INSPECTORATUL DE STAT ÎN CONSTRUCȚII

Devotament și profesionalism. Pentru siguranța ta!

Str. C.F. Robescu nr. 23, Sector 3
Cod postal 030217
Bucuresti

Tel: +40 21 318 17 00
Fax: +40 21 318 17 19
+40 21 318 17 03
+40 21 318 17 04
E-mail: isc@isc.gov.ro
www.isc.gov.ro

CAIET DE SARCINI
privind achiziția unui sistem de protecție de tip Web Application Firewall și mentenanță licențe semnături de securitate pentru sistemul de protecție de tip Web Application Firewall, pentru o perioadă de 1 an (12 luni)

1. Informații despre Autoritatea contractantă

Inspectoratul de Stat în Construcții denumit în continuare I.S.C, este organizat și funcționează în temeiul Ordonanței Guvernului nr. 63/2001, privind înființarea Inspectoratului de Stat în Construcții, cu modificările și completările ulterioare, ca instituție publică cu personalitate juridică și este organul tehnic specializat, finanțat integral din venituri proprii, care exercită, potrivit legii, controlul de stat cu privire la aplicarea unitară a prevederilor legale în domeniul calității în construcții și respectarea disciplinei în urbanism și a regimului de autorizare a construcțiilor.

2. Obiectul achiziției

Obiectul prezentului caiet de sarcini îl constituie achiziția unui sistem de protecție de tip Web Application Firewall, precum și achiziția de mentenanță licențe semnături de securitate pentru 1 an aferente acestuia, în scopul asigurării unui nivel ridicat de securitate cibernetică pentru aplicațiile web și serviciile online utilizate de Inspectoratul de Stat în Construcții.

Specificațiile tehnice care indică o anumită origine, sursă, producție, un produs special, o marcă de fabricație sau de comerț, un brevet de invenție, o licență de fabricație sunt menționate doar pentru identificarea cu ușurință a tipului de produs și nu au ca efect favorizarea sau eliminarea anumitor operatori economici sau anumitor produse.

Aceste specificații vor fi considerate ca având mențiunea "sau echivalent".

Toate cerințele din prezentul caiet de sarcini sunt minime și obligatorii, neîndeplinirea acestora va atrage respingerea ofertei.

3. Specificații tehnice

Sistemul Informatic și de Comunicații al Inspectoratului de Stat în Construcții - I.S.C. s-a dezvoltat, în ultimii 12 ani, ca un sistem unitar și integrat, prin implementarea progresivă a infrastructurilor hardware, software și de comunicații, precum și prin asigurarea securității sistemelor informatice, în contextul creșterii continue a cerințelor privind confidențialitatea, integritatea și disponibilitatea datelor. Totodată, dezvoltarea sistemului a avut ca obiectiv și punerea la dispoziția investitorilor a unor servicii publice digitalizate, necesare depunerii documentelor în relația cu I.S.C., precum și facilitarea procesării plăților online.

Sistemul Informatic și de Comunicații al I.S.C. a fost extins semnificativ prin finalizarea, în anul 2023, a proiectului intitulat „Consolidarea capacității ISC de a-și exercita competențele într-un mod unitar, eficient și eficace", având ca obiectiv specific „Extinderea Sistemului Informatic Integrat de Management existent", proiect cofinanțat din Fondul Social European. În cadrul acestuia, a fost achiziționată infrastructură hardware, constând în echipamente IT și licențe, care a fost integrată cu infrastructura existentă într-o soluție

omogenă, coerentă și unitară. Pe această bază a fost dezvoltată o infrastructură software alcătuită din module și aplicații IT concepute într-o manieră modulară, deschisă și flexibilă, care permite extinderea ulterioară cu funcționalități noi.

Platformele informatice astfel realizate deservesc atât utilizatorii interni, cât și beneficiarii externi, respectiv investitori, cetățeni și personal tehnic de specialitate, fiind esențiale pentru desfășurarea activităților instituției în regim digital, în condiții de securitate și eficiență operațională.

Pentru asigurarea sustenabilității proiectului menționat anterior, a securității serviciilor online și a consolidării măsurilor de securitate cibernetică la nivelul infrastructurii informatice a instituției, precum și pentru protejarea serviciilor digitale oferite investitorilor, este necesară asigurarea continuității protecției aplicațiilor web, în conformitate cu cerințele actuale de securitate cibernetică și cu standardele tehnice în vigoare.

