında Bilgi Güvenliği İhlalleri ile İlgili Cezai Yaptırımların Mevcut Durumu

Kamu kurumlarındaki **bilgi güvenliği ihlalleri**, önemli bir güvenlik riski teşkil etmektedir ve bu tür ihlallerin cezai yaptırımları, siber güvenlik politikalarının etkinliğini sağlamak adına kritik bir rol oynar. Türkiye'de bilişim suçlarıyla ilgili cezai yaptırımlar, temel olarak **Türk Ceza Kanunu (TCK)** ve **KVKK** çerçevesinde belirlenmiştir.

Türk Ceza Kanunu (TCK):

TCK, bilişim suçlarıyla ilgili düzenlemeleri içermektedir ve bu suçların cezai yaptırımlarını net bir şekilde tanımlar. **Veri hırsızlığı**, **veri kaybı** veya **veriye izinsiz erişim** gibi suçlar, TCK kapsamında cezalandırılabilir. TCK'nın 243. maddesi, bilişim sistemine izinsiz giriş yapan ve verileri ele geçiren kişilere **hapis cezası** öngörmektedir. Ayrıca, **sistemlere zarar verme** veya **bilgi hırsızlığı** gibi durumlar da cezai yaptırım gerektiren eylemler olarak tanımlanır.

Kişisel Verilerin Korunması Kanunu (KVKK):

Kamu kurumlarında bilgi güvenliği ihlali, **KVKK** çerçevesinde kişisel verilerin izinsiz işlenmesi, kaybedilmesi veya başkalarına aktarılması durumunda cezai yaptırımlarla karşı karşıya kalır. KVKK'ya aykırı hareket eden kamu kurumlarına **idari para cezaları** uygulanabilir. Ayrıca, kişisel verilerin güvenliğini sağlamayan kamu kurumları, **hukuki sorumluluklar** taşır ve zarar gören bireylere tazminat ödemekle yükümlü olabilir.

Bu cezai yaptırımlar, bilgi güvenliği ihlallerine karşı caydırıcı bir etki yaratırken, aynı zamanda kamu kurumlarının daha dikkatli ve güvenli sistemler kurmasını teşvik eder. Ancak, cezai yaptırımlar tek başına yeterli değildir; **eğitim**, **denetim** ve **şeffaflık** gibi unsurlar da ihlallerin önlenmesi için gereklidir.

5- Gizlilik ve Veri Koruma: Kamusal Verilerin Korunması ve Güvenliği İçin Uygulanan Önlemler

Kamusal verilerin korunması ve güvenliği, **gizlilik** ilkelerinin temelini oluşturur. Kamu kurumları, topladıkları kişisel ve ticari verileri, **gizlilik ve güvenlik** açısından belirli önlemlerle korumakla yükümlüdür. Türkiye'de bu güvenliği sağlamak için bazı uygulamalar mevcuttur:

Veri Şifreleme ve İzinli Erişim:

Kamu kurumları, topladıkları verileri **şifreleme** gibi güvenlik önlemleriyle korumaktadır. Ayrıca, veriye erişimi kontrol etmek ve yalnızca yetkilendirilmiş kişilerin erişmesini sağlamak için **izinli erişim politikaları** uygulanmaktadır. Bu politikalar, verinin yetkisiz kişiler tarafından ele geçirilmesini engeller.

Güvenlik Duvarları ve Ağ Koruma:

Kamu kurumları, verilerin korunması için **güvenlik duvarları**, **IDS/IPS (İntrusion Detection Systems / Intrusion Prevention Systems)** ve **antivirüs yazılımları** gibi ağ koruma sistemlerine yatırım yapmaktadır. Bu sistemler, veriye izinsiz erişimi engelleyerek, verilerin güvenliğini sağlamaktadır.

Veri Saklama Süreleri ve İmha Protokolleri:

Kamu kurumları, kişisel verilerin belirli sürelerle saklanmasını ve süresi dolan verilerin güvenli bir şekilde imha edilmesini sağlayan **veri saklama ve imha protokollerine** sahiptir. Bu uygulamalar, verilerin uzun süre saklanmasının engellenmesi ve verilerin yanlışlıkla veya kötü niyetle ifşa edilmesini önler.

Denetimler ve Uyumluluk İzleme:

Kamu kurumları, belirli aralıklarla **gizlilik denetimleri** ve **güvenlik denetimleri** yaparak, verilerin korunması ile ilgili önlemlerin etkinliğini test ederler. Ayrıca, bu denetimler aracılığıyla yasal uyumluluk sağlanır.

Çalışan Eğitimi ve Farkındalık Programları:

Kamu kurumlarında çalışanların, veri güvenliği konusunda sürekli olarak eğitilmesi gereklidir. Çalışanlar, **gizlilik sözleşmeleri** imzalayarak, kişisel verileri koruma sorumluluğuna sahip olduklarını kabul ederler. **Farkındalık programları** ise çalışanların güvenlik tehditlerine karşı daha dikkatli olmasını sağlar.

Türkiye'deki **gizlilik ve veri koruma** önlemleri, özellikle KVKK ve uluslararası standartlara dayalı olarak uygulanmaktadır. Bu önlemler, sadece kamu kurumlarının değil, aynı zamanda vatandaşların da güvenliğini sağlamayı amaçlar. Ancak, **teknolojik gelişmelere uyum sağlamak** ve **yeni tehditlere karşı hızlı aksiyon almak** için sürekli iyileştirme ve güncelleme gereklidir.

