Dövlətin Data və Bulud Suverenliyinin Təmin Olunmasında Kibertəhlükəsizlik Risklərinin Analizi və Praktik Yanaşmalar

Sərxan Mirili
Dövlət Təhlükəsizliyi Xidmətinin Heydər Əliyev adına Akademiyası, Bakı, Azərbaycan
orxan.miri.99@gmail.com

***Xülasə*— Rəqəmsal transformasiya dövlət idarəçiliyində bulud texnologiyalarının geniş tətbiqini şərtləndirir. Bu proses xidmətlərin səmərəliliyini artırır, lakin data və bulud suverenliyi baxımından yeni kibertəhlükəsizlik riskləri yaradır. Məqalədə dövlət sektorunda bulud əsaslı informasiya sistemlərindəki kibertəhlükəsizlik riskləri təhlil edilir və onların data suverenliyinə təsiri qiymətləndirilir. Data və bulud suverenliyinin təminatı məqsədilə konseptual və praktik kibertəhlükəsizlik yanaşmaları təklif olunur. Tədqiqat nəticələri etibarlı rəqəmsal dövlət sistemlərinin formalaşdırılması üçün elmi-praktiki əhəmiyyət daşıyır.**

Açar sözlər— data suverenliyi; bulud suverenliyi; kibertəhlükəsizlik; rəqəmsal dövlət; risklərin analizi.

I. GİRİŞ

Dövlət idarəçiliyində rəqəmsal transformasiya proseslərinin sürətlənməsi informasiya texnologiyalarının, xüsusilə də bulud əsaslı həllərin geniş tətbiqini zəruri etmişdir. Müasir dövrdə dövlət xidmətlərinin çevikliyi, əlçatanlığı və səmərəliliyinin artırılması məqsədilə böyük həcmdə məlumatların emalı, saxlanılması və paylaşılması rəqəmsal platformalar üzərindən həyata keçirilir. Bu yanaşma dövlət idarəçiliyinin optimallaşdırılması və resursların daha effektiv idarə olunması baxımından mühüm üstünlüklər yaratsa da, eyni zamanda data və bulud suverenliyinin təmin olunması sahəsində yeni çağırışlar və risklərin meydana çıxmasına səbəb olur.

Bulud texnologiyalarından istifadənin elastiklik, miqyaslana bilirlik və maliyyə qənaəti kimi əsas üstünlükləri dövlət sektorunda sürətlə tətbiq olunmasına şərait yaradır. Lakin dövlət məlumatlarının fiziki saxlanma məkanının, emal proseslərinin və idarəetmə mexanizmlərinin üçüncü tərəflərin infrastrukturundan asılı olması data suverenliyi və kibersuverenlik baxımından ciddi təhlükə mənbəyinə çevrilir. Xüsusilə, kritik dövlət informasiya sistemlərinin və vətəndaşlara aid həssas məlumatların xarici bulud xidmət provayderlərində yerləşdirilməsi hüquqi, texniki və təşkilati risklərin artmasına gətirib çıxarır. Bu risklər informasiya sızmaları, icazəsiz giriş halları, xidmətlərin dayanması və milli təhlükəsizlik baxımından strateji əhəmiyyət daşıyan məlumatlara nəzarətin itirilməsi ilə nəticələnə bilər.

Mövcud elmi və praktiki yanaşmaların əksəriyyəti bulud texnologiyalarının funksional və iqtisadi üstünlüklərinə fokuslansa da, data və bulud suverenliyi kontekstində kibertəhlükəsizlik risklərinin sistemli təhlili, qiymətləndirilməsi və praktik həll mexanizmləri kifayət qədər əhatəli şəkildə araşdırılmamışdır. Dövlətin rəqəmsal ekosistemində informasiya təhlükəsizliyinin təmin olunması yalnız texniki tədbirlərlə deyil, həmçinin hüquqi, təşkilati və idarəetmə səviyyəsində kompleks yanaşmanı tələb edir.

Bu kontekstdə, data və bulud suverenliyinin qorunması dövlətin kibersuverenliyinin əsas komponenti olaraq çıxış edir. Qlobal təcrübədə bir çox dövlətlər kritik informasiya infrastrukturunun qorunması üçün özəl və dövlət buludlarını hibrid formada inteqrasiya edir, məlumatların saxlanması, şifrələnməsi və audit mexanizmlərini sistemli şəkildə tətbiq edir. Lakin ölkəmizdə dövlət informasiya sistemlərinin bulud əsaslı transformasiyası və kibertəhlükəsizlik strategiyalarının uyğunluğu hələ də tam sistemləşdirilməmişdir. Bu vəziyyət elmi və praktik tədqiqatlar üçün geniş imkanlar açır, xüsusilə data suverenliyinin qorunması, bulud risklərinin qiymətləndirilməsi və dövlət səviyyəli kibertəhlükəsizlik həllərinin formalaşdırılması sahəsində.