În acest context, Sistemul Informatic Integrat de Management existent necesită achiziționarea unui echipament de tip Web Application Firewall, precum și achiziția de mentenanță pentru licențele de semnături de securitate aferente acestuia, pentru o perioadă de 1 an, în vederea prevenirii expunerii la atacuri cibernetice, consolidării nivelului de securitate cibernetică, asigurării conformității cu reglementările în vigoare privind protecția datelor cu caracter personal și garantării funcționării în condiții de siguranță a platformelor informatice administrate de Inspectoratul de Stat în Construcții.

4. Cerințe tehnice minime - sistem de protecție Web Application Firewall

4.1 Cerințe generale

Sistemul de protecție de tip Web Application Firewall trebuie să fie un echipament dedicat, de tip appliance hardware, destinat protejării aplicațiilor web și serviciilor online critice, capabil să funcționeze în regim de producție în infrastructuri informatice cu cerințe ridicate de disponibilitate și securitate.

Sistemul de protecție de tip Web Application Firewall va proteja infrastructura software a sistemului informatic și de comunicații a I.S.C. împotriva atacurilor cibernetice de tip SQL Injection, Cross Site Scripting, code executions, Browser Exploits, Brute Force Login, Buffer Overflows, Command Injection, Cookie Tampering/Poisoning, Cross Site Request Forgery, Denial Of Service, Directory Traversal Forms Tampering, Hidden Field Manipulation, HTTP Header overflow, Outbound Data Leakage, Local file Inclusion, Man în the Middle attacks, Remote File Inclusion, Session Hijacking, Site Reconnaissance, XML Intrusion Prevention etc.

Sistemul de protecție de tip Web Application Firewall va asigura o procesare cu o latență mică și performanțe foarte bune pentru inspecția atât a traficului http, cât și a traficului https, având posibilitatea de a oferi inspecție SSL și offload, cu o flexibilitate mare în vederea instalării.

Sistemul de protecție de tip Web Application Firewall va asigura protecție împotriva încercărilor de modificare nelegitimă a conținutului aplicațiilor web și bazelor de date, va efectua inspecția fișierelor și datelor încărcate în aplicațiile web, pentru a detecta virușii și malware-ul cunoscut.

Sistemul de protecție de tip Web Application Firewall va include un mecanism bazat pe captcha pentru identificarea utilizatorilor reali.

Sistemul de protecție de tip Web Application Firewall se va integra cu sistemul tehnic de protecție de tip Next Generation Firewall care este implementat în Sistemul Informatic și de Comunicații al I.S.C, astfel încât sursele carantinate de firewall să fie automat distribuite către web application firewall, pentru a nu le permite accesul către aplicațiile legitime.

4.2 Cerințe hardware și funcționale minime

Sistemul de protecție de tip Web Application Firewall trebuie să ofere funcționalități hardware dedicate și să fie dotat, fără a se limita la, cu următoarele caracteristici minime:

- interfețe de rețea, incluzând minimum 8 porturi Gigabit Ethernet (10/100/1000 Mbps) cu conectivitate RJ45;

- interfețe de rețea, incluzând minimum 8 porturi 10 Gigabit Ethernet SFP+, destinate traficului de date la nivel de aplicație web;
- suport pentru bypass hardware pentru minimum o parte dintre interfețele de date, în scopul asigurării continuității traficului;
- procesare SSL/TLS accelerată hardware, dedicată inspecției și offloading-ului criptografic;
- minimum un port USB pentru operațiuni de mentenanță și administrare;
- capacitate internă de stocare pe suport SSD de minimum 1,8 TB, configurată în regim de redundanță, utilizată pentru jurnalizare, rapoarte și funcții avansate de securitate;
- factor de formă de maxim 2U, adecvat montării în rack standard de centru de date;
- modul de securitate hardware de tip TPM sau echivalent, pentru protejarea cheilor criptografice și a integrității sistemului;
- suport pentru surse de alimentare redundante, de tip AC, hot-swappable, pentru asigurarea continuității operaționale.