6- Kamu Kurumları İçin Bilgi Güvenliği Stratejileri

Güvenlik Politikaları ve Protokoller: Kamu Kurumlarında Uygulanması Gereken Temel Bilgi Güvenliği Protokollerinin Belirlenmesi

Kamu kurumlarında bilgi güvenliğinin sağlanması, güçlü bir güvenlik politikasının ve protokollerinin uygulanmasına dayanır. Bu protokoller, kurumların bilgi varlıklarını koruyarak, dijital ortamda oluşabilecek tehditlere karşı direnç oluşturmayı hedefler. Güvenlik politikalarının belirlenmesinde dikkate alınması gereken ana unsurlar şunlardır:

Veri Koruma Protokolleri:

Kamu kurumları, hem kişisel hem de kurumsal verilerin güvenliğini sağlamak için güçlü veri koruma politikalarına sahip olmalıdır. Bu, verilerin şifrelenmesi, yetkisiz erişimlerin engellenmesi, veri saklama sürelerinin belirlenmesi ve düzenli veri imha süreçlerini içerir.

Erişim Kontrolü Protokolleri:

Erişim kontrolü, doğru kişilerin yalnızca belirli verilere ulaşmasını sağlamak için kritik bir öneme sahiptir. Kamu kurumlarında **çok faktörlü kimlik doğrulama (MFA)**, **rol tabanlı erişim kontrolü (RBAC)** ve **izinli erişim** yöntemleri uygulanmalıdır. Bu protokoller, kurum içindeki veri güvenliğini sağlamada önemli bir araçtır.

Ağ Güvenliği Protokolleri:

Kamu kurumlarının ağlarına yönelik tehditler, siber saldırılara karşı alınacak önlemlerle minimize edilmelidir. **Güvenlik duvarları**, **IDS/IPS sistemleri** ve **VPN çözümleri**, dış tehditlere karşı korunmanın temel unsurlarıdır. Ayrıca, iç ağlardaki güvenlik açıklarını tespit etmek için **ağ izleme** ve **sızma testleri** gibi süreçler kullanılmalıdır.

Acil Durum ve İhlal Yönetim Protokolleri:

Her kamu kurumu, bilgi güvenliği ihlali veya siber saldırı durumunda hızlı bir şekilde tepki verebilmek için **siber kriz müdahale planları** oluşturmalıdır. Bu protokoller, siber saldırıların etkisini minimize etmek ve hızlıca toparlanmayı sağlamak için gereklidir.

Yasal Uyumluluk ve Raporlama Protokolleri:

Kamu kurumları, özellikle **KVKK** ve **ISO 27001** gibi yasal gerekliliklere uymak zorundadır. Bu, veri işleme süreçlerinin denetimini ve **gizlilik raporlamalarının düzenli yapılmasını** içerir. Protokoller, kurumsal verilerin korunması ve denetim süreçlerinin şeffaflığını sağlamalıdır.

Eğitim ve Farkındalık Çalışmaları: Kamu Çalışanlarının Bilgi Güvenliği Konusundaki Eğitimi ve Farkındalık Düzeyinin Artırılması

Kamu kurumlarının bilgi güvenliği stratejisinde en önemli unsurlardan biri, çalışanların güvenlik bilincini artırmaktır. Bu, sadece teknik önlemleri değil, aynı zamanda insan faktörünü de güvenlik sürecinin bir parçası haline getirir. Eğitim ve farkındalık çalışmaları için önerilen stratejiler şunlar olmalıdır:

Sürekli Eğitim Programları:

Kamu kurumlarında tüm çalışanlar, **bilgi güvenliği eğitimlerinden** düzenli olarak geçmelidir. Bu eğitimler, hem yeni başlayanlar için temel güvenlik bilgilerinden, hem de mevcut çalışanlar için ileri düzey güvenlik tehditlerine kadar geniş bir yelpazeyi kapsamalıdır.

Eğitimde phishing saldırıları, güvenli şifre kullanımı, sosyal mühendislik gibi konulara özel olarak yer verilmelidir.

Simülasyonlar ve Tatbikatlar:

Eğitimlerin daha etkili olabilmesi için, çalışanların karşılaşabilecekleri siber saldırı türlerini simüle eden tatbikatlar düzenlenmelidir. Bu tatbikatlar, çalışanların **gerçek zamanlı senaryolar** üzerinden nasıl tepki vereceklerini görmelerini sağlar ve farkındalık düzeylerini artırır.

Farkındalık Kampanyaları:

Özellikle **yıl dönümleri** veya **haftalar** gibi belirli zaman dilimlerinde farkındalık kampanyaları düzenlenebilir. Bu kampanyalar, sosyal medya, e-posta bültenleri ve kurum içi posterler gibi çeşitli mecralar üzerinden bilgi güvenliği bilincini artırmak için etkin bir araç olabilir.

Kişisel Güvenlik Bilinci:

Çalışanlar, sadece kurum bilgisini değil, kendi kişisel bilgilerini de siber tehditlere karşı nasıl koruyacakları konusunda bilgilendirilmelidir. Bu, **kişisel bilgisayar güvenliği**, **mobil cihaz güvenliği** ve **sosyal medya güvenliği** gibi alanlarda eğitimlerle desteklenebilir.

Siber Güvenlik Eğitim Programları:
Kamu Personeline Yönelik Düzenli Güvenlik Eğitimlerinin Gerekliliği

Kamu personelinin, gelişen siber tehditlere karşı sürekli olarak eğitilmesi, kurumların güvenliğini sağlamada büyük önem taşır. Bu eğitimlerin içerik ve yapısı şu şekilde olmalıdır:

Temel Siber Güvenlik Eğitimleri:

Tüm kamu personeline yönelik temel siber güvenlik eğitimi, çalışanların siber saldırıları tanıyıp nasıl korunacaklarını öğrenmeleri için gereklidir. Bu eğitimlerde **phishing saldırıları**, **ransomware**, **malware** gibi temel siber tehditler öğretilmelidir.

İleri Düzey Eğitimler ve Uzmanlık Alanları:

Siber güvenlik uzmanları için ileri düzey eğitim programları düzenlenebilir. Bu eğitimlerde, **ağ güvenliği**, **kripto sistemler**, **şifreleme teknolojileri** ve **sızma testleri** gibi konulara yoğunlaşılmalıdır.

