ROMÂNIA
SERVICIUL ROMÂN DE INFORMAŢII
U.M. 0929 BUCUREŞTI
Nr. 86191 din 30.03.2022.

NECLASIFICAT
Ex. unic

RAPORT PRIVIND CONSULTAREA PIEȚEI

în cadrul proiectului CLOUD GUVERNAMENTAL

Persoana de contact: Manuela Maghiar
Date de contact: e-mail: iulia.maghiar@dcti.ro

Cod document:
Denumire document: Raport privind consultarea pieței

Informații utile

Acest document oferă un rezumat al procesului și rezultatului consultării pieței în ceea ce privește proiectul *Cloud Guvernamental*. Acest document nu reprezintă decizia Autorității Contractante cu privire la conținutul Strategiei de contractare pentru derularea procedurii de achiziție asociate acestei consultări a pieței.

Informațiile oferite de către persoanele/organizațiile respondente/participante la întâlnirile de consultare nu le vor aduce avantaje sau dezavantaje acestora în perspectiva derulării procedurii de atribuire asociate acestei consultări a pieței. Răspunsurile sau participarea operatorilor economici la această consultare a pieței nu vor constitui în nici un caz un motiv de excludere în cadrul viitoarei proceduri de atribuire.

Această consultare a piaței nu a avut ca scop selectarea unui anumit ofertant pentru viitoarea procedură de atribuire. Această consultare a pieței precede procedura de atribuire din care face parte și nu se substituie procesului de selecție. Respondenții/participanții nu au depus cereri de participare sau oferte ca răspuns la această consultare a pieței.

Participarea la această consultare a pieței a fost pur voluntară. Autoritatea contractantă nu a acordat și nu va acorda compensații financiare pentru participanții la consultarea pieței și nici nu a rambursat/nu va rambursa cheltuielile efectuate cu ocazia participării în cadrul aceasteia.

Informațiile primite de către Autoritatea Contractantă în cursul consultărilor pieței pot fi utilizate în planificarea și desfășurarea viitoarelor proceduri de achiziții, cu respectarea prevederilor legislației în domeniul achizițiilor publice, în special pentru a nu denatura concurența în cadrul viitoarei proceduri de atribuire și pentru a nu încălca principiile nediscriminării și transparenței. Pe parcursul procesului de consultare, Autoritatea Contractantă a luat toate măsurile necesare pentru a păstra confidențialitatea informațiilor declarate de către participanții la consultare drept confidențiale, clasificate sau protejate de un drept de proprietate intelectuală.

Nicio informație conținută în acest document, în documentele publicate în SEAP sau prin orice alte mijloace în legătură cu acest proces de consultare sau orice comunicare realizată între Autoritatea Contractantă și orice persoană/organizație în legătură cu această consultare a pieței nu poate fi invocată ca făcând parte dintr-un contract, acord sau orice altă formă similară.

Autoritatea Contractantă publică acest document în SEAP în secțiunea "Consultarea pieței"/ "Raportul final", ca rezultat al consultării pieței.

Cuprins

1. Contextul derulării consultării pieței

Implementarea proiectului de Cloud Guvernamental este o prioritate asumată de către Guvernul României în Programul de guvernare și prin Planul Național de Redresare și Reziliență (PNRR) - Componenta 7 - Transformare digitală având ca **obiectiv:**[1] *O infrastructura digitala coerentă și integrată la nivelul administrației publice din România care să ofere servicii digitale de înaltă calitate atât cetățenilor, cât și companiilor. Prin realizarea acestui obiectiv sunt create condițiile pentru adoptarea tehnologiilor digitale în toate sectoarele și domeniile de activitate ale instituțiilor statului și pentru creșterea numarului de cetațeni și companii care vor putea beneficia și fructifica oportunitățile oferite de digitalizare. Implementarea pe scară largă a soluțiilor digitale va contribui, la creșterea gradului de transparentizare a activității autorităților statului și la reducerea barierelor birocratice, contribuind, de asemenea, la realizarea obiectivelor de dezvoltare durabilă.*

Asociat acestei consultări, autoritatea contractantă Serviciul Român de Informații - Unitatea Militară 0929, va publica în SEAP și JOUE, *Anunțul de participare* la o procedură de *licitație deschisă* având ca obiect furnizarea de soluții de securitate cibernetică. Procedura de atribuire asociată procesului de consultare a pieței se va derula separat, toți participanții fiind informați atunci când aceasta va fi inițiată.