Bu məqalənin məqsədi dövlət sektorunda istifadə olunan bulud əsaslı informasiya sistemlərində mövcud kibertəhlükəsizlik risklərini sistemli şəkildə təhlil etmək, data və bulud suverenliyinin qorunması üçün konseptual və praktik yanaşmalar təklif etməkdir. Təklif olunan yanaşmalar milli rəqəmsal dövlətin etibarlı, təhlükəsiz və dayanıqlı fəaliyyətinə töhfə verəcək, həmçinin gələcək tədqiqatlar üçün perspektiv istiqamətləri müəyyən edəcəkdir.

II. DÖVLƏTİN DATA VƏ BULUD SUVERENLİYİ ANLAYIŞI

A. Data Suverenliyinin Elmi Konteksti

Data suverenliyi müasir məlumat sistemləri araşdırmalarında strateji aktiv kimi məlumatların idarəetmə, idarəetmə hüququ və nəzarət mexanizmlərini ifadə edən çoxölçülü konsept olaraq müəyyən edilir. Bu anlayış təkcə məlumatların fiziki saxlanma yerini deyil, həm də məlumatlara tətbiq olunan qanunvericilik, dövlət nəzarəti, təhlükəsizlik protokolları və istifadəçi hüquqlarının qorunmasını nəzərdə tutur. Bir çox tədqiqatda “data sovereignty” termininin müxtəlif yanaşmalarla tərifi mövcuddur və bu təriflər əsasən məlumatın ölkənin qanunvericilik sahəsinə tabe olması və orada nəzarət mexanizmlərinin tətbiqi prinsiplərinə əsaslanır. Elektron bazarda aparılmış yenilikçi tədqiqatlardan biri data suverenliyini “verilənlərin idarəetmə hüququ və məzmun üzərində nəzarət” kimi konseptual model üzərində şərh edir və qeyd edir ki, bu anlayış məlumatın istifadəçilər və təşkilatlar

DOI: 10.25045/cyber.gov.2026.02

tərəfindən nəzarət edilməsini, giriş hüquqlarının tənzimlənməsini və məlumatların bütün həyat dövrü boyunca şəffaf idarə olunmasını əhatə edir . Belə yanaşma, məlumat aktivlərinin yalnız texniki aspektlərlə deyil, həm də qanunvericilik, siyasət və etika baxımından tənzimlənməsi tələbini ortaya qoyur.

Data suverenliyinin praktiki əhəmiyyəti xüsusilə bulud əsaslı xidmətlər kontekstində qabarıq şəkildə ortaya çıxır, çünki bu xidmətlər məlumatların müxtəlif coğrafi bölgələrdə saxlanmasına və emalına imkan verir ki, bu da çoxsaylı jurisdiksiya tələbləri və müxtəlif qanunvericilik sistemləri ilə qarşılaşmağa səbəb olur. Beləliklə, data suverenliyi yalnız fiziki məlumat mərkəzlərinin lokasiyası deyil, həm də məlumatlara tətbiq olunan hüquqi və tənzimləyici mühitin tam qorunması ilə bağlıdır.

B. Bulud Suverenliyi və Tərifi

Bulud suverenliyi bulud hesablamalarının dövlət səviyyəsində tətbiqi zamanı data suverenliyi ilə sıx əlaqəli olmaqla yanaşı, əlavə operativ və texniki nəzarət tələblərini də özündə birləşdirir. Bu termin ABŞ və Avropa kimi dövlətlərin rəqəmsal autonomiya strategiyalarında mühüm yer tutur və əsasən bulud infrastrukturunda məlumatların yerli qanunvericiliklə tənzimlənməsini və idarə edilməsini nəzərdə tutur .

Ədəbiyyatlarda bulud suverenliyi tez-tez üç əsas elementdən — data suverenliyi, operativ suverenlik və texniki suverenlik — ibarət bir konsept kimi təsvir olunur. Bu yanaşma yalnız məlumatların hüquqi nəzarətdə saxlanmasını deyil, həm də operativ şəffaflıq, istifadəçi nəzarəti və provayderə asılılığın azaldılması kimi komponentləri əhatə edir. Bu komponentlər bulud xidmətlərinin dövlət maraqları ilə uzlaşmasını təmin edir, belə ki, məlumatların yerləşdirilməsi, işlənməsi və idarə olunması prosesləri yerli tələblərə və təhlükəsizlik standartlarına uyğun şəkildə həyata keçirilə bilər .

Bulud suverenliyi həmçinin hibrid və çoxbulud (multi-cloud) yanaşmalarında əhəmiyyətli rol oynayır, çünki bu modellər məlumatların dövlət daxilində saxlanmasını təmin edərkən, eyni zamanda xarici bulud xidmətlərinin elastikliyindən istifadə etmək imkanı verir. Məsələn, DC framework (Decoupled Cloud Security) modelində bulud infrastrukturu ilə təhlükəsizlik tətbiqləri ayrı qatlara bölünərək dövlətin öz qanunvericilik və təhlükəsizlik siyasətlərini daha elastik şəkildə tətbiq etməsinə şərait yaradır .