Acil Durum Müdahale Eğitimi:

Personel, acil durumlar için hazırlıklı olmalı ve olası bir güvenlik ihlali veya siber saldırı durumunda hızlı ve etkili bir şekilde müdahale edebilmelidir. Bu eğitimler, siber saldırı sırasında ne yapılması gerektiğini ve olay yönetimi sürecinin nasıl işlediğini içermelidir.

Güncel Tehditler ve Teknolojiler:

Eğitimler, **yeni tehditler** ve **gelişen teknolojiler** hakkında düzenli güncellemeler içermelidir. Bu, siber güvenlik dünyasındaki değişen dinamiklere hızlıca adapte olunmasını sağlar.

Denetim ve İzleme:
Kamu Kurumlarının Siber Güvenlik Durumunu İzlemek İçin Denetim Mekanizmalarının Kurulması

Kamu kurumlarında güvenliğin etkin bir şekilde sağlanabilmesi için, **denetim ve izleme mekanizmaları** kritik bir öneme sahiptir. Bu mekanizmalar, kurumların bilgi güvenliği uygulamalarını ve güvenlik açıklarını sürekli olarak izlemek için kullanılmalıdır. Uygulanması gereken ana unsurlar şunlardır:

Güvenlik İzleme Araçları:

Kamu kurumları, **güvenlik izleme araçları** kullanarak ağ trafiğini, sunucuları, veri tabanlarını ve kullanıcı etkinliklerini sürekli izlemelidir. Bu izlemeler, potansiyel tehditleri erkenden tespit etme ve buna göre önlem alma fırsatı sunar.

Denetim Raporları ve Performans Değerlendirmesi:

Düzenli olarak **denetim raporları** hazırlanmalı ve kurum içindeki güvenlik seviyeleri belirli aralıklarla değerlendirilmeli. Bu raporlar, kurumların siber güvenlik stratejilerinin ne kadar etkili olduğunu belirlemeye yardımcı olur.

İç ve Dış Denetim Süreçleri:

Kamu kurumlarında hem iç denetim ekiplerinin hem de dış bağımsız denetçilerin belirli periyotlarla güvenlik değerlendirmeleri yapması gerekmektedir. Bu denetimler, kurumların uyguladığı güvenlik önlemlerinin etkili olup olmadığını kontrol eder.

Olay Müdahale ve Raporlama:

Denetim ve izleme süreçlerinin bir parçası olarak, her siber saldırı ya da güvenlik ihlali olayının detaylı bir şekilde raporlanması, analiz edilmesi ve gerekli aksiyonların alınması gerekmektedir. Bu, gelecekteki tehditlere karşı stratejik önlemler almayı sağlar.

7- Teknolojik Altyapı ve Yatırımlar

Güçlü Siber Güvenlik Altyapısı:
Kamu Kurumlarının Sahip Olması Gereken Güncel Teknolojik Altyapılar

Kamu kurumlarının siber güvenlik altyapısı, tehditlere karşı dayanıklı olmalı ve modern teknolojilere dayalı olmalıdır. Bu altyapı şu bileşenleri içermelidir:

Güvenlik Duvarları ve IDS/IPS Sistemleri:

Dış tehditlere karşı güvenliği sağlamak için kurumlar, gelişmiş **güvenlik duvarları**, **saldırı tespit sistemleri (IDS)** ve **saldırı engelleme sistemleri (IPS)** kullanmalıdır.

Veri Şifreleme ve İleri Düzey Şifreleme Teknikleri:

Verilerin hem taşıma sırasında hem de depolanırken **şifrelenmesi**, veri sızıntıları ve izinsiz erişimleri engeller. **SSL/TLS** gibi güçlü şifreleme protokolleri kullanılmalıdır.

Yedekleme ve Felaket Kurtarma Sistemleri:

Herhangi bir siber saldırı veya doğal afet sonrası verilerin kaybolmaması için yedekleme sistemleri ve felaket kurtarma planları oluşturulmalıdır. Bu sistemler, **bulut tabanlı yedekleme çözümleri** ile güçlendirilebilir.

Bulut Güvenliği:
Bulut Tabanlı Sistemlere Geçişin Güvenlik Açısından Değerlendirilmesi

Bulut teknolojilerine geçiş, kamu kurumlarına esneklik ve verimlilik sağlar; ancak bu geçişin güvenlik açığı yaratmaması için dikkatli bir değerlendirme yapılmalıdır. Kamu kurumlarının bulut güvenliği şu stratejilerle sağlanabilir:

Bulut Güvenlik Protokolleri:

Veri şifreleme, **güvenli erişim kontrolü** ve **çok faktörlü kimlik doğrulama** gibi protokoller, bulut ortamında veri güvenliğini sağlamada kritik öneme sahiptir.

Bulut Sağlayıcılarıyla Güvenlik Sözleşmeleri:

Kamu kurumları, bulut hizmet sağlayıcılarıyla güvenlik standartları ve yükümlülükler konusunda açık sözleşmeler yapmalı ve güvenlik denetimlerini düzenli olarak yapmalıdır.

Siber Güvenlik Yatırımları ve Bütçeleme:
Kamu Kurumlarında Güvenlik Teknolojilerine Yapılacak Yatırımların Planlanması ve Bütçelendirilmesi

Kamu kurumları için siber güvenlik yatırımlarının bütçelenmesi, uzun vadeli güvenlik hedeflerine ulaşılabilmesi için gereklidir. Bu süreç şu adımları içermelidir:

Siber Güvenlik Yatırım Öncelikleri:

Öncelikle kritik altyapılar, ağ güvenliği, veri koruma ve kullanıcı eğitimi gibi alanlarda yapılacak yatırımlar belirlenmelidir.

Bütçeleme ve Finansal Planlama:

Siber güvenlik için ayrılan bütçe, her yıl belirli bir oranda arttırılmalı ve bu alandaki finansal planlamalar uzun vadeli olmalıdır.

