DİJİTAL DÖNÜŞÜM VE SİBER GÜVENLİK DERNEĞİ

KAMUDA DİJİTAL YERLİLEŞTİRME ÖNERİLERİ RAPORU

DURUM TESPİTİ, ÇÖZÜM ÖNERİSİ VE ÜLKE ÖLÇEĞİNE YAYGINLAŞTIRMA STRATEJİSİ

KAMU SEKTÖRÜNDE DİJİTAL EGEMENLİK VE SİBER DAYANIKLILIK MİMARİSİ

7545 Sayılı Siber Güvenlik Kanunu ve Cumhurbaşkanlığı BİGR Mevzuatına Uyum Stratejisi
Metropol Ölçekli Uygulama Deneyiminin Ulusal Ölçeğe Yaygınlaştırılmasına Yönelik Model Öneri Raporu

Hazırlayan

Taner ÇITAK

Genel Müdür (CEO) | Yönetim Kurulu Üyesi — Siber Güvenlik ve Kamu Bilişim Yöneticiliğinde 29 Yıllık Tecrübe

Ağustos 2026

Raporu Hazırlayan Hakkında

Bu raporun teknokratik ve tarafsız niteliğini güçlendiren temel unsur, yazarının konuya ilişkin doğrudan sahada edinilmiş, 29 yıla yayılan üst düzey yönetim tecrübesidir. Aşağıda bu tecrübenin siber güvenlik ve kamu yöneticiliği boyutlarını öne çıkaran bir özet sunulmaktadır.

Taner Çıtak — Genel Müdür (CEO) | Yönetim Kurulu Üyesi

Bilişim, telekomünikasyon ve enerji sektörlerinde 29 yıllık mühendislik, proje yönetimi, genel müdürlük ve yönetim kurulu üyeliği deneyimine sahip bir üst düzey yönetici olarak, kurumların stratejik dönüşüm ve büyüme süreçlerine liderlik etmiştir.

Siber Güvenlik ve Veri Yönetişimindeki Tecrübesi

- Kamu bünyesinde veri merkezi, bulut, siber güvenlik operasyon merkezi (SOC) ve telekomünikasyon altyapılarının kurulması ve kesintisiz yönetiminden bizzat sorumlu olmuştur.
- KVKK/GDPR uyumu ile ISO 27001 ve ISO 27701 gibi kurumsal bilgi güvenliği yönetişim süreçlerini denetlemiştir.
- En son siber güvenlik ve veri koruma teknolojileri şirketinde Genel Müdür (CEO) olarak, kişisel veri yönetimi ve dijital güvenlik rehberi uyum yazılımlarının ürün ve satış stratejilerini yönetmiş; sızma testi, ISO 27001 danışmanlığı ve KVKK uyum hizmetlerinin sunumunu denetlemiştir.

Kamu Yöneticiliğindeki Tecrübesi

- Türkiye'nin en büyük kamu yerel yönetim teknoloji ekosistemlerinden birinde Genel Müdür Vekili (CEO), Genel Müdür Yardımcısı (CIO) ve Bilişim Teknolojileri Müdürü kademelerinde toplam altı yılı aşkın süreyle görev yapmış; bu süreçte kurumun merkezi veri merkezini ve 32 iştirak/birime hizmet veren paylaşımlı bulut ve siber güvenlik altyapısını bizzat yönetmiştir.
- Kurumsal yönetişim, bütçe yönetimi, dijital dönüşüm ve akıllı şehir projelerinde (IoT, RPA, veri analitiği) üst düzey karar verici olarak görev almıştır.
- Kariyeri boyunca telekomünikasyon altyapı şirketlerinde kurucu genel müdürlük, yönetim kurulu üyeliği ve grup genel müdürlüğü görevlerini yürütmüştür.

Eğitim

Yeditepe Üniversitesi İşletme Yüksek Lisansı (MBA, İngilizce, 2002–2004); Yıldız Teknik Üniversitesi Elektrik Mühendisliği (1993–1997).