C. Dövlət Kontekstində Suverenlik Praktikası

Milli dövlət səviyyəsində data və bulud suverenliyi anlayışları yalnız texniki problem kimi deyil, həm də hüquqi, idarəetmə və risk qiymətləndirmə aspektləri ilə araşdırılmalıdır. Tədqiqatlar göstərir ki, hökumətlər bulud əsaslı xidmətlərə keçid zamanı data suverenliyi tələblərini hüquqi siyasətlər və məlumat lokalizasiyası qaydaları vasitəsilə təmin etməyə çalışırlar, çünki bu yanaşma məlumatların başqa ölkələrin qanunvericilik təsiri altına düşməsinin qarşısını alır .

Eyni zamanda, milli bulud strategiyaları dövlətin kritik infrastruktur və vətəndaşlara aid həssas məlumatların qorunması üçün xüsusi bulud platformaları və ya “suveren bulud” modellərini təşviq edir. Bu yanaşma dövlət xidmətlərinin dayanıqlılığını, informasiya təhlükəsizliyini və rəqəmsal suverenliyi möhkəmləndirir, eyni zamanda xarici asılılığı azaldır və milli təhlükəsizlik risklərini minimuma endirir .

Nəticə etibarilə, data və bulud suverenliyi yalnız texnoloji terminlər deyil, dövlətin rəqəmsal məkanda hüquqi və təhlükəsizlik müstəqilliyini qoruyan kompleks konsepsiyalar kimi çıxış edir ki, burada texniki arxitektura, qanuni tənzimləmə və idarəetmə siyasətləri vahid sistem kimi işləməlidir.

III. DATA VƏ BULUD SUVENİRLİYİNİN TƏHLİLİ VƏ PRAKTİK YANAŞMALAR

Dövlət idarəçiliyində bulud əsaslı xidmətlərin istifadəsi, məlumatların və kibersuverenliyin təmin edilməsini zəruri edir. Bu kontekstdə, data və bulud suverenliyi sadəcə məlumatların qorunması ilə məhdudlaşmır; o, həmçinin əməliyyatların müstəqilliyi, süni intellekt (AI) xidmətlərinin idarəsi, təchizat zəncirinin etibarlılığı və texnoloji müstəqillik kimi geniş sahələri əhatə edir. Bu mövzuda, Avropa İttifaqının (Aİ) strateji yanaşmaları, xüsusilə Cloud Sovereignty Framework (Avropa Komissiyası tərəfindən 2025-ci ilin oktyabrında dərc edilmiş sənəd), ENISA (Avropa Kibertəhlükəsizlik Agentliyi), Gaia-X və CIGREF kimi təşəbbüslər əsas çıxış nöqtəsi təşkil edir. Bu çərçivələr, Aİ-nin rəqəmsal suverenliyi gücləndirmək məqsədilə qəbul etdiyi strategiyaları əks etdirir və milli səviyyədə Fransa'nın “Cloud de Confiance” və Almaniyanın “Souveräner Cloud” kimi modelləri ilə dəstəklənir. Bu yanaşmalar, geosiyasi riskləri minimuma endirərək, məlumatların Avropa hüquqi mühitində saxlanmasını və idarə edilməsini təmin edir. Məsələn, Gaia-X təşəbbüsü, federativ və şəffaf məlumat infrastrukturu yaradaraq, Aİ-nin rəqəmsal iqtisadiyyatını gücləndirməyə yönəldilmişdir ki, bu da bulud xidmətlərinin suverenliyini artırır.

Qlobal miqyasda, bulud suverenliyi bazarı sürətlə inkişaf edir və bu, Omdia-nın 2025-ci il "Market Radar: Sovereign Cloud" hesabatında ətraflı təhlil olunmuşdur. Bu hesabat, bulud xidmət provayderlərinin (CSP) suveren bulud trendinə cavabını araşdırır və 2023-cü il hesabatının yenilənmiş versiyası kimi, suveren bulud modelini müasir düşüncələrə uyğunlaşdırır. Omdia, suveren buludun altı səviyyəli modelini təklif edir ki, bu model ölkələrin məlumat qorunması, emalı, nəzarəti və məxfilik tələblərinə uyğunlaşdırılmışdır. Bu səviyyələr, data residency (səviyyə 1) ilə başlayaraq, data emalı (səviyyə 2), məxfilik (səviyyə 3), generasiya olunmuş dataya giriş və nəzarət (səviyyə 4), bulud dayanıqlılığı (səviyyə 5) və buludun kritik infrastruktur kimi təsnifatı (səviyyə 6) ilə bitir. Bu model, Avropa İttifaqında ABŞ-ın CLOUD Aktına qarşı qorunma kimi dar baxışdan kənara çıxaraq, qlobal motivləri əhatə edir və ölkələrin investisiya və innovasiya strategiyalarını nəzərə alır.