Autoritatea Contractantă intenționează să achiziționeze produse **cu grad ridicat** de complexitate tehnică constând în soluții de securitate cibernetică pentru care dorește să definească specificațiile tehnice și valoarea estimată astfel încât să încurajeze participarea la viitoare procedură a tuturor operatorilor economici care prezintă capabilități tehnice performante în acest sector de activitate.

Consultarea pieței are ca scop:

1. identificarea posibilelor soluții de definire specificațiilor tehnice pentru soluțiile de securitate cibernetică respectiv identificarea valorii estimate reale și actuale a achiziției
2. identificarea capacității pieței de a furniza soluții cu privire la definirea specificațiilor tehnice pentru soluțiile de securitate cibernetică (potențiali ofertanți) precum și cu privire la valoarea estimată a unor astfel de produse;
3. furnizarea de informații în legătură cu dezvoltarea capacității pieței în acest sector, informații care vor crește gradul de cunoaştere a pieței de către Autoritatea Contractantă

[1] Mai multe informații referitoare la Planul Național de Redresare și Reziliență (PNRR) - Componenta 7 - Transformare digitală - Dezvoltarea unui cadru unitar pentru definirea arhitecturii unui sistem de tip cloud guvernamental pot fi găsite accesând https://mfe.gov.ro/pnrr/

4. reducerea numărului de solicitări de clarificări la Documentația de atribuire și/sau depunerea de contestații, efectuate ulterior inițierii procedurii de atribuire.

2. Rezumatul procesului de consultare a pieței

i. Calendarul activităților și etapele majore ale procesului de consultare a pieței

Activitățile majore care au avut loc în timpul consultării pieței pornind de la stadiul de planificare și până la pregătirea acestui raport sunt evidențiate în tabelul de mai jos:

Nr. crt.	Descrierea activității	Durata	Data de început	Data de încheiere
1.	Publicarea anunțului de consultare a pieței nr. MC1018738/28.02.2022	1 zi lucrătoare	28.02.2022	-
2.	Publicarea anunțului de consultare a pieței nr. MC1018858/09.03.2022	1 zi lucrătoare	09.03.2022	-
3.	Perioada de transmitere a propunerilor, conform anunțului MC1018858/09.03.2022	14 zile lucrătoare	28.02.2022	18.03.2022
4.	Analiza propunerilor depuse	8 zile lucrătoare	21.03.2022	30.03.2022
5.	Întocmirea și publicarea raportului final privind consultarea pieței	1 zi lucrătoare	31.03.2022	31.03.2022[2]

Procesul de consultare a pieței a presupus parcurgerea a două etape:

Etapa 1 - Transmiterea opiniilor/sugestiilor/recomandărilor sub forma *Formularului* prezentat în *Anexa 2* la *Instrucțiunile privind procesul de consultare a pieței* încărcat în SEAP cu ocazia publicării anunțului de consultare.

În data de 28.02.2022, a fost publicat în SEAP anunțul de consultare a pieței nr. MC1018738, în cadrul acestuia fiind încărcate Formularul „Instrucțiuni privind procesul de consultare a pieței" și cele două anexe aferente, respectiv anexa nr. 1 „Documentul cuprinzând aspectele tehnice - Consultare piață – Securitate cibernetică" și anexa nr. 2 „Formular prezentare opinii/sugestii/recomandări în cadrul procesului de consultare a pieței - Cloud Guvernamental".

