Autoritatea Națională pentru Administrare și Reglementare în Comunicații

Str. Delea Nouă nr.2, Sector 3, București, 030925 România
Tel: 0372 845 400 / 0372 845 454 Fax: 0372 845 402
ancom@ancom.ro www.ancom.ro

În atenția operatorilor economici interesați de „*achiziția directă*" organizată în vederea achiziționării unei ***subscripții care să asigure accesul pentru o perioadă de un an la o soluție de securitate de tip Web Application Firewall (WAF) în cloud, pentru protecția aplicațiilor web aparținând ANCOM de amenințări și atacuri cibernetice la adresa lor (cod CPV: 72910000-2)***

Anunț publicitar nr. ADV1475522 / 08.04.2025

În conformitate cu prevederile Legii nr. 98/2016 privind achizițiile publice, precum și ale Normelor metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achiziție publică/acordului-cadru din Legea nr. 98/2016 privind achizițiile publice, aprobate prin H.G. nr. 395/2016, se transmite răspuns la solicitarea de clarificări înregistrată la autoritatea contractantă cu nr. SC-7551/10.04.2025:

Solicitarea de clarificare nr. 1: Aceasta este lista completa de domenii?

- aisemnal.ro
- portabilitate.ro
- netograf.ro
- infocentru.ancom.ro
- ancom.ro
- monitor-emf.ro
- veritel.ro
- myAncom.ro
- sscpds.ancom.ro

Răspuns solicitare de clarificare 1: Prin prezenta achiziție dorim să asigurăm protecția față de amenințări și atacuri cibernetice, în mod prioritar, pentru aplicațiile web publice aparținând ANCOM care sunt găzduite pe lista de domenii inclusă în cerințele tehnice. În măsura în care va fi necesară asigurarea protecției și pentru alte aplicații, găzduite pe alte domenii, lista se va modifica în mod corespunzător, ulterior acestei achiziții.

Solicitarea de clarificare nr. 2: Există vreun caz mai special sau de importanță majoră în ceea ce privește un anumit domeniu? Mă refer aici la o soluție tehnică în materie de securitate care să fie diferită de cea a unui domeniu uzual?
Răspuns solicitare de clarificare 2: Aplicația web publică aparținând ANCOM care se regăsește pe domeniul netograf.ro măsoară viteza conexiunii la Internet a utilizatorilor din Romania și este singura aplicație oficială care poate fi utilizată în cazul plângerilor legate de calitatea serviciilor de internet prestate către utilizatori de către operatorii de servicii electronice. Din aceste motive protecția oferită de soluția de tip WAF care va fi implementată nu poate introduce latență în plus în cadrul testelor efectuate prin platforma netograf.ro.

Solicitarea de clarificare nr. 3: Ați avut parte de atacuri cibernetice în trecut?
Răspuns solicitare de clarificare 3: Soluțiile de securitate cibernetică implementate în ANCOM oferă informații privind atacurile / tentativele de atac care se desfășoară în mod constant asupra aplicațiilor web publice aparținând ANCOM. Din aceste considerente dorim implementarea unei

soluții WAF capabile să asigure o protecție sporită, permanentă, împotriva atacurilor / tentativelor de atac asupra aplicațiilor web aparținând ANCOM.

Solicitarea de clarificare nr. 4: Ne puteți comunica un număr mediu/estimativ de DNS records per domeniu?
Răspuns solicitare de clarificare 4: Domeniul ancom.ro are aproximativ 35 de înregistrări DNS (nu toate sunt folosite pentru aplicații web publice sau care fac subiectul soluției WAF), celelalte domenii au în medie aproximativ 3 înregistrări DNS.

Autoritatea Națională pentru Administrare și Reglementare în Comunicații

Str. Delea Nouă nr.2, Sector 3, București, 030925 România
Tel: 0372 845 400 / 0372 845 454 Fax: 0372 845 402
ancom@ancom.ro www.ancom.ro

În atenţia operatorilor economici interesaţi,

ANUNȚ PUBLICITAR

Autoritatea Națională pentru Administrare şi Reglementare în Comunicații (ANCOM), cu sediul în Mun. București, Str. Delea Nouă, Nr. 2, Sector 3, Cod poştal: 030925, intenționează să achiziționeze o *subscripție care să asigure accesul pentru o perioadă de un an la o soluție de securitate de tip Web Application Firewall (WAF) în cloud, pentru protecția aplicațiilor web aparținând ANCOM de amenințări și atacuri cibernetice la adresa lor*.