Yazarın bu raporda sunduğu tespit ve öneriler doğrudan sahada edindiği yönetim tecrübesine ve kamuya açık kurumsal verilere dayanmaktadır.

İçindekiler

1. Yönetici Özeti

2. Küresel Konjonktür: Dijital Egemenlik ve Bulut Bağımsızlığı

3. Ulusal Düzenleyici Çerçeve: Genelgelerden Bağlayıcı Kanuna

4. Metropol Ölçekli Altyapı Laboratuvarı: Bir Vaka Analizi

   4.1 Kurumsal Yapı

   4.2 Veri Merkezi Üzerinden Paylaşımlı Hizmet Modeli — Olmazsa Olmaz Bileşen

   4.3 Performans Göstergeleri

5. Model Analizi: Güçlü Yönler, Riskler ve Çıkarılan Dersler

6. Kamu Genelinde Öncelikli Yerlileştirme Planı (Uyum Matrisi)

7. Stratejik Yol Haritası: Ülke Ölçeğine Yaygınlaştırma

8. Yazarın Değerlendirmesi: Uygulamanın Pozitif ve Negatif Yönleri

9. Sonuç ve Üst Düzey Karar Vericilere Öneriler

1. Yönetici Özeti

Kamu kurum ve kuruluşlarında kullanılan yabancı menşeli yazılım, bulut altyapısı ve siber güvenlik servisleri; tedarik zinciri ambargoları, arka kapı (backdoor) riskleri ve küresel siber casusluk faaliyetleri nedeniyle artık salt ekonomik bir bağımlılık unsuru değil, doğrudan bir ulusal güvenlik ve egemenlik zafiyetidir.

Mart 2025'te yürürlüğe giren 7545 sayılı Siber Güvenlik Kanunu ile kurulan Siber Güvenlik Başkanlığı, kritik altyapı statüsündeki kamu birimlerine siber güvenlik ürün ve hizmetlerini yalnızca "yetkilendirilmiş tedarikçilerden" temin etme zorunluluğu getirmiştir. Bu yükümlülüklere uyumsuzluğun 100 milyon TL'ye varan idari para cezaları ile yaptırıma bağlanması, konuyu kurumsal bir tercihten çıkarıp yasal bir zorunluluğa dönüştürmüştür.

Bu strateji belgesi; Türkiye'nin en büyük metropol ölçekli, çok lokasyonlu ve yüksek veri hacmine sahip bir kamu bilişim ekosisteminde bizzat kurulan ve işletilen yerlileştirme ile altyapı bağımsızlığı pratiğini, tarafsız bir vaka analizi (case study) olarak masaya koymaktadır. Rapor; sistemin operasyonel doğrularını, finansal ve yönetimsel risklerini şeffaflıkla değerlendirerek, bu deneyimin ülke geneline nasıl ölçeklenebileceğine dair kamu karar vericileri için somut bir yol haritası sunmaktadır.

Raporun merkezinde yer alan temel tespit şudur: küçük ve orta ölçekli kamu kurumlarının tek başlarına kuramayacakları siber güvenlik (SOC) ve veri merkezi altyapısı, Metropol ölçeğinde geliştirilmiş "Veri Merkezi Üzerinden Paylaşımlı Hizmet Modeli" üzerinden devletin yerli firmaları ve DMO kataloğundaki ürünlerle en az maliyetle ve en yüksek uyum güvencesiyle kamu geneline yaygınlaştırılabilir. Bu model, raporun ilerleyen bölümlerinde ayrıntılandırıldığı üzere, kamu genelinde siber dayanıklılığın sürdürülebilir şekilde tesisi için olmazsa olmaz bir yapı taşı olarak değerlendirilmektedir.

2. Küresel Konjonktür: Dijital Egemenlik ve Bulut Bağımsızlığı

Devletlerin kamu bilişim altyapısını yerli alternatiflerle tahkim etme çabası küresel bir standart haline gelmiştir. Bu hareket başlıca üç hukuki araçla yürütülmektedir: yürütme kararnameleri ve zorunlu takvimler, ürüne özel idari yasaklar ve tedarik kriterleri/düzenleyici çerçeveler.