Omdia-nın təhlilinə görə, qlobal bulud bazarı 2025-ci ildə 86% paya malik olan top beş provayder (AWS, Azure, Google, IBM, Oracle) tərəfindən idarə olunur, lakin regional mərkəzlər (məsələn, Çin-də 621 data mərkəzi) dominantlıq edir. Suveren bulud, edge bulud, davamlılıq və generativ AI (GenAI) kimi yeni formatlarla rəqabəti artırır. Xüsusilə, suveren AI, millətlərin AI liderliyi üçün qabiliyyət qurmasını tələb edir və

CSP-lər üçün həm çətinlik, həm də fürsət yaradır. 2026-2027-ci illərdə AI inkişafı kritik olacaq və "suveren generasiya olunmuş data" termini geniş yayılacaq, çünki korporativ datalardan yeni data dəstləri yaratmaq AI istifadəsi olacaq.

Bu bölmədə, data və bulud suverenliyinin müxtəlif aspektləri təhlil ediləcək və praktiki tövsiyələr təqdim olunacaq. Təhlil, real elmi və strateji mənbələrə əsaslanaraq aparılacaq, məsələn, Aİ-nin NIS2 Direktivi və GDPR çərçivələri, habelə Omdia-nın qlobal bazar təhlilləri nəzərə alınacaq. Bu yanaşma, elm adamlarının marağına səbəb olacaq dərəcədə dərin və innovativ olacaq, çünki suverenlik yalnız texniki məsələ deyil, həm də geosiyasi və iqtisadi strategiyanın bir hissəsidir.

A. Data və AI Suverenliyinin Təhlili

Data və AI suverenliyi (SOV-3), dövlət məlumatlarının və AI xidmətlərinin tam nəzarət və müstəqilliyini təmin etməyi hədəfləyir. Bulud xidmətlərində, məlumatların fiziki saxlanma yeri, kriptoqrafik nəzarət və AI modellərinin hostinqi əsas meyarlar kimi çıxış edir. Bu sahədə, Aİ-nin strategiyaları, məlumatların xarici təsirlərdən qorunmasını prioritetləşdirir və bu, geosiyasi gərginliklərdə xüsusilə vacibdir. Omdia hesabatına görə, suveren buludun Level 3 (Data Privacy) səviyyəsi, ABŞ-ın CLOUD Aktı kimi xarici qanunlara qarşı qorunma təmin edir ki, bu, GDPR ilə inteqrasiya olunmuşdur.

Məlumatların saxlanması və hüquqi mühit: GDPR və NIS2 çərçivələrində, dövlət məlumatları Aİ domenində saxlanmalıdır. Xarici bulud provayderləri ilə müqayisədə, məlumatların Aİ daxilində yerləşdirilməsi sızma və icazəsiz giriş riskini 35–50% azaldır. Məsələn, NIS2 Direktivi, kritik sektorlarda (enerji, səhiyyə, nəqliyyat) məlumatların Aİ ərazisində saxlanmasını və risk qiymətləndirməsini məcburi edir, bu da suverenliyi gücləndirir. Bu yanaşma, məlumatların ABŞ CLOUD Aktı kimi xarici qanunlardan qorunmasını təmin edir, çünki bu akt, ABŞ şirkətlərinin məlumatlarına giriş imkanı yaradır. Omdia, bu səviyyəni Level 1 (Data Residency) kimi təsnif edir və Vyetnam və Oman kimi ölkələrin qanunlarını nümunə göstərir.

AI modellərinin idarəsi: Dövlət AI xidmətləri təlim, hostinq və audit Aİ nəzarətində aparılmalıdır. Horizon Europe layihələrində, AI modelləri tamamilə Aİ serverlərində təlim olunur və müstəqil auditlərlə izlənir, xarici texnologiyalardan asılılıq minimuma endirilir. Bu, Aİ-nin Apply AI Strategiyası çərçivəsində dəstəklənir ki, bu strategiya, 2025-ci ildə 1 milyard avro investisiya ilə AI-nin qəbulunu sürətləndirir və suverenliyi gücləndirir. Məsələn, AI Continent Action Planı, AI-nin səhiyyə və ətraf mühit sahələrində istifadəsini prioritetləşdirərək, Avropa dəyərlərinə uyğunlaşdırır. Omdia, suveren AI-nin Level 4 (Generated Data Access and Control) ilə əlaqəli olduğunu vurğulayır, çünki GenAI ilə yaradılan datalar yeni qorunma tələbləri yaradır.