Cu ocazia publicării anunțului de consultare, au fost stabilite următoarele date limită:

- dată limită pentru transmiterea propunerilor: 11.03.2022 și
- dată limită consultare: 18.03.2022.

Ulterior, în data de 09.03.2022, în contextul actualizării termenelor asociate proiectului, a fost publicat anunțul de consultare a pieței nr. MC1018858, prin care s-a decalat termenul stabilit pentru depunerea propunerilor în cadrul consultării de piață

[2] Data la care devine activ în SEAP butonul pentru încărcarea Raportului final, ulterior finalizării termenului alocat consultărilor.

care făcea obiectul anunțului nr. MC1018738 din data de 28.02.2022, după cum urmează:

- dată limită pentru transmiterea propunerilor: 18.03.2022;
- dată limită consultare: 30.03.2022.

Etapa 2 - Analiza propunerilor depuse și elaborarea prezentului raport.

În conformitate cu dreptul instituit prin prevederile *Instrucțiunilor privind procesul de consultare a pietei și art. 19 din HG 395/2016*[3], nu au fost organizate întâlniri de consultare cu persoanele/organizațiile care au tarnsmis propuneri.

Perioada alocată analizei propunerilor și întâlnirilor de consultare este cea menționată în tabelul de mai sus, respectiv 19.03 - 30.03.2022.

ii. Abordările folosite în procesul de consultarea pieței

a) *Numărul deopinii/sugestii/recomandări primite cu cele așteptate de Autoritatea Contractantă:*

În urma analizei de piață și a propunerilor rezultate, a fost identificată o varietate mare de soluții, servicii și tehnologii complexe, care pot asigura un nivel ridicat al securității cibernetice a Cloud-ul Guvernamental, prin implementarea de mecanisme care să asigure confidențialitatea, integritatea și disponibilitatea datelor entităților găzduite, inclusiv protejarea datelor în tranzit, precum și detectarea și prevenirea atacurilor cibernetice complexe de tip APT. În acest sens, intenția entităților private de a susține implementarea și operaționalizarea Cloud-ului Guvernamental este susținută de propunerile primite, care corespund așteptărilor și nevoilor de implementare a proiectului.

b) *Lista organizațiilor care au transmis opinii/sugestii/recomandări sub formă de răspuns la **Anunțul privind consultarea** publicat:*

Până la termenul limită stabilit pentru depunerea propunerilor, 18.03.2022, următorii operatori economici au transmis opinii/sugestii/recomandări:

1. Atos Convergence Creators SRL;
2. Best Internet Security SRL;
3. Check Point Software Technologies Ltd.;
4. Critical Technologies SRL;
5. Cyber Dacians SRL;
6. Datanet Systems SRL;
7. Ernst&Young SRL;
8. General Microsoft;

[3] pentru aprobarea Normelor metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achiziție publică/acordului-cadru din Legea nr. 98/2016 privind achizițiile publice

9. CIBM Security Services;
10. Kapsch SRL;
11. Mida Soft Business SRL;
12. Oracle România SRL;
13. Orange România Communications SA;
14. Palo Alto Networks;
15. Power Net Consulting;
16. S&T România SRL;
17. Trend Micro;

c) Temele abordate în formularul de răspuns.

Pentru asigurarea securității cibernetice a cloud-ului guvernamental, a fost avută în vedere aplicarea următoarelor principii în mod unitar, incluse în cadrul unui sistem de management al securității cibernetice:

1. Asigurarea securității cibernetice a cloud-ului guvernamental în toate etapele de dezvoltare și funcționare ale acestuia prin raportare la confidențialitatea, integritatea și disponibilitatea datelor, prin:

- mecanisme de tipul secure-by-design, ceea ce presupune implementarea de politici, mecanisme și practici de securitate în etapa de dezvoltare a cloud-ului.
- implementarea, administrarea tehnică și operațională, mentenanța, precum și dezvoltarea ulterioară a serviciilor de securitate cibernetică ale Cloud-ului Guvernamental.