- Çin'in finans, enerji ve kamu teşebbüslerini yabancı yazılımdan arındırmayı hedefleyen gizli "Document 79" direktifi (2027 hedefi), Microsoft ve Cisco gibi devlerin Çin pazar payını %5'in altına indirmiştir.
- Rusya'nın 1 Ocak 2025 itibarıyla "dost olmayan ülkelerden" siber güvenlik hizmeti alımını yasaklayan kararnamesine rağmen kurumların ancak %20'si tam yerlileşmeyi tamamlayabilmiş; bu durum, yerli tedarikçi ekosisteminin olgunluğu gözetilmeden atılan adımların sahada operasyonel tıkanma yaratabileceğini göstermiştir.
- ABD Ticaret Bakanlığı'nın Haziran 2024'te Kaspersky ürünlerine getirdiği tam satış ve kullanım yasağı ile Almanya BSI'nin benzer idari uyarıları, tekil siber güvenlik aktörlerine yönelik müdahalelerin küreselleştiğini ortaya koymuştur.
- Avrupa Birliği, Kasım 2025'te devreye giren Gaia-X Trust Framework 3.0 (Danube) ve Nisan 2026'da uygulamaya konan 180 milyon avro bütçeli "Bulut Egemenliği Çerçevesi" ile sertifikasyon ve egemenlik kriterleri üzerinden dolaylı bir yerlileştirme yürütmektedir.
- Hindistan, 2020 yılından itibaren ulusal güvenlik gerekçesiyle çok sayıda yabancı mobil uygulamayı dalgalar halinde yasaklamış; eşzamanlı olarak "Atmanirbhar Bharat" (Kendine Yeten Hindistan) girişimi çerçevesinde kamu ihalelerinde yerli üreticilere öncelik tanımış ve ulusal standart sertifikasyonunu elektronik/bilişim ürünleri ithalatında ön şart haline getirmiştir.

Bu örnekler, yerlileştirmenin evrensel bir kamu politikası önceliği olduğunu, ancak kullanılan aracın ülkeden ülkeye değiştiğini göstermektedir: bazı ülkeler yürütme kararnameleriyle zorunlu takvim dayatırken, bazıları ürüne özel idari işlemlerle hareket etmekte, bazıları ise tedarik kriterleri ve sertifikasyon çerçeveleriyle dolaylı bir yerlileştirme uygulamaktadır. Türkiye'nin konumu, genelge, strateji belgesi ve nihayetinde bağlayıcı kanunu aşamalı olarak birleştiren bir model sunmaktadır.

Bu örnekler, yerlileştirmenin evrensel bir kamu politikası önceliği olduğunu; ancak siyasi kararlılığın tek başına yeterli olmadığını, uygulamanın tedarikçi ekosistemi olgunluğuna ve doğru mimari tercihlere bağlı olduğunu göstermektedir.

3. Ulusal Düzenleyici Çerçeve: Genelgelerden Bağlayıcı Kanuna

Türkiye'de kamuda yerlileşme stratejisi, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO) koordinasyonunda yürütülen 2019/12 sayılı (Bilgi ve İletişim Güvenliği Tedbirleri) ve 2023/13 sayılı (Kamuda Açık Kaynak Kodlu Yazılım Kullanımı) Cumhurbaşkanlığı Genelgeleri ile yapısal bir zemine oturmuştur. Bu genelgeleri, 7 Eylül 2024 tarihli Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028) izlemiştir.

19 Mart 2025'te yürürlüğe giren 7545 sayılı Siber Güvenlik Kanunu, konuyu idari bir tavsiye olmaktan çıkarıp yasal bir zorunluluğa dönüştürmüştür. Kanun uyarınca: kritik altyapı kapsamındaki tüm kamu kurumları, siber güvenlik ürün ve hizmetlerini yalnızca Siber Güvenlik Başkanlığı tarafından "yetkilendirilmiş tedarikçilerden" temin etmek zorundadır; bildirim, tedbir alma ve yetkilendirilmiş yerli/millî ekosistem oyuncularını kullanma yükümlülüklerine aykırılık, 1 milyon TL ile 100 milyon TL arasında idari para cezası yaptırımına bağlanmıştır.