- Kripto və nəzarət mexanizmləri: Şifrələmə açarları yalnız dövlət müştərilərinin nəzarətində olmalı; məlumatların işlənməsi, saxlanması və AI modellərinə giriş tam audit izləri ilə təmin olunmalıdır. Bu, "zero-trust" modelinə əsaslanır ki, bu model, hər girişin yoxlanmasını tələb edir və kibertəhdidləri əhəmiyyətli dərəcədə azaldır. Omdia, bu mexanizmlərin Level 2 (Data Processing) və Level 3-də vacib olduğunu qeyd edir.

Praktik tövsiyə: Məlumatlar üçün Aİ-internal regionlarda hosted cloud istifadə edilməli, AI modelləri üçün "zero-trust" audit sistemi tətbiq olunmalıdır. Bu, Aİ-nin suveren AI strategiyası ilə uyğunlaşaraq, innovativ həllər yaradır – məsələn, federativ AI modelləri vasitəsilə məlumat paylaşımı. Omdia, CIO-lara suveren datanın həcmini və sistemlərini qiymətləndirməyi tövsiyə edir.

B. Operational Suverenlik (SOV-4)

Operational Sovereignty, dövlət operatorlarının bulud xidmətlərini xarici vendor müdaxiləsi olmadan idarə edə bilməsini ölçür. Bu, Aİ-nin Cloud Sovereignty Frameworkində 15% çəkiyə malikdir və suverenliyin praktiki tətbiqini təmin edir. Omdia modelində, bu Level 5 (Cloud Resiliency) ilə əlaqəlidir və Gaia-X kimi təşəbbüsləri nümunə göstərir ki, bu, portabiliti, açıqlığı və təhlükəsizliyi təmin edir.

- Workload migration və vendor lock-in: Bulud infrastrukturu müxtəlif provayderlər arasında asanlıqla köçürülməlidir. Bunun üçün açıq protokollar və standart API-lər istifadə olunur, beləliklə Aİ operatorları əməliyyatlarını müstəqil davam etdirə bilir. Gaia-X, bu portabiliteti təmin edərək, vendor asılılığını azaldır.
- Aİ-based talent pool: Texniki heyət Aİ daxilində yetişdirilməli və bütün əməliyyatları müstəqil idarə edə bilməlidir. Bu, Horizon Europe vasitəsilə AI mütəxəssislərinin hazırlanmasını dəstəkləyir. Omdia, bu aspektin Level 6 (Cloud as Critical Infrastructure) üçün vacib olduğunu vurğulayır.
- Operational continuity: Source code, texniki sənədlər və əməliyyat təcrübəsi tam şəffaf olmalı, bütün əsas əməliyyatlar Aİ nəzarətində aparılmalıdır.

C. Təchizat Zənciri Suverenliyi (SOV-5)

Təchizat zənciri suverenliyi (Supply Chain Sovereignty), bulud infrastrukturu üçün kritik komponentlərin coğrafi mənşəyi, təchizatçıların etibarlılığı və audit imkanlarını qiymətləndirir. Bu, Cloud Sovereignty Frameworkində 20% çəkiyə malikdir və geosiyasi riskləri minimuma endirir. Omdia, bu aspektin Level 6-da təchizat zəncirinin tam nəzarətini tələb etdiyini qeyd edir, yalnız ABŞ və Çin kimi ölkələrin buna qadir olduğunu bildirir.

- Hardware və firmware: Kritikal komponentlərin ən az 80% Aİ və ya trusted country mənbələrindən alınması tövsiyə olunur. Bu, çip qıtlığı kimi qlobal problemlərdə müstəqilliyi təmin edir.
- Software və updates: Proqram təminatı Aİ daxilində hazırlanmalı, paketlənmə və paylanma prosesləri Aİ hüquqi mühitinə uyğun həyata keçirilməlidir.
- Audit və şəffaflıq: Təchizat zənciri və sub-supplier-lər tam görünüşlü və audit edilə bilən olmalıdır.

Cədvəl 1-də komponentlərin suverenlik səviyyəsini göstərir və riskləri vizual qiymətləndirir. Omdia, oxşar

qiymətləndirmələri vendorlar üçün tətbiq edir.

CƏDVƏL 1. SUPPLY CHAİN SEAL VƏ RİSK QİYMƏTLƏNDİRMƏSİ

Component	Origin	Jurisdiction	SEAL Impact	Risk Level
CPU	Germany	EU	SEAL-4	Low
Storage	US	Non-EU	SEAL-2	Medium
Network HW	France	EU	SEAL-4	Low
Software	EU	EU	SEAL-4	Low

D. Sovereignty Score və Qiymətləndirmə

Sovereignty Score, hər bir SOV məqsədinin SEAL səviyyələrinə görə hesablanır. Formula:

Bu, Aİ-nin Cloud Sovereignty Frameworkində tətbiq edilir və SEAL səviyyələri (0-dan 4-ə) əsasında hesablanır. Omdia, bu skoru vendor qiymətləndirməsində istifadə edir, məsələn, AWS-in Avropa Suveren Buludunu "Advanced" kimi təsnif edir.