Punct de contact: Direcția Achiziții / Serviciul Achiziții Operaționale, telefon: 0372.845.377, în atenția: Cristiana Mihaela STOIAN, e-mail: cristiana.stoian@ancom.ro

1. **Tip anunț:** Cumpărare directă.
2. **Tip contract:** Servicii.
3. **Denumirea achiziției:** Contract/comandă având ca obiect achiziția unei subscripții care să asigure accesul pentru o perioadă de un an la o soluție de securitate de tip Web Application Firewall (WAF) în cloud, pentru protecția aplicațiilor web aparținând ANCOM de amenințări și atacuri cibernetice la adresa lor.
4. **Cod CPV: 72910000-2**
5. **Descrierea Contractului/Comenzii:**

Se dorește achiziția unei subscripții care să asigure accesul pentru o perioadă de un an la capabilitățile oferite de o soluție de securitate de tip WAF (Web Application Firewall) în cloud, în scopul:

- asigurării accesului securizat al publicului și al operatorilor de comunicații electronice la resursele și serviciile prestate prin intermediul aplicațiilor WEB aparținând ANCOM (printre care menționăm: aisemnal.ro, portabilitate.ro, netograf.ro, infocentru.ancom.ro, ancom.ro, monitor-emf.ro, aisemnal.ro, veritel.ro, myAncom.ro, sscpds.ancom.ro);
- protejării, stabilității și a suportului continuu pentru sistemele și aplicațiile informatice cu expunere în internet, necesare desfășurării activității ANCOM;
- reducerii semnificative a riscului pierderilor de date sau a blocării accesului la aplicațiile WEB existente datorate unor eventuale atacuri reușite asupra acestora.

Toate cerințele tehnice, precum și alte cerințe minime obligatorii sunt detaliate în Specificațiile tehnice, anexate prezentul Anunț publicitar.

6. **Valoarea totală estimată, fără TVA: 172.000,00 Lei.**
7. **Condiții Contract/Comandă:**

Subscripția va asigura accesul la o soluție de securitate de tip Web Application Firewall (WAF) în cloud, pentru protecția aplicațiilor web aparținând ANCOM pentru o perioadă de un an.

***Termenul de prestare a serviciilor**:* Se va asigura configurarea înregistrărilor DNS și a politicilor de securitate aferente aplicațiilor ce vor fi protejate, astfel încât să nu existe întreruperi în utilizarea acestora, în termen de maxim **15 (cincisprezece) zile lucrătoare** de la semnarea Contractului de către ambele parți/transmiterea Comenzii. Termenul de realizare se consideră respectat în măsura în care procesul-verbal de recepție este semnat până la expirarea acestui termen.

Pentru depășirea termenului asumat, Prestatorul va datora penalități de întârziere de 0,15% din valoarea totală a Contractului/Comenzii, fără TVA, pentru fiecare zi de întârziere în îndeplinirea corespunzătoare a oricărei obligații, penalități ce vor fi pretinse și/sau deduse și reținute de către ANCOM din obligațiile de plată a prețului, fără nicio formalitate prealabilă de punere în întârziere. În cazul în care penalitățile de întârziere nu pot fi deduse din preț, Prestatorul are obligația de a le plăti în termen de maxim 10 (zece) zile calendaristice de la solicitarea ANCOM.

Conditii de plată: Plata prețului se va efectua de către ANCOM către prestator în contul deschis de către acesta la Trezorerie. Factura aferentă va fi transmisă prin sistemul național privind factura electronică RO e-Factura, cu respectarea condițiilor si prevederilor reglementate prin O.U.G. nr. 120/2021, precum si celelalte acte normative emise în aplicarea acesteia. În cuprinsul facturii electronice se vor utiliza codul CPV și codul de angajament comunicate de autoritatea contractantă în cuprinsul Contractului/Comenzii.

Plata prețului se va efectua în lei, prin ordin de plată, în baza facturii emise prin e-Factura, primită și acceptată de ANCOM, numai după semnarea procesului-verbal de recepție a serviciilor.

În situația în care factura este primită anterior sau la data recepției, plata se va efectua în termen de maxim 30 (treizeci) de zile de la data semnării procesului-verbal de recepție a serviciilor.

În situația în care factura este primită după semnarea procesului-verbal de recepție a serviciilor, ANCOM are dreptul de a efectua plata în termen de maxim 30 (treizeci) de zile de la data primirii facturii.

Nu se admite efectuarea de plăți în avans sau plăți parțiale. Plata se consideră efectuată la data debitării contului ANCOM.

Prestatorul garantează achizitorului faptul ca serviciile prestate nu încalcă și nu vor încălca in vreun fel drepturile vreunei terțe părți.