Dolayısıyla kamu genelinde yürütülecek bir yerlileştirme projesi, artık yalnızca bir bütçe tasarrufu hamlesi değil, kurum yöneticilerini yasal ve mali şahsi sorumluluktan koruyan bir mevzuat uyum kalkanıdır. Siber Güvenlik Başkanlığı koordinasyonundaki USOM, 2025 yılı sonu itibarıyla 101.000'den fazla kötücül bağlantıyı etkisiz hale getirmiştir.

4. Metropol Ölçekli Altyapı Laboratuvarı: Bir Vaka Analizi

Teorik yerlileştirme modellerinin karmaşık, çok lokasyonlu ve milyonlarca kullanıcıya dokunan devasa bir kamu yapısında çalışıp çalışmayacağını test etmek amacıyla, Türkiye'nin en büyük metropol bilişim altyapısına sahip bir kamu yerel yönetim ekosistemi ("Metropol") ve buna bağlı Teknoloji Grubu Şirketleri, dönemsel bir laboratuvar ve vaka analizi olarak incelenmiştir.

4.1 Kurumsal Yapı

Metropol, bilişim ve telekomünikasyon hizmetlerini iştirakler teknoloji grup başkanlığı koordinasyonunda birden fazla iştirak şirketi üzerinden yürütmektedir: güvenlik kamerası donanımı ile görüntü/ses sistemlerinde öne çıkan bir iştirak; veri barındırma, bulut ve telekomünikasyon altyapısında faaliyet gösteren Teknoloji Grubu Şirketleri ana unsuru; ve kentsel ödeme/iş uygulamaları sistemlerini işleten bir diğer iştirak. Türkiye'nin en büyük 500 bilişim şirketini sıralayan bağımsız bir araştırmanın güncel sonuçlarına göre bu üç iştirak de listede üst sıralarda yer almıştır.

4.2 Veri Merkezi Üzerinden Paylaşımlı Hizmet Modeli — Olmazsa Olmaz Bileşen

Bu ekosistemde hayata geçirilen ve kamu geneline ölçeklenebilecek mimarinin merkezinde, tek bir Merkezi Veri Merkezi ve Altyapı katmanı (özel/hibrit bulut) bulunmaktadır. Bu katman üzerine iki ana hizmet katı kurulmuştur: siber güvenlik katı (merkezi SOC hizmeti, uç nokta analizi, BİGR ve KVKK uyumu) ve dijital dönüşüm katı (yerli e-posta, robotik süreç otomasyonu, veri analitiği).

Mimarinin işleyiş mantığı basittir: tüm iştirak ve birimler kendi sunucu odalarını kurmak yerine merkezi veri merkezine bağlanır; siber güvenlik ve dijital dönüşüm hizmetleri buradan tek bir yönetişim çatısı altında, standardize edilmiş güvenlik politikalarıyla tüm bağlı kurumlara eşzamanlı olarak sunulur. Bu sayede hem yatırım tekrarının önüne geçilir hem de denetim ve uyum süreçleri tek bir merkezden yürütülebilir hale gelir; kamu genelinde ölçeklendirildiğinde aynı mantık, il/ilçe ve bakanlık düzeyindeki kurumlar için de geçerli olacaktır.

Vaka analizinin kamu politikası açısından en kritik sonucu şudur: küçük ve orta ölçekli kamu birimlerinin tek başlarına kuramayacakları yüksek maliyetli siber güvenlik (SOC) ve veri merkezi altyapısı, ancak merkezi bir Veri Merkezi Üzerinden Paylaşımlı Hizmet Modeli ile ekonomik ve operasyonel olarak sürdürülebilir hale gelmektedir. Bu rapor kapsamında incelenen alternatif senaryolarda, paylaşımlı veri merkezi mimarisinden vazgeçilmesi hem maliyeti hem de uyum riskini kabul edilemez seviyeye çıkarmaktadır; bu nedenle söz konusu model, kamu genelinde yerlileştirme stratejisinin olmazsa olmaz bileşeni olarak konumlandırılmalıdır.