2. Protejarea datelor în tranzit împotriva activităților de exfiltrare, respectiv de alterare a acestora, prin

- protejare a rețelei prin implementarea de mecanisme care nu permit interceptarea datelor;
- criptare a datelor prin implementarea de mecanisme care nu permit vizualizarea în clar a pachetelor de date decât de către persoanele abilitate (canale de comunicații securizate).

Datele trebuie protejate atât pe parcursul transmiterii de la end user la serviciul cloud, cât și în interiorul cloud-ului și în timpul transmiterii lor din cloud către diferite servicii.

3. Securitatea operațională – mecanisme pentru detectarea și prevenirea atacurilor cibernetice, prin raportare la o abordare pe nivele, conform conceptului defence in depth:

- managementul vulnerabilităților – implementarea cu promptitudine a actualizărilor de securitate;
- monitorizarea activității, în scopul detectării atacurilor cibernetice și a activităților neautorizate– SOAR, colectarea logurilor independent de soluția SIEM utilizată, utilizarea unei soluții centralizate de stocare a logurilor;

- managementul evenimentelor de securitate cibernetică realizat în afara arhitecturi cloud-ului, fiind create entități distincte în funcție de clasificarea datelor, cu posibilitatea de creare a unor fluxuri unidirecționale;
- managementul incidentelor de securitate cibernetică prin implementarea de politici de securitate, care să includă controale de securitate la nivel de:
  - o aplicație – WAF, scanare de vulnerabilități, securitate API;
  - o infrastructură cloud – loguri;
  - o endpoint – antivirus, loguri, EDR;
  - o sistem de operare;
- stabilirea unei proceduri de verificare a soluțiilor de securitate cibernetică: stress test, pentest;
- implementarea unor soluții de Threat Hunting, pentru identificarea amenințărilor cibernetice avansate la adresa Cloud-ului Guvernamental;
- utilizarea unor soluții forensics în scopul extragerii live a unor copii de memorie/disc;
- implementarea unor mecanisme de asset management și attack surface management, inclusiv prin testarea continuă a aplicațiilor web (DAST, IAST);
- implementarea unor mecanisme de tip remote browser isolation pentru zona de client;
- implementarea unor soluții de back-up;
- awareness structural și situațional.

4. Managementul identității și controlul accesului, inclusiv prin mecanisme de digital rights management:

- autentificarea utilizatorilor anterior accesării unui serviciu cloud (prin raportare la modelul Zero-trust, autentificare MFA, tokenizare, limitare drepturilor pe baza adresei IP, utilizarea unor parole cu nivel ridicat de complexitate, soluții de User Behavior Analytics);
- implementarea unui mecanism de tip risk based authentication în cazul în cate nu se poate implementa un mecanism de tip MFA;
- implementarea unui mecanism de tip software define perimeter (SDP) pentru zona de acces securizat la resurse;
- implementarea unor politici de control al accesului și definire de roluri - limitarea accesului utilizatorilor astfel încât acțiunile/ compromiterea unui utilizator să nu afecteze serviciile cloud sau datele vehiculate/ stocate:
  - o utilizarea unor terminale dedicate pentru administrarea cloud-ului – echipamentele nu vor fi utilizate în alte scopuri;
  - o aplicație specială pentru gestionarea accesului;
  - o aplicație specială pentru gestionarea fluxurilor;
  - o aplicație specială pentru gestionarea excepțiilor de securitate.
- nu este dezirabilă existența unui rol de administrator la nivelul întregului cloud.

- solicitările de modificare a standardelor de securitate trebuie transmise de către client spre administratorul cloud, în scopul revizuirii, aprobării sau propunerii de soluții alternative;
- implementarea unor mecanisme de risk assessment pentru entitățile care vor să acceseze date din Cloud-ul Guvernamental.