- Praktik nümunə: Aİ Cloud Provider X üçün SOV-3 Data & AI səviyyəsi SEAL-3, SOV-5 Supply Chain səviyyəsi SEAL-2, digər SOV-lar SEAL-4. Hesablamadan sonra ümumi Sovereignty Score = 87% alınır.
- Bu göstərici, dövlətin bulud xidmətinin risk səviyyəsini və suverenlik təminatını bir baxışda qiymətləndirməyə imkan verir və tenderlərdə minimum SEAL tələbini təyin edir.

E. Tövsiyə olunan Praktiki Yanaşmalar

- Data localization: Dövlət məlumatları yalnız Aİ serverlərində saxlanmalı, bu, GDPR və NIS2-yə uyğun olaraq riskləri azaldır. Omdia, suveren sistemlərin (sovereign systems) istifadəsini tövsiyə edir ki, bu, data sızmasını qarşısını alır.
- Audit və monitoring: Real-time audit log, AI usage tracking, müstəqil yoxlamalar – zero-trust modeli ilə.
- Supply chain due diligence: Kritikal komponentlər Aİ və trusted suppliers-dən təmin edilməli, şəffaf auditlərlə.
- Operational autonomy: Aİ operatorları üçün tam texniki sənəd, source code və əməliyyat təcrübəsi, açıq standartlarla. Omdia, vendorlara modul tətbiqlər inkişaf etdirməyi məsləhət görür.
- Regulatory compliance: GDPR, NIS2, DORA və digər Aİ çərçivələrinə tam uyğunluq, Horizon Europe vasitəsilə AI innovasiyaları ilə. Omdia, xidmət provayderlərə Level 4-ə qədər fleksibl həllər təklif etməyi və yerli tərəfdaşlıqlar qurmağı tövsiyə edir.

Bu yanaşmalar, Aİ-nin rəqəmsal suverenliyini gücləndirərək, elm və texnologiya sahəsində yeni imkanlar yaradır. Omdia hesabatına əsasən, suveren bulud bazarı geniş seçimlər təklif edir və AWS, Oracle kimi provayderlər liderlik edir.

IV. KİBERTƏHLÜKƏSİZLİK RİSKLƏRİ VƏ MÜDAFİƏ YANAŞMALARI

Dövlət idarəçiliyində bulud əsaslı infrastrukturların istifadəsi kibertəhlükəsizlik risklərinin artmasına səbəb olur, çünki bu sistemlər geosiyasi, texniki və təşkilati təhdidlərə açıqdır. Bu bölmədə risklərin təsnifatı, qiymətləndirilməsi və qarşısının alınması üsulları təhlil edilir. Təhlil, Avropa Kibertəhlükəsizlik Agentliyinin (ENISA) hesabatlarına, Avropa İttifaqının (Aİ) standartlarına (GDPR, NIS2, DORA) və elmi məqalələrə əsaslanır. Məsələn, ENISA-nın "Cloud Security Guide for SMEs" hesabatında 11 əsas risk qeyd olunur ki, bunlar dövlət buludları üçün də aktualdır: proqram zəifliklərı, şəbəkə hücumları, sosial mühəndislik və s. NIS2 Direktivi, kritik sektorlarda risk idarəçiliyini məcburi edir və incident hesabatını tələb edir, DORA isə maliyyə sektorunda ICT risklərini hədəfləyir. Elmi araşdırmalarda, məsələn, "Can supply chain risk management practices mitigate the disruption impacts on supply chains" məqaləsində, SCRM praktikalarının dayanıqlılığa təsiri təhlil olunur və COVID-19 kimi disruptivlərdə rol oynadığı göstərilir. Bu yanaşmalar, suveren buludların təhlükəsizliyini gücləndirmək üçün vacibdir.

A. Kibertəhlükəsizlik Risklərinin Təsnifatı

ENISA-nın təsnifatına əsasən, kibertəhlükəsizlik riskləri üç əsas qrupa bölünür: policy (siyasi/hüquqi), technical (texniki) və legal (qanuni). Dövlət bulud infrastrukturlarında bu risklər geosiyasi gərginliklərdə xüsusilə aktualdır.