4.3 Cerințe

Sistemul de protecție de tip Web Application Firewall trebuie să integreze funcționalități hardware și să fie dotat, fără a se limita la, cu următoarele caracteristici:

- protecție împotriva atacurilor web cunoscute, inclusiv OWASP Top 10;
- detecția și prevenirea atacurilor de tip SQL Injection, Cross Site Scripting, CSRF, DoS, brute force, session hijacking și altele similare;
- inspecție SSL/TLS cu posibilitate de offload;
- detecția și blocarea fișierelor malițioase de tip malware din tranzacțiile procesate;
- mecanisme de reputație IP și blocare automată a surselor malițioase;
- mecanisme de validare a utilizatorilor reali, inclusiv captcha sau metode echivalente;
- integrare cu soluții de tip Next Generation Firewall sau sisteme de securitate echivalente aflate în infrastructura existentă.

4.4 Servicii incluse

Furnizarea sistemului va include obligatoriu:
- instalarea la sediul autorității contractante a echipamentului;
- punerea în producție și integrarea în infrastructura existentă;
- testarea funcțională și de performanță;
- instruirea personalului desemnat de autoritatea contractantă pentru administrare și operare.

5. CERINȚE MINIME - MENTENANȚĂ ANUALĂ LICENȚE SEMNĂTURI DE SECURITATE

5.1 Descriere generală

Se solicită achiziția de mentenanță pentru licențele de semnături de securitate aferente sistemului de protecție de tip Web Application Firewall, pentru o perioadă de 12 luni.

Ofertantul va furniza mentenanță licențe semnături de securitate aferente sistemului de protecție de tip Web Application Firewall, pentru o perioadă de 12 luni, astfel încât să se asigure continuitatea dreptului de utilizare.

5.2 Conținutul serviciilor de mentenanță

Mentenanța pentru licențele de semnături și securitate aferente sistemului de protecție de tip Web Application Firewall (WAF), pentru o perioadă de 12 luni, trebuie să includă cel puțin următoarele funcționalități:

- actualizarea periodică și automată a bazelor de date de semnături de securitate, utilizate pentru identificarea amenințărilor la nivel de aplicație web;
- actualizarea reputației adreselor IP, cu suport pentru clasificarea pe categorii, surse și comportamente, și pentru blocarea automată a adreselor IP malițioase;

- detecția și prevenirea automată a atacurilor cibernetice la nivel de aplicație web, inclusiv identificarea noilor vectori de atac prin mecanisme de analiză și corelare;
- protecție împotriva fișierelor malițioase (malware), prin scanarea, detectarea și blocarea automată a conținutului periculos din traficul și tranzacțiile procesate;
- protecție împotriva atacurilor web cunoscute și emergente, inclusiv a celor descrise de standarde și bune practici recunoscute la nivel internațional, precum OWASP Top 10;
- suport continuu pentru funcționalități avansate de securitate, actualizări de intelligence de amenințări și mecanisme de corelare a evenimentelor de securitate;
- acces la servicii de suport tehnic și asistență pentru menținerea nivelului de securitate, conform politicilor producătorului soluției utilizate.

Cerințele de mai sus sunt minime și obligatorii și trebuie asigurate integral pe întreaga durată a perioadei de mentenanță.

Ofertantul va furniza mentenanță pentru licențele de semnături de securitate aferente sistemului de protecție de tip Web Application Firewall, pentru o perioadă de 12 luni, în scopul asigurării continuității dreptului de utilizare.

6. Servicii de garanție și suport tehnic

Sistemul de protecție de tip Web Application Firewall va beneficia de minim 12 luni de garanție și suport tehnic, ce va include:

- Înlocuirea echipamentului în caz de defecțiune hardware
- Înlocuirea echipamentului, în cazul în care echipamentul și accesoriile necesită înlocuire în perioada de garanție tehnică, ca urmare a defectării sau funcționării neconforme cu cerințele specificate în prezentul caiet de sarcini, se va realiza în maximum 24 de ore, în timpul programului de lucru al Autorității contractante, transportul de la și înapoi la Autoritatea contractantă intrând în sarcina ofertantului.
- Update firmware versiuni minore și majore.
- Update-uri automate de semnături de securitate pentru îndeplinirea tuturor funcționalităților cerute mai sus, timp de minim 12 luni.
- După expirarea serviciilor de suport tehnic, actualizare de semnături și de actualizare software, echipamentul trebuie să funcționeze, să permită atât administrarea, cât și fluxurile de date.
- Ofertantul va asigura Autorității contractante accesul pe site-ul producătorului pentru descărcarea de actualizări firmware sau alte componente software ale echipamentului și tehnologiilor livrate.
- În perioada de garanție, Ofertantul va repara sau înlocui, după caz, orice componentă defectă a echipamentului livrat. În cazul reparării, vor fi utilizate numai piese noi.
- Produsul înlocuit va beneficia de aceleași condiții de suport și garanție de la data semnării unui nou proces-verbal de recepție.
- Produsul înlocuit va respecta cel puțin specificațiile minime și obligatorii din caietul de sarcini.

Perioada de garanție începe din momentul semnării procesului verbal de recepție calitativă, iar pentru echipamentul livrat Ofertantul va asigura, fără costuri suplimentare, servicii de garanție și suport tehnic hardware și software.

Suportul tehnic va fi asigurat de către ofertant în baza unui Service Level Agreement (SLA), iar cererile de suport vor fi direcționate către un singur punct de contact, pe baza unei proceduri de tip helpdesk.

Serviciul de helpdesk va asigura obligatoriu cel puțin următoarele funcționalități:

- Validarea incidentelor de către personalul autorizat al Autorității contractante;
- Detalierea, validarea și aprobarea acțiunilor care trebuie desfășurate atât de către personalul Ofertantului, cât și de către personalul Autorității contractante, în vederea rezolvării incidentului (activități, livrabile, termene de realizare etc.);
- Urmărirea acțiunilor stabilite în vederea rezolvării incidentelor și a istoricului privind evenimentele legate de fiecare acțiune;

- Ataşarea de documente descriptive în fiecare moment al fluxului de rezolvare a incidentelor;
- Comunicare între părţi cu privire la acţiunile desfăşurate în vederea rezolvării incidentelor;
- Notificări automate cu privire la tratarea incidentelor;
- Proceduri de închidere a incidentelor;
- Sistem de raportare cu privire la incidentele din perioada de derulare a contractului.
- Ofertantul se obligă să păstreze confidenţialitatea tuturor informaţiilor la care are acces, prevederile legale de prelucrare şi protecţie a datelor cu caracter personal, precum şi cele legate de protecţia muncii.

Serviciile de helpdesk vor fi prestate utilizând exclusiv infrastructura de helpdesk a Ofertantului.

Ofertantul va oferi conturi de utilizator în cadrul aplicaţiei de tip helpdesk.

Clasificarea nivelurilor de deranjament (pentru solicitările/incidentele referitoare la activităţile de garanţie şi suport):

CRITIC
- Deranjamente care afectează activitatea instituţiei prin nefuncţionarea echipamentului sau blocarea anumitor funcţionalităţi.
- Aceste deranjamente afectează în mod direct funcţionarea echipamentului, componente hardware sau software cu impact asupra activităţii Autorităţii contractante sunt inoperabile sau întregul sistem este inoperabil.

MAJOR
- Problemele majore care au un impact semnificativ în funcţionarea echipamentului şi afectează în mod direct activitatea Autorităţii contractante. O componentă hardware sau software este parţial inoperabilă avand un impact major asupra activitaţii Autorităţii contractante. Aceste probleme nu sunt tolerate în folosinţa sistemelor.

MINOR
- Problemele minore care nu au un impact semnificativ în funcţionarea echipamentului şi nu afectează în mod direct activitatea Autorităţii contractante. O componentă hardware sau software fără impact critic nu funcţionează în parametri optimi. Aceste probleme sunt tolerate în folosinţa sistemelor.

Orar de preluare solicitări de intervenţie, timp de răspuns şi de remediere:

- Orar: luni - joi, orele 8 - 16,30; vineri, orele 8 - 14 considerate zile şi ore lucrătoare.
- Pentru probleme critice (de severitate 1) care au ca efect oprirea funcţionării echipamenului şi/sau activităţii sau serviciilor instituţiei, ofertantul va oferi asistenţă permanentă, 24 x 24, 7 x 7, pe toata durata contractului.
- Timpul de răspuns la solicitările Autorităţii contractante reprezintă timpul de identificare a problemelor sesizate, chiar prin deplasare în locaţia de unde există acces la echipamentul/aplicaţiile software care fac obiectul sesizării.
- Timpul de remediere a problemelor apărute în funcţionarea echipamentului instalat sau în curs de instalare: (Fix time) reprezintă durata de timp până la oferirea soluţiei finale.