Bu altyapı mimarisi, Türkiye'nin en prestijli bağımsız bilişim araştırması olan ilgili sektör araştırmasının güncel (2024 ve 2025) sonuçlarında kendi alanında üst sıralarda yer almış ve "Veri Merkezi Hizmetleri" kategorisinde birincilik ödülüne layık görülmüştür. Konsolide cirosunu 1,3 milyar TL barajının üzerine çıkaran ve 32 farklı entegre kamu birimine/iştirakine kesintisiz hizmet sunan bu model, küçük ve orta ölçekli kamu birimlerinin tek başlarına kuramayacakları altyapıyı merkezi bir havuzdan güvenle alabilmelerini sağlamaktadır.

4.3 Performans Göstergeleri

Teknoloji Grubu Şirketleri'nin yıllık faaliyet sonuçlarına yansıyan büyüme, yerlileştirme yatırımlarının somut çıktısıdır. İlgili iştirakin geliri, birkaç yıl içinde yaklaşık on katına çıkarak 1,3 milyar TL barajını aşmış; aynı dönemde 1.000'den fazla kritik noktaya fiber altyapı götürülmüş, metro hatlarında internet hizmeti yeniden devreye alınmıştır.

Bağımsız sektör araştırmasının sonuçlarına göre Teknoloji Grubu Şirketleri, genel sıralamada ilk 100 içinde yer almış ve "Veri Merkezi Hizmetleri" kategorisinde birincilik ödülü almıştır; grup bünyesindeki diğer iştirakler de aynı listede yer bulmuştur. Bu sonuç, bir yerel yönetim iştirakinin ulusal ölçekte özel sektör bilişim şirketleriyle rekabet edebilir bir veri merkezi/bulut altyapısı kurabildiğini göstermektedir.

Bu büyüme görünümünün yanında, konsolide faaliyet raporu verilerine göre ilgili iştirakin aynı dönemde küçük miktarda da olsa zarar kaydettiği bildirilmiştir. Bu veri, altyapı yatırımlarının gelir tablosuna kısa vadede doğrusal

yansımadığını ve finansal sürdürülebilirliğin yerlileştirme başarısının ayrılmaz bir parçası olarak izlenmesi gerektiğini hatırlatması açısından bu analize dengeli bir unsur olarak eklenmiştir.

5. Model Analizi: Güçlü Yönler, Riskler ve Çıkarılan Dersler

Bir sistemin mimarı olmak, onun zayıf yönlerini ve getirdiği riskleri de şeffaflıkla ortaya koymayı gerektirir. Bizzat sahada edinilen tecrübeye dayanarak, model vaka analizinden kamu sektörü için çıkarılan kritik dersler aşağıda özetlenmiştir.

5.1 Güçlü Yönler (Tekrarlanabilir Doğrular)

- Kademeli Doğrulama (Sandbox Etkisi): Geliştirilen yerli çözümler önce Teknoloji Grubu Şirketleri'nin kendi iç grup şirketlerinde (32 iştirak ve birim) test edilmiş, referanslandırılmış ve ardından dış kamu kurumlarına açılmıştır. Kamu, rüştünü iç pazarda ispatlamamış hiçbir ürünü doğrudan ana omurgaya almamalıdır.
- Hibrit İş Birlikleri ve Çeviklik: Tamamen yerli muadili bulunmayan katmanlarda küresel ölçekteki yerli operatörler ve bulut sağlayıcıları ile hibrit mimariler kurulmuştur. Bu, "ya hep ya hiç" katılığı yerine operasyonel sürekliliği koruyan rasyonel bir ara adımdır.
- Önce Kendi Ekosisteminde Kanıtla, Sonra Kamuya Yaygınlaştır: Bu sıralama, diğer kamu kurumları için tekrarlanabilir bir model sunmaktadır.