Verimlilik Analizleri:

Yatırımların etkinliğini ölçmek için **geri dönüş (ROI)** analizleri yapılmalı ve siber güvenlik önlemlerinin ne kadar başarılı olduğu düzenli olarak değerlendirilmektedir.

8- Kriz Yönetimi ve Olay Müdahale Planları

Siber Saldırı Sonrası Müdahale:
Siber Saldırıların Ardından Nasıl Bir Müdahale Süreci İzlenmelidir?

Siber saldırılar, kamu kurumlarının bilgi güvenliğini tehdit eden önemli bir risktir. Bu nedenle, her kurum için etkili bir **olay müdahale planı** geliştirilmesi kritik öneme sahiptir. Siber saldırı sonrası müdahale süreci şu temel adımlardan oluşmalıdır:

Hızlı Tespit ve İzolasyon:

Siber saldırıdan etkilenmiş sistemler, ilk aşamada hızla tespit edilmeli ve izole edilmelidir. Böylece, saldırının yayılmasının önüne geçilir. Bu aşamada, **saldırı tespit sistemleri (IDS)** ve **anormal trafik izleme** araçları aktif bir şekilde kullanılarak zararlı yazılımlar hızla tespit edilmelidir.

Olayın Değerlendirilmesi ve Anlamlandırılması:

Saldırı türü belirlenmeli ve etkileri değerlendirilmelidir. Bu aşama, siber güvenlik ekiplerinin **saldırı türü analizi** yaparak, saldırganların hedeflerini ve kullandıkları yöntemleri anlamalarına yardımcı olur.

Müdahale ve İyileştirme:

Saldırının etkilediği sistemlerdeki zararlı yazılımlar temizlenmeli ve sistemler geri yüklenmelidir. **Yedekleme sistemleri** ve **felaket kurtarma planları** devreye sokulmalıdır. Ayrıca, saldırıya karşı alınacak tedbirler (örneğin, şifrelerin sıfırlanması, yazılımların güncellenmesi) hızla uygulanmalıdır.

Halkla İletişim ve Şeffaflık:

Saldırı sonrası, kamuoyunun bilgilendirilmesi ve şeffaf bir şekilde durumun paylaşılması gerekmektedir. Bu, hem güven inşa eder hem de olası yanlış bilgi akışlarını engeller.

İzleme ve Raporlama:

Müdahale süreci sonrasında, olayın detaylı bir şekilde raporlanması ve kurumsal güvenlik sistemlerinin güçlendirilmesi için öğrenilen derslerin kaydedilmesi önemlidir.

Acil Durum Planları ve Yedekleme Sistemleri:
Kamu Kurumlarında Yaşanacak Veri Kayıpları veya Saldırılar Sonrası Veri Kurtarma Stratejileri

Veri kaybı ve siber saldırılar sonrası etkin bir veri kurtarma stratejisi, kamu kurumlarının devamlılığını sağlamak adına önemlidir. Acil durum planları ve yedekleme sistemleri şu unsurları içermelidir:

Veri Yedekleme Protokolleri:

Otomatik yedekleme sistemleri her kurumda aktif olmalı ve kritik veriler **günlük** olarak yedeklenmelidir. Ayrıca, yedekleme verilerinin **bulut ortamında** veya **coğrafi olarak ayrı bir lokasyonda** depolanması, olası afetlere karşı daha fazla güvenlik sağlar.

Felaket Kurtarma Planları:

Felaket kurtarma planları, veri kaybı durumunda her adımın nasıl uygulanacağını belirten açık ve etkili bir kılavuz olmalıdır. Bu planlarda, sistemlerin nasıl yeniden yapılandırılacağı, hangi verilerin kurtarılacağı ve kurtarma süresinin nasıl hızlandırılacağına dair prosedürler bulunmalıdır.

Veri Entegrasyonu ve Sürekliliği:

Yedeklenen verilerin yalnızca fiziksel olarak saklanması yeterli değildir. Aynı zamanda verilerin **en son sürümleriyle uyumlu** şekilde sistemlere entegre edilmesi ve her kurumda **veri kurtarma tatbikatları** yapılması gerekmektedir.

Yedekleme ve Kurtarma Sürekliliği Testleri:

Sistemlerin etkinliğini ve yedekleme süreçlerinin sağlıklı işleyişini test etmek amacıyla, **düzenli tatbikatlar** yapılmalıdır. Bu tatbikatlar, olası bir siber saldırıya karşı anında çözüm üretebilme kapasitesini artırır.

Sosyal ve Ekonomik Etkiler:
Hacklenmiş Kamu Verilerinin Toplumsal ve Ekonomik Etkileri Üzerine Analiz

Siber saldırılar yalnızca teknik değil, toplumsal ve ekonomik olarak da ciddi sonuçlar doğurur. Hacklenmiş kamu verilerinin toplumsal ve ekonomik etkileri şu şekilde analiz edilebilir:

Toplumsal Güvenin Sarsılması:

Kamu verilerinin ele geçirilmesi, halkın devlet ve kamu kurumlarına olan güvenini ciddi şekilde zedeler. Özellikle kişisel ve finansal verilerin açığa çıkması, vatandaşlar arasında **gizlilik endişeleri** yaratır.

Ekonomik Kayıplar ve Zararlar:

Kamu verilerinin sızdırılması veya zarar görmesi, ekonomik kayıplara yol açabilir. Bu kayıplar, **doğrudan finansal zarar** (örneğin, dolandırıcılık, fidye yazılımlarına ödenen bedeller) ve **dolaylı zararlar** (örneğin, itibar kaybı, iş gücü kaybı) şeklinde kendini gösterebilir.

Sosyal Eşitsizlik ve Marjinalleşme:

Veri sızıntıları, özellikle **azınlık gruplarını** hedef alarak toplumsal dışlanmayı artırabilir. Özellikle **sosyal sigorta**, **sağlık verileri** ve **kimlik bilgileri** gibi hassas verilerin ele geçirilmesi, marjinalleşme ve **toplumsal eşitsizlik** yaratabilir.