Garanția de bună execuție:

Se va solicita ofertantului câștigător constituirea garanției de bună execuție, cantitativă și calitativă, a obligațiilor ce decurg din contractul de achiziție publică încheiat, în cuantum de 10% din prețul contractului de servicii (fără TVA), conform prevederilor art. 40 alin. (1) din Normele metodologice aprobate prin H.G. nr. 395/2016, prin una dintre următoarele modalități:

a) virament bancar;

b) instrumente de garantare emise în condițiile legii, astfel:

(i) scrisori de garanție emise de instituții de credit bancare sau de instituții financiare nebancare din România sau din alt stat;

(ii) asigurări de garanții emise:

- fie de societăți de asigurare care dețin autorizații de funcționare emise în România sau într-un alt stat membru al Uniunii Europene şi/sau care sunt înscrise în registrele publicate pe site-ul Autorității de Supraveghere Financiară, după caz;
- fie de societăți de asigurare din state terțe prin sucursale autorizate în România de către Autoritatea de Supraveghere Financiară;

c) prin combinarea modalităților de constituire prevăzute la lit. a)-b).

Instrumentul de garantare trebuie prezentat în conformitate cu modelul din ***Anexa nr. 4*** la prezentul Anunț publicitar.

Viramentul bancar se efectuează în contul autorității contractante nr. RO22TREZ7005005XXX000932 - deschis la Trezoreria Operativă a Mun. București.

Conform art. 40 alin.(2) din Normele aprobate prin H.G. nr. 395/2016 garanția de bună execuție se poate constitui și prin depunerea sumei în numerar (dacă valoarea acesteia este mai mică de 5.000,00 lei), la casieria autorității contractante.

8. **Locul de prestare a serviciilor**: Subscripția se va asigura electronic, la adresele de email ce vor fi comunicate ulterior, în cadrul contractului/comenzii.

9. Condiții de participare:

Modalitatea de prezentare a ofertei:

Oferta va fi structurată conform cerințelor de mai jos și va include Propunerea tehnică, Propunerea financiară și documentele solicitate conform prezentei Solicitări de oferte.

Pentru a fi admiși în cadrul prezentei achiziții, ofertanții trebuie să depună următoarele documente:

1) **Propunerea tehnică**, care va include toate informațiile solicitate în Specificațiile tehnice anexate prezentului Anunț publicitar. De asemenea, în Propunerea tehnică vor fi menționate și alte informații considerate semnificative pentru evaluarea corespunzătoare a acesteia, dacă este cazul.

Prin Propunerea tehnică ofertantul trebuie să se angajeze că va asigura respectarea tuturor activităților și termenului de prestare a serviciilor, astfel cum a fost solicitat. În situația în care în cuprinsul ofertei dvs. este indicat un termen mai mare sau acesta nu este menționat, oferta urmează a fi considerată ca fiind **neconformă**.

Ofertanții au obligația de a indica, motivat, în cuprinsul ofertei care informații din propunerea tehnică și/sau din propunerea financiară sunt confidențiale, clasificate sau sunt protejate de un drept de proprietate intelectuală, în baza legislației aplicabile. Informațiile indicate de operatorii economici ca fiind confidențiale, inclusiv secrete tehnice sau comerciale și elementele confidențiale ale ofertelor, trebuie să fie însoțite de dovada care să le confere caracterul de confidențialitate, dovadă ce devine anexă la ofertă, în caz contrar autoritatea contractantă neavând obligația de a nu dezvălui informațiile respective.

2) **Propunerea financiară**, care va conține prețul exprimat în Lei, fără TVA, pentru serviciile care fac obiectul prezentei achiziții, conform ***Anexei nr. 3*** la prezentul Anunț publicitar. Prețul ofertat trebuie să includă toate costurile Prestatorului, directe și indirecte, legate de prestarea serviciilor care fac obiectul prezentei achiziții. Prețul ofertat va fi ferm și nu poate fi modificat pe toată perioada prestării serviciilor care fac obiectul prezentei achiziții.