5.2 Riskler ve Eksiklikler (Kaçınılması Gereken Hatalar)

- Finansal Sürdürülebilirlik Bariyeri (TCO): İlgili dönemde yüksek altyapı yatırımları nedeniyle ciro büyümesine rağmen kamu iştirakinde dönemsel mali zararlar raporlanmıştır. Çıkarılan ders: Toplam Sahip Olma Maliyeti (TCO) ve doğru fiyatlandırma politikası baştan kurgulanmazsa, teknik başarı finansal sürdürülemezlik duvarına çarpar.
- Yapay Zekâda Derinlik Sorunu: Kurumsal söylemlerde yapay zekâ yoğun şekilde vurgulanmasına rağmen, yerel kurum imkanlarıyla özgün bir Büyük Dil Modeli (LLM) geliştirmek kaynak israfıdır. Kamu kurumları kendi yapay zekâ modellerini üretmeye çalışmamalı; ulusal ölçekteki Kumru LLM (VNGRS) veya T3 AI gibi platformları kendi güvenli sunucularına (on-premise) kurarak entegre etmelidir.
- Değişim Yönetimi ve İnsan Faktörü: Pardus ve LibreOffice geçişlerinde yaşanan en büyük tıkanıklık teknik yetersizlik değil, personel alışkanlıklarıdır. İdari bir zorlama yerine, kullanıcı adaptasyon eğitimleri projenin sıfırıncı gününe yerleştirilmelidir.

Bu risk tablosu, Rusya örneğinde gözlemlenen "siyasi kararlılığın tek başına yeterli olmadığı" tespitiyle örtüşmektedir: maliyet ve sürdürülebilirlik sorunları çözülmediği sürece yerlileştirme hedefleri sahada tıkanabilmektedir.

6. Kamu Genelinde Önerilen Öncelikli Yerlileştirme Planı (Uyum Matrisi)

Aşağıdaki matris, kamuda yaygın kullanılan yabancı çözümleri, 7545 sayılı Kanun uyumluluğu ve DMO Teknolojik Ürün Kataloğu kayıt durumlarına göre önceliklendirerek yerli alternatiflerinin olgunluk durumu ile eşleştirmektedir.

Sıra	Öncelik Grubu	Kategori	Yerli Çözüm Olgunluğu	Uyum Notu
1	1 — Yapay Zekâ	Büyük Dil Modeli / YZ Entegrasyonu	Erken Aşama	Yerli çözümler beta/erken operasyonel aşamada; on-premise kurulum mümkün. Pilot uygulama ile doğrulama önerilir.
2	2 — Siber Güvenlik	Güvenlik Duvarı / UTM	Olgun	Kategori olgun; kritik altyapılarda uzun süreli saha referansı mevcut. Doğrudan geçişe uygun.
3	2 — Siber Güvenlik	SIEM / Güvenlik İzleme (SOC)	Olgun	Kategori olgun; paylaşımlı SOC mimarilerinde test edilmiş operasyonel yetkinlik mevcut.
4	2 — Siber Güvenlik	KVKK Uyum Yazılımı	Operasyonel	Operasyonel; kamu tedarik kataloglarında listeleniyor ve VERBİS süreçleriyle uyumlu.
5	2 — Siber Güvenlik	GRC / BİGR Uyumu	Operasyonel	Operasyonel; kamu tedarik kataloglarında listeleniyor ve BİGR uyum süreçlerini destekliyor.
6	2 — Siber Güvenlik	Uç Nokta Güvenliği (Antivirüs/EDR)	Gelişmekte	Gelişmekte; ürün doğrulama ve yetkilendirme süreçleri devam ediyor. Kademeli geçiş önerilir.
7	3 — Bulut & Veri Merkezi	IaaS / Genel Bulut	Olgun	Operasyonel; yurt içinde konumlu veri merkezleri sayesinde KVKK gerekliliklerini karşılıyor.
8	4 — Üretkenlik	Masaüstü İşletim Sistemi & Ofis	Operasyonel	Operasyonel; 2023/13 sayılı Genelge kapsamında tanımlı ve doğrulanmış göç metodolojisi mevcut.