9- Kamu-Özel Sektör İşbirliği ve Uluslararası İşbirliği

Özel Sektör ile İşbirlikleri:
Kamu Kurumlarının Özel Sektör ile Birlikte Bilgi Güvenliğini Güçlendirme Yolları

Kamu kurumları, özel sektörle işbirliği yaparak siber güvenlik alanında önemli faydalar elde edebilir. Kamu-özel sektör işbirlikleri şu şekilde sağlanabilir:

Teknoloji Sağlayıcılarıyla İşbirliği:

Kamu kurumları, güçlü **güvenlik yazılımları** ve **saldırı tespit sistemleri** sağlayan teknoloji firmalarıyla işbirliği yaparak daha etkili bir güvenlik altyapısı oluşturabilir. Bu tür işbirlikleri, devletin siber tehditlere karşı daha dayanıklı hale gelmesini sağlar.

Güvenlik Standartlarının Uygulanması:

Özel sektörle yapılan anlaşmalarla, **ISO 27001**, **GDPR** ve **PCI-DSS** gibi uluslararası güvenlik standartlarına uyum sağlanabilir. Bu tür işbirlikleri, güvenlik süreçlerinin küresel normlara uygun hale gelmesini sağlar.

Veri Paylaşımı ve Araştırma:

Özel sektör, veri güvenliği konusunda kamuya bilgi sağlayabilir. Özellikle **yeni tehditlerin** tespiti ve karşı önlemlerin geliştirilmesi için ortak araştırmalar yapılabilir.

Uluslararası Siber Güvenlik İşbirlikleri:
Türkiye'nin Siber Güvenlik Alanındaki Uluslararası İşbirliklerinin Artırılması

Siber güvenlik tehditleri sınırları aşan küresel sorunlardır ve bu nedenle uluslararası işbirliği önemlidir. Türkiye'nin siber güvenlik alanındaki uluslararası işbirliklerinin artırılması için şunlar önerilebilir:

Uluslararası Bilgi Paylaşımı:

Türkiye, diğer ülkelerle siber tehditler ve güvenlik açıkları konusunda bilgi paylaşımını teşvik etmelidir. Bu tür işbirlikleri, **global tehditlerin** karşısında daha sağlam bir savunma oluşturulmasına olanak tanır.

Siber Güvenlik Konferansları ve Eğitimler:

Türkiye, uluslararası siber güvenlik konferanslarında yer almalı ve düzenlemeler yaparak uzmanları bir araya getirmelidir. Bu tür etkinlikler, **bilgi alışverişi** sağlar ve **yenilikçi güvenlik çözümleri** üretmeye yardımcı olur.

Siber Güvenlik İttifakları:
Küresel Tehditlerle Mücadele İçin Siber Güvenlik İttifakları Kurma

Küresel siber tehditlerle mücadele için **siber güvenlik ittifakları** kurulması gereklidir. Türkiye'nin bu ittifaklara katılması veya kendi ittifaklarını kurması, ulusal ve küresel güvenliğin güçlendirilmesi için önemlidir:

Bölgesel Güvenlik İşbirlikleri:

Türkiye, bölgesindeki diğer ülkelerle **siber güvenlik ittifakları** kurarak, özellikle **bölgesel siber saldırılara karşı** kolektif bir savunma oluşturabilir. Bu ittifaklar, ortak siber güvenlik politikalarının uygulanmasına olanak tanır.

Küresel Siber Savunma Ortaklıkları:

NATO, Avrupa Birliği ve Birleşmiş Milletler gibi küresel aktörlerle siber güvenlik konusunda işbirliği artırılmalı ve **global tehditlere karşı** daha güçlü bir siber savunma stratejisi geliştirilmelidir.

Sonuç ve Alınması Gereken Tedbirler: Türkiye'nin Kamu Kurumlarında Siber Güvenlik Düzeyinin Güçlendirilmesi

Bu raporda ortaya konan analiz ve değerlendirmeler, Türkiye'deki kamu kurumlarının siber güvenlik alanında karşı karşıya olduğu riskleri, zafiyetleri ve eksiklikleri detaylı bir şekilde gözler önüne sermiştir. Siber güvenlik, yalnızca bir teknoloji sorunu değil, aynı zamanda kamu hizmetlerinin sürekliliği, toplumsal güvenin korunması ve ekonomik istikrarın sağlanması için kritik bir öneme sahiptir. Bu bağlamda, aşağıda geniş kapsamlı sonuçlar ve öneriler sunulmuştur:

1. Türkiye'nin Siber Güvenlik Durumunun Genel Değerlendirmesi

Kritik Güvenlik Açıkları: Kamu kurumlarında eski altyapılar, güncellenmeyen yazılımlar ve yetersiz güvenlik politikaları, siber tehditlere karşı savunmasız bir yapı yaratmaktadır.

Kurumsal Eşitsizlikler: Büyük ve merkezi kurumlarla yerel yönetimler arasında ciddi siber güvenlik farkları bulunmaktadır. Özellikle yerel yönetimlerin kaynak yetersizliği, bu alandaki zayıflıkları artırmaktadır.

Hacklenme Vakaları: Sağlık, enerji, finans ve seçim süreçleri gibi kritik alanlarda yaşanan hacklenme olayları, hem kamu hizmetlerini kesintiye uğratmış hem de toplumsal güveni zedelemiştir.

İnsan Faktörü: Kamu personelinin bilgi güvenliği bilinci ve farkındalığı, siber tehditlerle mücadelede önemli bir zayıf halka olarak ortaya çıkmaktadır.