5. Implementarea de tehnologii specifice cloud:

- CSPM – Cloud Security Posture Management (compliantă și guvernanță)
- CASB – Cloud Security Broker Acess (pe zona de client care accesează datele)
- CWPP – Cloud Workload protection platform (virtualizare, containere si serverless)
  - Hardening, configuration and vulnerability management
  - Network firewalling, visibility and microsegmentation
  - System integrity assurance
  - Application control/whitelisting
  - Exploit prevention/memory protection.
  - Server workload EDR, behavioral monitoring and threat detection/response.
  - Anti-malware scanning

d) Rezumatul opiniilor/sugestiilor/recomandărilor primite în prima etapă ca răspuns la întrebările adresate/temele abordate.

În urma analizei celor 17 propuneri depuse, au fost primite 147 de soluții de securitate, dintre care 125 de produse (hardware și software), 16 servicii și 6 soluții integrate de tip hibrid (cloud și on-prem). Propunerile primite au acoperit o plajă diversificată de producători, tehnologii și modalități de implementare, care asigură securizarea Cloud-ului Guvernamental, respectând principiile enumerate în consultarea de piață. Astfel, au fost identificate o serie de soluții care apar în cadrul propunerilor mai multor operatori economici, bazându-se pe tehnologii dezvoltate de către producători precum PaloAlto, CheckPoint și Microsoft.

e) Concluziile care decurg din opiniile/sugestiile/recomandările primite

Analizând propunerile primite s-a constatat faptul că există instrumentele necesare pentru asigurarea securității cibernetice a Cloud-ul Guvernamental, prin implementarea de mecanisme care să asigure confidențialitatea, integritatea și disponibilitatea datelor entităților găzduite, inclusiv protejarea datelor în tranzit, precum și detectarea și prevenirea atacurilor cibernetice complexe de tip APT. În același timp, estimările de costuri, primite în cadrul propunerilor, se încadrează în bugetul previzionat.

3. Rezultatul procesului de consultarea pieței

Prezentarea temelor abordate în cadrul propunerilor, rezumatul opiniilor și concluziile care se desprind din acestea sunt prezentate la punctele c), d) și e) de mai sus. Rezultatul procesului de consultare a pieței a relevat o gamă extinsă de soluții, servicii și tehnologii, care vizează securitatea cibernetică a Cloud-ul Guvernamental, prin implementarea de mecanisme care asigură confidențialitatea, integritatea și disponibilitatea datelor entităților găzduite, inclusiv protejarea datelor în tranzit, precum și detectarea și prevenirea atacurilor cibernetice complexe de tip APT. Propunerile primite și expertiza tehnică existentă la nivelul Serviciul Român de Informații vor sta la baza întocmirii ulterioare a documentației necesare implementării proiectului.

4. Alte informații relevante pentru a demonstra aplicarea principiilor achizițiilor publice în timpul consultării pieței

i. Autoritatea contractantă, pe parcursul întregului proces privind consultarea pieței, a urmărit respectarea prevederilor legislației în domeniul achizițiilor în ceea ce privește acordarea unei atenții speciale pentru a nu denatura competiția în cadrul viitoarei proceduri de atribuire și de a nu încălca principiile nediscriminării și transparenței;

ii. În ceea ce privește păstrarea confidențialității informațiilor declarate de participanții la consultare ca fiind confidențiale, clasificate sau protejate de un drept de proprietate intelectuală, Autoritatea contractantă precizează că a luat toate măsurile pentru a nu dezvălui și pentru a proteja acele propuneri/sugestii/recomandări declarate confidențiale, clasificate sau protejate de un drept de proprietate intelectuală, în măsura în care această situație a fost incidentă;

iii. Prezentul Raport privind consultarea pieței va fi publicat în SEAP și va fi disponibil tuturor participanților sau persoanelor interesate.

5. Anexe

Nu este cazul.