7. Stratejik Yol Haritası: Ülke Ölçeğine Yaygınlaştırma

Acil Uyum Fazı (0–12 Ay)

7545 sayılı Kanun uyarınca siber güvenlikte uç nokta (EDR) ve SIEM/SOAR katmanlarında yetkilendirilmiş yerli ürünlere geçiş pilotları başlatılır. Metropol'ün paylaşımlı SOC modeli, talep eden diğer büyükşehir belediyelerine ve kamu kurumlarına paylaşımlı hizmet olarak açılır. DMO kataloğunda kayıtlı yerli çözümlerle Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO) BİGR uyum açıkları kapatılarak idari ceza riskleri bertaraf edilir.

Platform ve Yapay Zekâ Entegrasyonu (1–3 Yıl)

Tekil siber güvenlik ürünleri merkezi bir platform mimarisine (M-SOC) bağlanır. Kurumsal doküman işleme, vatandaş ilişkileri yönetimi ve arşiv tarama süreçlerinde Kumru LLM, Tübitak Bilge veya T3 AI gibi yerli büyük dil modelleri kamu kurumlarının kendi lokal sunucularına (on-premise) kurularak veri güvenliği tam kontrol altına alınır. Bulut altyapısında çoklu yerli bulut stratejisi benimsenir.

Tam Dijital Egemenlik Fazı (3–5 Yıl)

Masaüstü işletim sistemlerinde ve ofis paketlerinde Pardus/LibreOffice geçişleri, kurumsal değişim yönetimi ve kullanıcı adaptasyon eğitimleriyle tüm yaygın kamu birimlerine ulaştırılır. Altyapıda bulut bağımsız (cloud-agnostic) çoklu yerli bulut mimarisine tam geçiş sağlanır; Veri Merkezi Üzerinden Paylaşımlı Hizmet Modeli, tüm ülke, il ve ilçe ölçeğindeki kamu kurumlarını kapsayacak şekilde ulusal bir omurgaya dönüştürülür.

8. Yazarın Değerlendirmesi: Uygulamanın Pozitif ve Negatif Yönleri

Yazarın, hem kamu yöneticiliğinde hem de siber güvenlik/veri koruma alanında edindiği doğrudan tecrübeye dayanan değerlendirmesi şu şekilde özetlenebilir:

Pozitif Yönler

- Paylaşımlı hizmet modeli, küçük ölçekli kamu kurumlarının münferiden karşılayamayacağı SOC ve veri merkezi maliyetlerini merkezi bir havuzda toplayarak ölçek ekonomisi sağlamaktadır.
- Kademeli doğrulama (önce iç grupta test, sonra dış kamuya açma) yaklaşımı, yerli ürünlerin olgunlaşmadan ana omurgaya alınması riskini azaltmaktadır.
- 7545 sayılı Kanun'un getirdiği yaptırım çerçevesi, yerlileştirmeyi gönüllü bir tercihten kurumsal bir zorunluluğa dönüştürerek uygulamayı hızlandırma potansiyeli taşımaktadır.

Negatif Yönler / Dikkat Edilmesi Gereken Riskler

- Altyapı yatırımlarının kısa vadede gelir tablosuna doğrusal yansımaması, finansal sürdürülebilirlik açısından merkezi bütçe desteği veya net bir fiyatlandırma politikası gerektirmektedir.
- Yapay zekâ alanında kurumsal söylem ile somut ürün derinliği arasındaki fark, ulusal ölçekli LLM girişimleriyle (Kumru LLM, Tübitak Bilge, T3 AI) tamamlanmadığı sürece açık kalmaya devam edecektir.
- Paylaşımlı hizmet modelinin ulusal ölçeğe taşınması, tek bir yerel yönetim iştirakinin kapasitesini aşan bir yönetişim ve finansman mimarisi (örneğin merkezi bir kamu SOC/veri merkezi işletmecisi) gerektirmektedir; aksi halde model, yerel başarıyı ulusal ölçekte tekrarlamakta zorlanabilir.