3) **Declarația reprezentantului legal/împuternicit al *Ofertantului*** din care să rezulte că oferta prezentată respectă toate cerințele/condițiile precizate în prezentul Anunț publicitar ***(Anexa nr. 1);***

4) **Declaratia reprezentantului legal/împuternicit al *Ofertantului*** din care să rezulte că acesta își desfășoară activitatea respectând toate regulile obligatorii prevăzute de reglementările legale referitoare la mediu, condițiile de muncă și protecție a muncii în vigoare la nivel național, corespunzător domeniului său de activitate în conformitate cu ***Anexa nr. 2*** la prezentul Anunț publicitar;

5) **Declaratia reprezentantului legal/împuternicit al *Ofertantului*** din care să rezulte că acesta este înregistrat în condițiile legii, în țara de rezidență, că este legal constituit, că este în funcțiune și că are capacitatea de a presta serviciile solicitate, precum și că nu a fost condamnat prin hotărâre definitivă a unei instanțe judecătorești pentru comiterea unei infracțiuni, și că și-a îndeplinit obligațiile de plată a impozitelor, taxelor și contribuțiilor la bugetul general consolidat în conformitate cu ***Anexa nr. 5*** la prezenta Solicitare de oferte.

10. Criterii de adjudecare:

Va fi selectată oferta depusă care îndeplinește în totalitate cerințele solicitate prin prezentul Anunț publicitar și care are **prețul total cel mai scăzut în Lei, fără TVA**.

11. Informații suplimentare:

Oferta se va transmite pe e-mail la adresa cristiana.stoian@ancom.ro până la data de **23.04.2025, ora 16^{00},** astfel:

Documentele ofertei se vor semna de către reprezentantul legal al ofertantului sau de o persoană împuternicită expres, caz în care va fi prezentată împuternicirea formulată în acest sens. Oferta și documentele însoțitoare se vor transmite electronic la adresa mai sus-menționată până cel târziu la data de **23.04.2025, ora 16^{00}**.

În situația în care nu este posibilă transmiterea ofertei conform celor de mai sus, aceasta se va depune direct sau prin poștă la Registratură – sediul ANCOM din Mun. București, Cod poștal 030925, Sector 3, Str. Delea Nouă, Nr. 2 (program de lucru: luni-joi: 8:30 – 17:00; vineri: 8:30 – 14:30) până cel târziu la data de **23.04.2025, ora 16^{00}**.

În cazul în care oferta se depune direct sau prin poștă, operatorul economic trebuie să prezinte oferta în plic sigilat și marcat cu denumirea/numele și sediul/adresa operatorului economic. De asemenea, pe plic se va menționa „În atenția Direcției Achiziții / Serviciul Achiziții Operaționale – "*Oferta pentru achiziția unei subscripții care să asigure accesul pentru o perioadă de un an la o soluție de securitate de tip Web Application Firewall (WAF) în cloud, pentru protecția aplicațiilor web aparținând ANCOM de amenințări și atacuri cibernetice la adresa lor*". Dacă plicul nu este marcat conform prevederilor de mai sus, ANCOM nu îşi asumă nicio responsabilitate pentru rătăcirea ofertei.

Oferta trebuie să fie valabilă cel puțin până la data de **22.05.2025.**

Oferta se poate retrage și modifica înainte de data limită de depunere a ofertei, respectiv **23.04.2025, ora 16^{00}.**

Oferta transmisă/depusă la o altă adresă sau după data de **23.04.2025, ora 16^{00},** nu va fi luată în considerare.

Anunțul publicitar împreună cu **Specificațiile tehnice și Anexele nr. 1, 2, 3, 4, 5** pot fi vizualizate pe pagina de internet a ANCOM la adresa **www.ancom.ro, secțiunea Anunțuri/achiziții publice** și în SEAP (www.e-licitatie.ro, secțiunea Documente/Publicitate-Anunțuri – Listă anunțuri publicitare).

Notă GDPR: Atât ANCOM în calitate de autoritate contractantă, cât și operatorii economici care depun ofertă vor respecta dispozițiile legale care reglementează protecția datelor cu caracter personal, inclusiv Regulamentul General privind Protecția Datelor cu Caracter Personal nr. 679/2016 ("GDPR") aplicabil în Uniunea Europeană. Datele cu caracter personal solicitate de ANCOM prin prezenta și pe perioada evaluării ofertelor vor fi utilizate și prelucrate exclusiv în scopul atribuirii și derulării contractului. Prin depunerea ofertelor ofertanții recunosc dreptul autorității contractante de a prelucra datele cu caracter personal incluse în ofertă, în scopul sus menționat.

SPECIFICAȚII TEHNICE

Subscripție soluție de securitate de tip Web Application Firewall (WAF) în cloud

1. Denumirea achiziției

Achiziția unei subscripții care să asigure accesul pentru o perioadă de un an la o soluție de securitate de tip Web Application Firewall (WAF) în cloud, pentru protecția aplicațiilor web aparținând ANCOM (printre care menționăm: aisemnal.ro, portabilitate.ro, netograf.ro, infocentru.ancom.ro, ancom.ro, monitor-emf.ro, aisemnal.ro, veritel.ro, myAncom.ro, sscpds.ancom.ro), de amenințări și atacuri cibernetice la adresa lor.