2. Alınması Gereken Tedbirler ve Öneriler

Kamu kurumlarının siber güvenlik seviyelerini artırmak ve toplumsal güveni sağlamak için aşağıdaki adımların atılması gerekmektedir:

2.1. Teknolojik Altyapının Güçlendirilmesi

Yerli Siber Güvenlik Yazılımlarının Geliştirilmesi

Siber güvenlik alanında yerli yazılımların geliştirilmesi, özellikle veri gizliliği ve güvenliğinin kritik önem taşıdığı kurumlarda öncelikli bir politika olarak benimsenmelidir. Yerli yazılımlar, milli bağımsızlığın korunması, stratejik altyapının güvence altına alınması ve ulusal siber güvenlik ekosisteminin oluşturulması açısından stratejik bir rol üstlenmektedir.

Yerli yazılımların avantajları şu şekilde özetlenebilir:

Veri Güvenliği: Ulusal düzeyde kritik bilgilerin sızmasını engelleyerek, veri güvenliğini sağlar.

Yabancı Yazılım Risklerinin Azaltılması: Yabancı yazılımlarda bulunabilecek kasıtlı veya riskli güvenlik açıklarının önüne geçer.

Uyum ve Özelleştirme: Yerel ihtiyaçlara ve yasal düzenlemelere uygun olarak kolayca uyarlanabilir ve özelleştirilebilir.

Ekonomik Katkı: İstihdam oluşturarak, döviz kaybını önler ve yerel ekonomiye katkı sağlar.

Denetlenebilirlik: Kodların incelenebilir olması, güvenlik açıklarının hızlı tespit edilmesine olanak tanır ve yazılımlar daha şeffaf bir şekilde denetlenebilir.

Teknolojik Bağımsızlık: Uzun vadede bağımsız bir teknoloji altyapısı oluşturur.

2.2. Kapalı Devre Ağ Yapısının Oluşturulması ve Güçlendirilmesi

Kapalı devre ağ yapılarının kullanımı, özellikle kritik altyapıların ve kurumların siber güvenliğinin sağlanmasında öncelikli bir yöntem olarak benimsenmelidir. Bu sistemler, internete erişimi olmayan izole ağ yapıları olarak tasarlanmış olup, dış tehditlere karşı üstün koruma sağlamaktadır.

Kapalı devre ağ yapılarına ilişkin temel özellikler ve avantajlar şunlardır:

Dış Saldırılara Karşı Koruma: İnternet erişimi olmadığı için, dışarıdan gelen siber saldırılara tamamen kapalıdır.

Veri Sızıntısının Engellenmesi: Hassas bilgilerin yalnızca yetkilendirilmiş kullanıcılar tarafından erişilebilmesini sağlayarak veri sızıntısını önler.

Zararlı Yazılım Koruması: Fidye yazılımları gibi zararlı yazılımlara karşı güvenlik sağlar.

Kontrol ve Denetim: Veri akışı ve ağ erişimi üzerinde daha sıkı bir kontrol ve denetim mekanizması sunar.

Kritik Altyapıların Korunması: Savunma sanayi, enerji, sağlık ve endüstriyel kontrol sistemleri gibi kritik altyapılar için uluslararası standartlarda güvenlik sunar.

Ancak, kapalı devre ağların tam anlamıyla güvenli olabilmesi için içeriden gelebilecek tehditlere karşı önlemlerin alınması ve manuel güncellemelerin dikkatli bir şekilde yönetilmesi gereklidir.

Kapalı devre ağ sistemleri, kritik altyapıların güvenliğini sağlamak ve siber tehditlerden korunmak için vazgeçilmez bir unsurdur. Bu nedenle, ulusal güvenlik stratejilerinin bir parçası olarak bu ağ yapılarının kurulması ve güçlendirilmesi öncelikli hedefler arasında yer almalıdır.

Gelişmiş Güvenlik Sistemleri: Kamu kurumlarında güvenlik duvarları (firewall), saldırı tespit sistemleri (IDS/IPS) ve veri şifreleme teknolojilerinin modernize edilmesi gerekmektedir.

Bulut Güvenliği ve Yedekleme: Verilerin yedeklenmesi ve bulut tabanlı sistemlerin güvenli hale getirilmesi, kritik veri kayıplarını önleyecek önemli bir adımdır.

Sızma Testleri ve Sürekli İzleme: Kamu kurumlarında düzenli sızma testleri yapılmalı, ağ güvenliği ve veri trafiği sürekli izlenmelidir.

2.3. Devlet Eliyle Kripto Blokzincir Sistemlerinin Kullanımı ve Veri Güvenliği

Blokzincir teknolojisi, merkezi olmayan, şeffaf ve değiştirilemez bir yapıya sahip olması nedeniyle veri güvenliği açısından önemli fırsatlar sunmaktadır. Devlet eliyle kurulabilecek kripto blokzincir sistemleri, özellikle güvenlik, veri doğrulama ve saklama süreçlerinde etkin bir çözüm sunabilir. Bu sistemler, kişisel verilerin korunması, yetkisiz erişimin engellenmesi ve siber güvenlik tehditlerinin azaltılması açısından güçlü bir altyapı sağlayabilir.

Merkezi Olmayan Güvenlik Sistemi

Blokzincir tabanlı sistemler, verilerin merkezi bir noktada toplanmasını engelleyerek güvenlik açıklarını minimize eder. Devlet eliyle oluşturulan blokzincir tabanlı bir veri güvenliği sistemi, aşağıdaki alanlarda etkili olabilir:

Kimlik Doğrulama: Vatandaşların kimlik bilgilerini güvence altına alarak yetkisiz erişimleri engelleyebilir.

Veri Bütünlüğü: Kayıt edilen verilerin değiştirilememesi ve yetkisiz kişilere erişimin engellenmesi sağlanabilir.

Takip ve Şeffaflık: Verilerin kimler tarafından ne zaman erişildiğinin izlenebilir olması, veri güvenliğini artırır.

Kamu Hizmetlerinde Uygulama Alanları

Blokzincir teknolojisi, kamu hizmetlerinde aşağıdaki alanlarda kullanılabilir:

Kişisel Veri Yönetimi: KVKK kapsamında kişisel verilerin işlenmesi ve saklanması blokzincir teknolojisi ile daha güvenli hale getirilebilir.