9. Sonuç ve Üst Düzey Karar Vericilere Öneriler

Yazılım ve siber güvenlikte yerlileştirme; dönemsel siyasi rüzgarlardan, kurumlar arası rekabetten veya yerel halkla ilişkiler faaliyetlerinden tamamen bağımsız, devletin en üst düzey stratejik önceliğidir. Karşımızda, siber uzayda egemenlik iddiasını yasal yaptırımlarla tahkim etmiş bir devlet iradesi (Siber Güvenlik Başkanlığı) ve uymakla yükümlü olduğumuz modern bir mevzuat (7545 sayılı Kanun) bulunmaktadır.

Metropol ölçeğindeki karmaşık ve zorlu test yataklarından elde edilen en önemli teknokratik tecrübe; yerlileştirmenin rasyonel, finansal olarak sürdürülebilir, risk analizleri yapılmış ve Veri Merkezi Üzerinden Paylaşımlı Hizmet Modeli temelinde platform tabanlı bir mimariyle yürütülmesi gerektiğidir.

Bu doğrultuda, devletin en üst kademelerine sunulmak üzere aşağıdaki öneriler öne çıkarılmaktadır:

- Metropol ölçeğinde doğrulanmış Veri Merkezi Üzerinden Paylaşımlı Hizmet Modeli, küçük ve orta ölçekli kamu kurumları için ulusal düzeyde zorunlu/teşvikli bir referans mimari olarak benimsenmelidir; bu bileşen, kamu genelinde siber dayanıklılığın olmazsa olmaz temel taşı olarak konumlandırılmalıdır.
- Yerlileştirme projelerinde Toplam Sahip Olma Maliyeti (TCO) analizi ve merkezi fiyatlandırma/finansman mekanizması, projenin ilk gününden itibaren tasarlanmalıdır.
- Yapay zekâ yerlileştirmesi, yerel ölçekli tekrarlardan kaçınılarak Kumru LLM, Tübitak Bilge ve T3 AI gibi ulusal girişimler üzerinden konsolide edilmelidir.
- Değişim yönetimi ve kullanıcı adaptasyonu, teknik geçişle eşzamanlı, projenin sıfırıncı gününden itibaren planlanmalıdır.
- Metropol örneğinde görülen finansal zarar riskinin ulusal ölçekte tekrarlanmaması için, paylaşımlı hizmet modelinin ulusal omurgaya taşınması sürecinde merkezi bütçeden ayrılacak bir kurulum/işletme fonu ile net bir hizmet bedeli tarifesi baştan tanımlanmalıdır.

Sonuç olarak, bu raporun ortaya koyduğu durum tespiti nettir: kamu genelinde siber dayanıklılık, dağınık ve tekil çözümlerle değil, Metropol deneyiminde sınanmış Veri Merkezi Üzerinden Paylaşımlı Hizmet Modeli'nin ulusal ölçeğe taşınmasıyla sürdürülebilir hale gelecektir. Yazarın hem kamu yöneticiliğinde hem siber güvenlik alanında edindiği tecrübe, bu modelin sahada çalıştığını, ancak finansal disiplin ve merkezi yönetişim olmadan ulusal ölçekte tekrarlanamayacağını göstermektedir.

Bu dökümanda sunulan uyum matrisi, yol haritası ve yazarın sahada edindiği tecrübeye dayanan değerlendirme, kamu kurumlarının 7545 sayılı Kanun kapsamındaki yasal ceza risklerinden kaçınırken, eşzamanlı olarak ulusal siber dayanıklılık seviyelerini en üst düzeye çıkarmaları için tarafsız ve rehber bir model olarak tasarlanmıştır.