2. Cerințe tehnice

Se dorește achiziția unei subscripții care să asigure accesul pentru o perioadă de un an la capabilitățile oferite de o soluție de securitate de tip WAF (Web Application Firewall) în cloud, în scopul:

- asigurării accesului securizat al publicului și al operatorilor de comunicații electronice la resursele și serviciile prestate prin intermediul aplicațiilor WEB aparținând ANCOM;
- protejării, stabilității și a suportului continuu pentru sistemele și aplicațiile informatice cu expunere în internet, necesare desfășurării activității ANCOM;
- reducerii semnificative a riscului pierderilor de date sau a blocării accesului la aplicațiile WEB existente datorate unor eventuale atacuri reușite asupra acestora.

Soluția de securitate de tip WAF în cloud trebuie să asigure următoarele funcționalități principale:

- protejarea a minimum 10 aplicații WEB aparținând ANCOM și a API-urilor aferente acestora împotriva amenințărilor cunoscute sau emergente și a atacurilor informatice la adresa acestora;
- protejarea aplicațiilor WEB împotriva exploatării vulnerabilităților existente, inclusiv cele din categoria OWASP Top 10;
- blocarea adreselor IP ce trimit cereri malițioase (IP Black listing), inclusiv a celor care fac parte din rețele botnet, TOR, proxy-uri anonime sau IP-uri folosite curent de diverși atacatori;
- inspecția traficului și detectarea cel puțin a atacurilor de tip zero-day, client side sau în care sunt folosite aplicații malițioase (malware, spyware, viruși etc.);
- protecția la nivelul tranzacțiilor HTTP/HTTPS de atacuri asupra elementelor tranzacției, cum ar fi adresele URL, numele parametrilor, valorile parametrilor, numele antetelor (headers) și valorile antetelor, metodele HTTP (GET, POST) și datele transmise;
- reguli de securitate predefinite ce includ protecția pentru cel puțin: SQL injection, cross-site scripting attacks, command injection, directory traversal etc.;
- crearea de reguli de securitate specifice pentru ANCOM;
- protecția împotriva atacurilor de tip DoS/DDoS, inclusiv atacurile volumetrice și atacurile DoS la nivel de aplicație (SlowLoris, RUDY, Slow Read etc.).
- informații din surse de threat inteligence pentru a asigura detecția rapidă a noilor amenințări;
- implementare de politici și măsuri de securitate pentru protejarea aplicațiilor web împotriva atacurilor care exploatează vulnerabilitățile cunoscute (virtual patching);
- exportul de log-uri către soluția SIEM IBM QRadar existentă în ANCOM.

Soluția de securitate de tip WAF în cloud trebuie să asigure și:

- Funcționalități pentru crearea și gestionarea politicilor și regulilor de protecție/securitate a aplicațiilor WEB:
  a) Reguli de securitate pentru tranzacțiile HTTP (HTTP Requests) ce includ:
     - configurarea lungimii maxime a cererii (request limit);

- configurarea lungimii maxime a câmpurilor URL, Query;
- dimensiunile maxime asociate cu obiectele de tip cookie: numărul de obiecte, lungimea numelui obiectului cookie, lungimea valorii obiectului cookie;
- dimensiunile maxime asociate cu antetele (headers) de pagină: numele antetului, valoarea antetului;
- reguli care permit modificarea câmpurilor URL și a antetelor (headers) în tranzacțiile HTTP primite (rescriere URL, redirecționare URL, rescriere header, înlăturare header, introducere header).

b) Reguli pentru protecția adresei URL în tranzacția HTTP care includ:
   - detectarea și blocarea atacurilor încadrate în OWASP Top 10, (Injection, Broken Access Control, Identification and Authentication Failures, Server-Side Request Forgery, etc.);
   - numărul maxim de parametri și fișiere încărcate în aplicație (maximum upload files);
   - blocarea adreselor URL care conțin semnul tilde („~”) sau secvența de caractere slash-dot („/.”);
   - construirea unei liste de metode HTTP permise (GET, POST și altele);
   - dimensiunea maximă a tranzacției efectuate prin metoda POST;
   - protecție împotriva atacurilor de tip Cross Site Request Forgery;
   - creare listă de formate de date permise (tipuri de conținut, de exemplu text/xml, application/json, image/jpeg etc.);
   - sistem de normalizare a conținutului câmpului URL: impunerea unui set standard de caractere (de exemplu, UTF-8, impunerea unor separatori uniformi de parametri în câmpul URL (de exemplu, doar caracterul ampersand („&”)) etc.;
   - crearea de reguli URL ce includ: redirecționarea temporară sau permanentă către o altă adresă URL, blocarea accesului la URL fie cu blocarea adresei IP a clientului, fie cu afișarea unui câmp CAPTCHA;