Sağlık Verileri: Hastaların sağlık verilerinin blokzincir üzerinde saklanarak, hem hasta mahremiyeti hem de yetkili sağlık personelinin erişimi için güvenli bir ortam oluşturulabilir.

Adli Veri Saklama: Ceza davalarında delil niteliği taşıyan verilerin güvenli bir şekilde saklanması ve izlenebilirliği sağlanabilir.

Siber Güvenlik: Elektronik ortamdaki veri ihlallerini engellemek ve güvenlik tehditlerine karşı daha dayanıklı bir sistem oluşturmak için blokzincir altyapısı kullanılabilir.

2.4. Veri Güvenliği ve Uluslararası İşbirliği

Blokzincir teknolojisinin devlet eliyle uygulanması, Türkiye'nin uluslararası işbirliklerinde daha güçlü bir konuma gelmesini sağlayabilir. Özellikle EUROPOL, EUROJUST gibi uluslararası kuruluşlarla yürütülen veri güvenliği işbirliklerinde, şeffaf ve güvenilir bir blokzincir altyapısı Türkiye'nin veri güvenliği taahhütlerini güçlendirebilir.

Çözüm Önerileri

Ulusal Blokzincir Altyapısı Kurulması: Kamu kurumlarının ortak kullanabileceği bir ulusal blokzincir altyapısı oluşturulmalıdır. Bu altyapı, veri paylaşımı ve güvenliği süreçlerini standartlaştırabilir.

Blokzincir Temelli Kimlik Yönetimi: E-Devlet sistemine entegre bir kimlik doğrulama ve veri saklama hizmeti geliştirilmelidir.

Hukuki ve Teknik Düzenlemeler: Blokzincir teknolojisinin yasal altyapısı hazırlanmalı ve teknolojinin kamu hizmetlerinde uygulanabilirliği artırılmalıdır.

Uluslararası Sertifikasyonlar: Türkiye, blokzincir tabanlı veri güvenliği uygulamalarında uluslararası standartlara uygun sertifikasyon süreçlerini benimsemelidir.

AR-GE ve Eğitim Çalışmaları: Blokzincir teknolojisinin etkin kullanımını sağlamak için teknik altyapı geliştirme ve insan kaynağı yetiştirme faaliyetlerine ağırlık verilmelidir.

2.5. Eğitim ve Farkındalık Çalışmalarının Artırılması

Personel Eğitimi: Tüm kamu personeline düzenli siber güvenlik eğitimleri verilerek, temel tehditlerin tanınması ve korunma yöntemleri öğretilmelidir.

Farkındalık Kampanyaları: Kamu kurumlarında güvenlik bilincini artırmak için farkındalık kampanyaları düzenlenmeli ve çalışanların dikkat düzeyleri yükseltilmelidir.

Yönetici Eğitimi: Kurum yöneticilerinin, siber tehditler ve kriz yönetimi konusunda daha bilinçli hale gelmesi sağlanmalıdır.

2.6. Yasal Düzenlemelerin Güçlendirilmesi

KVKK ve ISO 27001 Uyumunun Yaygınlaştırılması: Kişisel Verilerin Korunması Kanunu ve uluslararası bilgi güvenliği standartlarına uyum tüm kurumlarda zorunlu hale getirilmelidir.

Yeni Yasal Düzenlemeler: Mevcut yasalar, yeni tehditler ve teknolojilere uyum sağlayacak şekilde güncellenmeli; cezai yaptırımlar caydırıcı hale getirilmelidir.

Denetim ve Şeffaflık: Kamu kurumlarının bilgi güvenliği uygulamaları düzenli olarak denetlenmeli, raporlamalar şeffaf bir şekilde yapılmalıdır.

2.7. Kamu-Özel Sektör İşbirliklerinin Geliştirilmesi

Teknoloji Sağlayıcıları ile Ortaklıklar: Özel sektörle yapılacak işbirlikleri, kamu kurumlarının siber güvenlik altyapısını güçlendirebilir.

Araştırma ve Geliştirme: Kamu ve özel sektörün işbirliğiyle yeni güvenlik teknolojilerinin geliştirilmesi teşvik edilmelidir.

2.8. Uluslararası İşbirlikleri

Bilgi Paylaşımı: Türkiye, diğer ülkelerle siber tehditlere dair bilgi paylaşımı yaparak küresel işbirliklerini artırmalıdır.

Uluslararası Standartlar: NATO, Avrupa Birliği ve diğer uluslararası organizasyonlarla ortak çalışarak uluslararası standartlara uyum sağlanmalıdır.

Uluslararası İşbirliğinde Karşılaşılan Zorluklar

Kişisel Verilerin Korunması Kanunu'nun (KVKK) gerekçesinde belirtildiği üzere, Türkiye'de böyle bir yasal düzenlemenin yapılmasındaki önemli dış etkenlerden biri, EUROPOL ve EUROJUST gibi uluslararası kuruluşlarla etkili işbirliğinin sağlanmasıdır. Ancak Türkiye, 6698 sayılı KVKK'nın etkin bir şekilde uygulanamaması ve siber güvenlik açıklarının etkili bir şekilde korunamaması nedeniyle bu kuruluşların kara listesinde yer almakta ve işbirliği yapamamaktadır. Bu durum, uluslararası veri güvenliği standartlarına uyum sağlanamamasından kaynaklanmakta olup, hem ekonomik hem de güvenlik açısından ciddi bir problem teşkil etmektedir.

Türk Ceza Kanunu ve Kişisel Verilerin Korunması

Türk Ceza Kanunu'nun (TCK) 135. ve 136. maddeleri doğrudan kişisel verilerin korunmasını amaçlamaktadır. Bu maddeler, özellikle elektronik ortamda işlenen suçlar açısından da geçerlidir. Örneğin, Discord gibi platformlarda gençlerin kişisel verilerinin kaydedilerek tehdit edilmesi, TCK'nın bu maddeleri kapsamında değerlendirilmektedir. Bu tür vakalar, siber güvenlik ihlallerinin kişisel veriler üzerindeki olumsuz etkilerini gözler önüne sermektedir.