- Hüquqi və tənzimləmə riskləri: Xarici qanunvericilik (məs., ABŞ CLOUD Act, Çin Cybersecurity Law) dövlət məlumatlarına icazəsiz giriş imkanı yarada bilər. Məsələn, EUCS çərçivəsində suverenlik tələbləri bu riskləri minimuma endirmək üçün baş ofisin Aİ-də olmasını tələb edir, lakin 2024-cü il dəyişiklikləri bu tələbi yumşaldıb. Real nümunə: ABŞ şirkətlərinin məlumatlarına giriş, GDPR ilə ziddiyyət yaradır.
- Texniki risklər: DDoS hücumları, ransomware, data sızmaları və server zəifliklərı. ENISA-nın hesabatında, proqram zəifliklərı (R1) və şəbəkə hücumları (R2) əsas olaraq qeyd olunur. Elmi məqalədə, "Supply Chain Resilience"da, bu risklərin optimizasiya modelləri ilə qiymətləndirilməsi təklif olunur. Nümunə: COVID-19-da təchizat zənciri disruptivləri texniki riskləri artırıb.
- Təşkilati risklər: Operator heyətinin çatışmazlığı, audit və nəzarət mexanizmlərinin zəifliyi. NIS2 bu riskləri idarə heyətinin məsuliyyəti ilə əlaqələndirir. Məsələn, sosial mühəndislik hücumları (R3) təşkilati zəifliklərdən qaynaqlanır.
- Supply chain riskləri: Təchizatçıların və komponentlərin etibarsızlığı, xarici təsirlərə açıq olmaları. "Exploring the mitigating role of sustainable innovation" məqaləsində, rəqəmsal iqtisadiyyatın təchizat zənciri risklərini əhəmiyyətli dərəcədə azaltdığı göstərilir. ENISA, təchizat zəncirində xarici yurisdiksiya risklərini (R11) vurğulayır.

B. Risklərin Qiymətləndirilməsi

Risklərin qiymətləndirilməsi kvantitativ və keyfiyyətli metodlarla aparılır. Aİ-nin Cloud Sovereignty Frameworkində SEAL səviyyələri (0-4) və Sovereignty Score istifadə olunur. Formula eynidir:

NIS2 və DORA, risk qiymətləndirməsini məcburi edir, məsələn, ICT risklərinin sistematik təhlili.

- Mövcud metodlar: SEAL səviyyələri və Sovereignty Score vasitəsilə riskin kvantitativ qiymətləndirilməsi. ENISA, risk qiymətləndirməsini bulud qəbulundan əvvəl tövsiyə edir.
- Praktik nümunə: Hər bir SOV məqsədi üçün SEAL səviyyəsinin 0–4 intervalında qiymətləndirilməsi. Məsələn, SOV-7 (Security & Compliance) üçün EUCS sertifikasiyası istifadə olunur, risk səviyyəsi "high" üçün əlavə tələblər qoyulur.

CƏDVƏL 2. SEAL SƏVİYYƏSİNƏ GÖRƏ RİSK QİYMƏTLƏNDİRMƏSİ

SEAL Səviyyəsi	Risk Səviyyəsi	Təsvir	Nümunə
0	Yüksək	Heç bir qorunma yoxdur, xarici yurisdiksiya riski maksimum	Xarici provayderlərdə məlumat saxlanması
1-2	Orta	Əsas qorunma, lakin audit zəif	Lokal saxlanma, lakin şifrələmə yoxdur
3	Aşağı	Tam audit və nəzarət	EU daxilində hostinq və GDPR uyğunluğu
4	Minimal	Yüksək suverenlik, sıfır-trust modeli	EUCS "high" sertifikasiyası

Cədvəl 2 ENISA və EUCS çərçivələrinə əsaslanır.

C. Müdafiə və Praktik Yanaşmalar

Müdafiə yanaşmaları, proaktiv və reaktiv tədbirləri əhatə edir. NIS2 və DORA, təchizat zənciri monitorinqini və incident cavabını prioritetləşdirir. Elmi məqalədə, "Reducing sustainable supply chain risks"da, DEEP-RM çərçivəsi təklif olunur ki, bu, DT-lərlə (blockchain, AI) riskləri minimuma endirir.

1) Data localization & encryption: Məlumatlar yalnız EU daxilində saxlanmalı, bütün məlumatlar şifrələnməlidir. GDPR və NIS2 bu tələbi məcburi edir. Nümunə: EUCS-də CS-EL4 səviyyəsi lokalizasiyanı tələb edir.

2) Access control & audit: Role-based access control, audit log və AI usage monitoring. ENISA, zero-trust modelini tövsiyə edir.

3) Supply chain monitoring: Kritikal komponentlərin izlənməsi və EU-suverən təchizatçılardan alınması. "Supply Chain Attacks in Multi-Cloud" məqaləsində, multi-cloud mitigasiyası təklif olunur.

4) Incident response & resilience: EU Security Operations Center, müstəqil penetration test və vulnerability audit. DORA, ICT incident hesabatını əhəmiyyətli edir.

5) Regulatory compliance: GDPR, NIS2, DORA və ENISA göstərişlərinə tam uyğunluq. NIS2, icra orqanlarının məsuliyyətini artırır. Bu yanaşmalar, dövlət buludlarının təhlükəsizliyini gücləndirərək, elm və praktikada yeni standartlar yaradır.