c) Reguli pentru protecția împotriva traficului provenind de la adrese IP ce includ cel puțin:
   - reguli de blocare a traficului, bazate pe adrese IP: dintr-o țară specificată (Geolocation IP), din adrese cu reputație proastă (reputation block list), din sisteme de anonimizare a traficului (anonymous proxy), din rețeaua TOR;
   - creare listă de gazde de încredere (trusted hosts).

- Funcționalități specifice pentru asigurarea protecției aplicațiilor web:
   - protecție bazată pe observarea traficului din browsere și monitorizarea nivelului de risc;
   - protecție aplicații care publică API în standardul JSON sau GraphQL;
   - scanare antivirus a fișierelor încărcate în aplicație (file upload scanning);
   - sandboxing pentru detectare atacuri de tip zero-day, ransomware sau mascate în fișierele încărcate în aplicație;
   - protecție împotriva atacurilor asupra formularelor și procesului de autentificare (cel puțin protecția împotriva testării posibilităților de acces prin utilizarea de baze de date de credențiale (utilizatori și parole) furate și protecția conturilor privilegiate;
   - protecție împotriva scurgerilor de date pe internet cel puțin prin blocarea tranzacțiilor care dezvăluie date sensibile (coduri PIN, CNP, conturi bancare etc.) și prin mascarea datelor din aplicație înainte de afișarea lor în browserul clientului (de exemplu, mascarea cifrelor din mijlocul numărului de card de credit).

- Funcționalități de management al soluției ce includ:
   - generare automată de certificate publice pentru aplicațiile protejate;
   - două moduri de operare pentru configurarea protecției:

        - mod de monitorizare în care informațiile despre amenințările detectate sunt înregistrate dar traficul nu este blocat;
        - mod de blocare în care amenințările sunt înregistrate și traficul este blocat;
        - comutarea între cele două moduri de operare trebuie să se facă pentru toate modulele și funcțiile de protecție simultan, la nivelul fiecărei aplicații protejate;
    - managementul politicilor de securitate a aplicațiilor web, cu modele (template-uri) predefinite care pot fi modificate/utilizate pentru noi politici;
    - creare de politici pe baza rezultatelor scanărilor de vulnerabilități;
    - generare automată de recomandări de configurare;
    - control identitate și acces cu suport cel puțin pentru SAML și SSO (single sign on);
    - autentificare pe bază de certificat client, integrare cu Active Directory, LDAP, Kerberos, RADIUS, suport pentru autentificare cu doi factori (Two-factor-authentification);
    - control acces pe bază de roluri (Role based access control - RBAC);
    - logging ce cuprinde log-uri de access, log-uri de firewall și log-uri de audit stocate în cloud pe o perioadă de minim 30 de zile și cu posibilitatea de export cel puțin în format tabelar (CSV);
    - funcționalități de raportare care asigură rapoarte în format tabelar și/sau grafic, rapoarte tip drill-down și programarea periodică a acestora, cu posibilitatea de selectare a intervalelor cel puțin la o oră, zi, săptămână sau lună, care să includă:
        - cele mai frecvente categorii de atacuri;
        - clienții care efectuează cel mai mare număr de atacuri;
        - aplicațiile și adresele URL cele mai atacate;
        - țările de origine din care se efectuează cel mai mare număr de atacuri;
        - numărul de accesări ale aplicațiilor în funcție de timp;
        - lățimea de bandă utilizată în funcție de timp;
        - rezumatul lățimii de bandă utilizate.
    - transmitere de alerte, atunci când apar incidente importante legate de aplicațiile web protejate (server de aplicații indisponibil, certificat expirat, atac DDoS, licență expirată etc.), cel puțin prin intermediul email-ului.

3. Alte cerințe minime obligatorii

Prestatorul trebuie să asigure toate operațiile necesare aferente pentru implementarea soluției de securitate de tip WAF în cloud:

- suportul pentru configurarea și optimizarea politicilor de securitate a aplicațiilor WEB aparținând ANCOM care vor fi protejate prin soluția ofertată;
- accesul la serviciile de suport tehnic oferite de producător pentru raportarea problemelor apărute, actualizarea licențelor și accesul la documentația oficială și bazele de date de cunoștințe aferente soluției WAF, pe toată perioada derulării contractului;
- asigurarea exportului politicilor de securitate și a configurărilor specifice la sfârșitul perioadei contractuale.