Yabancı Şirketlerle İşbirliği Eksikliği

Türkiye'nin uluslararası veri koruma standartlarına uyum sağlayamaması, Discord veya Wattpad gibi merkezi ülke dışında bulunan şirketlerle işbirliği yapılmasını zorlaştırmaktadır. Bu şirketler, ülkemizde gerekli soruşturmalar için ihtiyaç duyulan verileri paylaşmamakta ve bu durum soruşturmaların etkinliğini azaltmaktadır. Sonuç olarak, bu şirketler işbirliğine yanaşmadığında, devlet politikası gereği erişim engelleri getirilerek bu uygulamalar kapatılmaktadır. Bu durum, hem bireysel kullanıcıları hem de kurumları etkilemekte, dijital dönüşüm süreçlerinde gecikmelere yol açmaktadır.

5651 Sayılı Kanun'un Rolü

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Kanunu, siber güvenlik açısından kritik bir yasal düzenlemedir. Bu kanun, internet ortamındaki suçlarla mücadeleye yönelik önlemler içermekte ve özellikle veri güvenliği ile ilgili hususlarda düzenlemeler getirmektedir. Ancak bu düzenlemelerin etkinliği, uygulama sürecinde karşılaşılan teknik ve hukuki zorluklar nedeniyle sınırlı kalmaktadır.

Çözüm Önerileri

- KVKK'nın etkin uygulanmasını sağlamak ve uluslararası standartlarla uyumlu hale getirmek için teknik ve hukuki altyapının geliştirilmesi gerekmektedir.
- Siber güvenlik açıklarını kapatmak için yerel ve uluslararası işbirliklerinin artırılması önem taşımaktadır.
- Yabancı şirketlerle işbirliğini kolaylaştırmak için uluslararası veri güvenliği garantilerinin güçlendirilmesi ve gerekli düzenlemelerin yapılması gerekmektedir.
- 5651 sayılı Kanun'un kapsamı, modern teknolojiler ve dijital tehditler dikkate alınarak güncellenmelidir.
- Kullanıcıların bilinçlendirilmesine yönelik kampanyalar düzenlenmeli ve bireylerin veri güvenliği konusundaki farkındalığı artırılmalıdır.

2.9. Kriz Yönetimi ve Acil Durum Planları

Siber Saldırı Müdahale Protokolleri: Her kamu kurumu için detaylı bir siber kriz yönetim planı hazırlanmalı ve düzenli tatbikatlarla bu planlar test edilmelidir.

Yedekleme ve Kurtarma: Verilerin güvenli bir şekilde yedeklenmesi ve kurtarma süreçlerinin hızlandırılması için altyapı yatırımları yapılmalıdır.

3. Geniş Çaplı Bir Siber Güvenlik Stratejisinin Gerekliliği

Türkiye'nin siber güvenlik alanında daha dirençli bir yapıya kavuşması için kapsamlı, çok katmanlı ve proaktif bir stratejiye ihtiyacı vardır. Bu strateji, kamu kurumlarının teknoloji, insan kaynağı, yasal düzenlemeler ve uluslararası işbirlikleri ekseninde entegre bir yaklaşımı benimsemesini sağlamalıdır. Özellikle:

Ulusal Siber Güvenlik Merkezi: Tüm kamu kurumlarının koordinasyon içinde çalışabileceği merkezi bir yapı oluşturulmalıdır.

Yeni Nesil Tehditlere Karşı Savunma: Yapay zekâ tabanlı siber tehditlere karşı gelişmiş savunma mekanizmaları hayata geçirilmelidir.

Toplumsal Bilinçlendirme: Vatandaşlar arasında veri güvenliği bilinci artırılmalı ve kamu güvenliği halkın katılımıyla güçlendirilmelidir.

Kamu kurumlarının bilgi güvenliği, yalnızca teknik bir zorunluluk değil, aynı zamanda devletin güvenilirliği ve kamu hizmetlerinin sürdürülebilirliği için kritik bir gerekliliktir. Siber tehditlerin hem yerel hem de küresel boyut kazandığı günümüzde, Türkiye'nin daha güçlü bir siber güvenlik altyapısına ve dayanıklı bir savunma stratejisine sahip olması elzemdir. Önerilen tedbirler ve politikalar, sadece siber saldırılara karşı savunma sağlamakla kalmayacak, aynı zamanda Türkiye'nin dijitalleşme sürecini hızlandırarak ekonomik ve toplumsal kalkınmayı da destekleyecektir.

KAMU KURUMLARINDA SİBER GÜVENLİK ve TÜRKİYE'NİN TOPLUMSAL MAHREMİYETİ

2025

DURUM RAPORU

Bu raporun amacı, Türkiye'deki kamu kurumlarının siber güvenlik durumunu değerlendirmek, mevcut tehdit ve açıkları tespit etmek, gerekli önlemleri belirlemek ve bilgi güvenliğini güçlendirmeye yönelik somut öneriler sunmaktır. Ayrıca, siber saldırıların toplumsal, ekonomik ve siyasi etkilerini analiz ederek kamu hizmetlerinin sürekliliği için stratejik bir yol haritası oluşturmayı hedeflemektedir.

DURUM RAPORLARI SERİSİ
SERİ 2

ORTAK AKIL **İLERİ TÜRKİYE**

ANAHTAR PARTİ
AR-GE ve PARTİ İÇİ EĞİTİM OKULU BAŞKANLIĞI

anahtararge anahtararge

Hilal Mah. Rabindranath Tagore Cd.
No:66, 06550 Çankaya - Ankara - Türkiye
www. anahtarparti.org | arge@anahtarparti.org