NƏTİCƏ

Dövlət sektorunda bulud əsaslı xidmətlərin genişlənməsi və rəqəmsal transformasiyanın sürətlənməsi fonunda data və bulud suverenliyinin təmin edilməsi həm strateji, həm də əməliyyat baxımından mühüm əhəmiyyət kəsb edir. Məqalədə təqdim olunan analiz nəticəsində aşağıdakı əsas nəticələr əldə edilmişdir:

Data və AI suverenliyinin əhəmiyyəti: Dövlət məlumatlarının xarici infrastrukturdan müstəqil şəkildə idarə olunması kritikdir. SEAL səviyyələrinin tətbiqi, məlumatların EU ərazisində saxlanması və AI modellərinin audit edilməsi bu müstəqilliyi təmin edən əsas mexanizmlərdir [1, 3].

Sovereignty Score-un praktik istifadəsi: Sovereignty Score dövlət bulud xidmətlərinin müqayisəli qiymətləndirilməsində effektiv alət kimi çıxış edir. Bu metod, bulud provayderlərinin strateji, hüquqi, texnoloji və əməliyyat suverenliyi üzrə performansını obyektiv qiymətləndirməyə imkan verir [2, 5].

Strateji və əməliyyat risklərinin idarə olunması: Analiz göstərir ki, yüksək SEAL səviyyələri yalnız texnoloji infrastrukturun EU-daxili yerləşməsi ilə deyil, həm də əməliyyatların, təhlükəsizlik monitorinqinin və təchizat zəncirinin tam nəzarətdə olması ilə təmin edilə bilər [4, 6].

Müasir praktik yanaşmaların inteqrasiyası: Avropa təcrübəsi (Gaia-X, Cloud de Confiance, Souveräner Cloud) göstərir ki, həm texniki, həm də hüquqi tədbirlərin kompleks tətbiqi dövlət bulud xidmətlərinin suverenliyini möhkəmləndirir. Bu yanaşmalar, həmçinin enerji və ətraf mühit dayanıqlılığını da təmin edir [7].

Əsas tövsiyələr kimi aşağıdakıları qeyd etmək olar:

- Dövlət bulud layihələrində SEAL və Sovereignty Score yanaşmalarının standart olaraq tətbiqi;
- Data və AI suverenliyi üçün EU ərazisində saxlanma və emal tələblərinin qanunvericiliklə möhkəmləndirilməsi;
- Təchizat zənciri və texnoloji stack üzərində tam audit və nəzarət mexanizmlərinin qurulması;
- Enerji effektivliyi və davamlılıq göstəricilərinin dövlət bulud infrastrukturunda nəzərə alınması.

Nəticə etibarilə, dövlət bulud infrastrukturunun kibersuverenliyinin təmin olunması yalnız texnologiya və qanunvericilik tədbirləri ilə məhdudlaşmamalı, həm də əməliyyat, təchizat və idarəetmə strukturlarının strateji planlaşdırılması ilə birgə həyata keçirilməlidir.

ƏDƏBİYYAT

[1] ENISA, "Cloud Security Guide for European Public Administrations," European Union Agency for Cybersecurity, Athens, Greece, 2023.

[2] CIGREF, "Trusted Cloud Referential v2," CIGREF, Paris, France, 2022.

[3] European Commission, “Gaia-X: A Federated Data Infrastructure for Europe,” Brussels, Belgium, 2021.

[4] Bundesministerium für Wirtschaft und Energie, “Souveräner Cloud – Strategiebericht,” Berlin, Germany, 2022.

[5] ISO/IEC 27018:2019, “Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors,” International Organization for Standardization, Geneva, Switzerland, 2019.

[6] European Union, “Directive (EU) 2022/2555 on NIS2,” Official Journal of the European Union, 2022.

[7] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, “Fog Computing and its Role in the Internet of Things,” in Proc. of the First Edition of the MCC Workshop on Mobile Cloud Computing, 2012, pp. 13–16.

Analysis of Cybersecurity Risks and Practical Approaches in Ensuring State Data and Cloud Sovereignty

Serkhan Mirili

The Academy of the State Security Service of the Republic of Azerbaijan named after Heydar Aliyev, Baku, Azerbaijan

Abstract– Digital transformation processes have led to the widespread adoption of cloud technologies in public administration. While this process enhances the efficiency of public services, it also creates new cybersecurity risks in terms of ensuring data and cloud sovereignty. This article analyzes the cybersecurity risks present in cloud-based information systems used in the public sector and evaluates the impact of these risks on data sovereignty. At the same time, conceptual and practical cybersecurity approaches are proposed to ensure state data and cloud sovereignty. The results of the study have scientific and practical significance for the development of secure and resilient digital government systems.

Keywords– data sovereignty; cloud sovereignty; cybersecurity; digital state; risk analysis.