Termenul de prestare a serviciilor: Se va asigura configurarea înregistrărilor DNS și a politicilor de securitate aferente aplicațiilor ce vor fi protejate, astfel încât să nu existe întreruperi în utilizarea acestora, în termen de maxim 15 zile lucrătoare de la data semnării contractului.

Recepția serviciilor: Procesul-verbal de recepție va fi semnat în termen de 5 zile lucrătoare de la asigurarea accesului la subscripție și efectuarea operațiunilor menționate anterior, și stă la baza efectuării ulterioare a plății către prestator.

Locul de prestare a serviciilor: Subscripția se va asigura electronic, la adresele de email ce vor fi comunicate ulterior, în cadrul contractului.

Anexa nr. 1

OFERTANT,

_____

(*denumirea/numele****)***

DECLARAŢIE

din care rezultă că oferta prezentată respectă toate cerințele/condițiile precizate în Anunțul publicitar

Subsemnatul(a)_____, reprezentant legal/împuternicit al _____, *(denumirea/numele și sediul/adresa operatorului economic),* în calitate de ofertant la achiziția unei ***subscripții care să asigure accesul pentru o perioadă de un an la o soluție de securitate de tip Web Application Firewall (WAF) în cloud, pentru protecția aplicațiilor web aparținând ANCOM de amenințări și atacuri cibernetice la adresa lor (cod CPV: 72910000-2),*** organizată de Autoritatea Națională pentru Administrare și Reglementare în Comunicații, declar pe propria răspundere, sub sancțiunea excluderii din prezenta achiziție și a sancțiunilor aplicate falsului în declarații, că oferta prezentată respectă toate cerințele/condițiile precizate în anunțul publicitar.

Subsemnatul(a) declar că informațiile furnizate sunt complete și corecte în fiecare detaliu și înțeleg că autoritatea contractantă are dreptul de a solicita, în scopul verificării și confirmării declarațiilor orice documente doveditoare de care dispunem.

Data completării:_____.

OFERTANT,

_____

(*semnătura autorizată şi ştampila****)***

Anexa nr. 2

OFERTANT,

_____

(*denumirea/numele****)***

DECLARAŢIE

din care rezultă că la elaborarea ofertei operatorul economic a ținut cont de obligațiile referitoare la mediu, social, condițiile de muncă și protecția muncii

Subsemnatul(a)_____, reprezentant legal/împuternicit al _____, *(denumirea/numele şi sediul/adresa operatorului economic),* în calitate de ofertant la achiziția unei ***subscripții care să asigure accesul pentru o perioadă de un an la o soluție de securitate de tip Web Application Firewall (WAF) în cloud, pentru protecția aplicațiilor web aparținând ANCOM de amenințări și atacuri cibernetice la adresa lor (cod CPV: 72910000-2)***, organizată de Autoritatea Națională pentru Administrare și Reglementare în Comunicații, declar pe propria răspundere, sub sancțiunea excluderii din prezenta achiziție și a sancțiunilor aplicate falsului în declarații, că pe parcursul derulării Contractului/Comenzii care face obiectul prezentei achiziții vom respecta reglementările obligatorii în domeniul mediului, social și al relațiilor de muncă stabilite prin legislația adoptată la nivelul Uniunii Europene, legislația națională, prin acorduri colective sau prin tratatele, convențiile și acordurile internaționale în aceste domenii.

Subsemnatul(a) declar că informațiile furnizate sunt complete și corecte în fiecare detaliu și înțeleg că autoritatea contractantă are dreptul de a solicita, în scopul verificării și confirmării declarațiilor orice documente doveditoare de care dispunem.

Data completării:_____.

OFERTANT,

_____

(*semnătura autorizată* **)**

Anexa nr. 3

OFERTANT,

_____

(*denumirea/numele****)***

FORMULAR DE OFERTĂ

Către,

Autoritatea Națională pentru Administrare și Reglementare în Comunicații

Str. Delea Nouă nr. 2, Sector 3, București

1. Referitor la achiziția unei ***subscripții care să asigure accesul pentru o perioadă de un an la o soluție de securitate de tip Web Application Firewall (WAF) în cloud, pentru protecția aplicațiilor web aparținând ANCOM de amenințări și atacuri cibernetice la adresa lor (cod CPV: 72910000-2)***, organizată de Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM), subsemnatul(a) ....., reprezentantul legal / împuternicit al ofertantului ..... *(denumirea ofertantului*), ne oferim ca, în conformitate cu prevederile și cerințele cuprinse în anunțul publicitar, să prestăm serviciile de mai sus pentru **suma totală** de ..... *(suma în litere şi cifre)* Lei, fără TVA.

Termenul de prestare a serviciilor este de maxim ..... zile lucrătoare de la semnarea Contractului de către ambele părți / transmiterea comenzii.

Înțelegem că plata serviciilor se va efectua în termen de maxim 30 (treizeci) de zile în baza facturii emise prin e-Factura, primită și acceptată de ANCOM.

2. Ne angajăm ca, în cazul în care oferta noastră este stabilită câștigătoare, să prestăm serviciile mai sus menționate în conformitate cu prevederile anunțului publicitar.

3. Ne angajăm să menținem această ofertă valabilă până la data de **22.05.2025** și ea va rămâne obligatorie pentru noi și poate fi acceptată oricând înainte de expirarea perioadei de valabilitate.

Data completării:_____.

OFERTANT,

_____

(*semnătura autorizată* **)**

Anexa nr. 4

EMITENT,

_____

(denumirea)

INSTRUMENT DE GARANTARE
DE BUNĂ EXECUŢIE

Către,

Autoritatea Națională pentru Administrare și Reglementare în Comunicații
Str. Delea Nouă, Nr. 2, Sector 3, București

Cu privire la contractul având ca obiect achiziția unei ***subscripții care să asigure accesul pentru o perioadă de un an la o soluție de securitate de tip Web Application Firewall (WAF) în cloud, pentru protecția aplicațiilor web aparținând ANCOM de amenințări și atacuri cibernetice la adresa lor (cod CPV: 72910000-2)***, încheiat între _____, în calitate de Prestator, și Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM), în calitate de Achizitor, ne obligăm irevocabil prin prezenta să plătim în favoarea Achizitorului, până la concurența sumei de _____(_____), reprezentând 10% din valoarea contractului respectiv, fără TVA, orice sumă cerută de acesta în condițiile art. 41 din Normele metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achiziție publică din Legea nr. 98/2016 privind achizițiile publice, aprobate prin H.G. nr. 395/2016.

Prezenta garanție este valabilă până la data de _____.

În cazul în care părțile contractante sunt de acord să prelungească perioada de valabilitate a garanției sau să modifice unele prevederi contractuale care au efecte asupra angajamentului emitentului, se va obține acordul nostru prealabil, în caz contrar, prezentul instrument de garantare își pierde valabilitatea.

Parafată de emitent _____ în ziua ___ luna _____ anul _____
(semnătura autorizată)

Anexa nr. 5

OFERTANT,

_____

(*denumirea/numele****)***

DECLARAŢIE

din care rezultă că ofertantul are capacitatea de a realiza obiectul contractului/comenzii

Subsemnatul(a)_____, reprezentant legal/împuternicit al _____, *(denumirea/numele şi sediul/adresa operatorului economic),* în calitate de ofertant la achiziția unei ***subscripții care să asigure accesul pentru o perioadă de un an la o soluție de securitate de tip Web Application Firewall (WAF) în cloud, pentru protecția aplicațiilor web aparținând ANCOM de amenințări și atacuri cibernetice la adresa lor (cod CPV: 72910000-2),*** organizată de Autoritatea Națională pentru Administrare şi Reglementare în Comunicații, declar pe propria răspundere, sub sancțiunea excluderii din prezenta achiziție și a sancțiunilor aplicate falsului în declarații, următoarele:

- ..... *(denumirea operatorului economic)* este înregistrat în condițiile legii, în țara de rezidență, este legal constituit , se află în funcțiune și are capacitatea de a realiza activitățile care fac obiectul achiziției;
- ..... *(denumirea operatorului economic)* și/sau vreo persoană care este membru al organului de administrare, de conducere sau de supraveghere sau care are putere de reprezentare, de decizie sau de control în cadrul ..... *(denumirea operatorului economic)* nu a fost condamnat prin hotărâre definitivă a unei instanțe judecătorești pentru comiterea unei infracțiuni;
- ..... *(denumirea operatorului economic)* și-a îndeplinit obligațiile de plată a impozitelor, taxelor și contribuțiilor la bugetul general consolidat, în conformitate cu prevederile legale în vigoare în țara de rezidență;

Subsemnatul(a) declar că informațiile furnizate sunt complete și corecte în fiecare detaliu și înțeleg că autoritatea contractantă are dreptul de a solicita, în scopul verificării și confirmării declarațiilor orice documente doveditoare de care dispunem.

Data completării:_____.

OFERTANT,

_____

(*semnătura autorizată și ștampila****)***