Nivel de deranjament	Timp de răspuns	Timp de remediere
Critic	30 min	4 h
Major	1 h	8 h
Minor	4 h	2 zile

Nerespectarea orarului de preluare a solicitărilor, a timpilor de răspuns şi/sau de remediere la solicitările Autorităţii contractante menţionaţi mai sus, dă dreptul Autorităţii contractante de a percepe penalităţi şi/sau a pretinde plata de daune-interese.

Fiecare intervenție va fi consemnată într-un Raport de activități în vederea recepției serviciilor prestate.

a. <u>Livrare, ambalare, etichetare, transport și asigurare pe durata transportului</u>

Termenul de livrare este de maxim ***45 zile calendaristice(livrare, instalare, punere în funcțiune)*** de la data semnării contractului de către ambele părți. Echipamentul este considerat livrat și pus în funcțiune când toate activitățile în cadrul contractului au fost realizate și produsul este instalat, funcționează în parametri optimi și este acceptat de Autorității contractante.

Echipamentul livrat va respecta specificațiile tehnice solicitate și la livrare va fi însoțit de toate accesoriile necesare punerii în funcțiune, de fișa tehnică și de certificatul de garanție.

Echipamentul va fi livrat cantitativ și calitativ la **sediul ISC, str. C.F. Robescu nr. 23, sector 3, București.**

Transportul și toate costurile asociate cad în sarcina exclusivă a ofertantului.

b. <u>Instalarea, punerea în funcțiune, testarea echipamentului livrat</u>

Înainte de livrarea echipamentului, instalarea și integrarea acestuia în sistemul informatic și de comunicații al Autorității contractante, ofertantul va elabora un document de analiză cu aplicațiile web existente în infrastructura Autorității contractante, ce vor fi protejate de echipamentul dedicat și de noua soluție de securitate,în care va preciza detaliile de execuție, soluția de implementare recomandată (Inline, Proxy sau alternativ), precum și configurația inițială a profilurilor de inspecție, detecție și protecție.

Ofertantul va instala corespunzător echipamentul la sediul ISC și va efectua toate operațiile necesare pentru a asigura funcționarea optimă a echipamentului.

Testarea produsului va avea în vedere următoarele elemente: acces direct prin utilizator de tip administrator, verificare conectivitate în rețea, verificare resurse sistem - conform cerințelor din caietul de sarcini și ofertei tehnice. Operațiunile se vor finaliza prin întocmirea unui raport de instalare și punere în funcțiune.

Ofertantul va efectua pe cheltuiala sa toate testele, pentru a asigura Autorității contractante că echipamentul funcționează în parametri optimi.

După testarea funcțională a echipamentului, ofertantul în colaborare cu personalul de specialitate IT al Autorității contractante, va proceda la migrarea tuturor aplicațiilor web prin noul echipament dedicat protecției, prin noua soluție de securitate.

Această activitate se va realiza pe baza documentului redactat în faza de analiză și întreaga operațiune (pentru toate aplicațiile) va dura maxim 1 zi calendaristică.

Ofertantul se va sigura că întreruperea serviciilor și accesibilității aplicațiilor va fi minimală.

Ofertantul este responsabil pentru transferul certificatelor digitale de tip SSL de pe serverele de aplicații existente pe echipamentul de protecție web.

După migrarea aplicațiilor, ofertantul este responsabil să monitorizeze pentru cel puțin 3 zile calendaristice traficul către aplicații pentru a efectua eventuale optimizări ale configurației profilurilor de inspecție, detecție și protecție.

La finalizarea perioadei de monitorizare, ofertantul va prezenta un raport de migrare a aplicațiilor pe baza căruia se va întocmi procesul verbal de recepție calitativă.

c. <u>Documentații ce trebuie furnizate Autorității contractante în legătură cu produsul</u>

La livrare, Produsul trebuie să fie însoțite de următoarele documente:

- certificatul de garanție, emis de producător (ofertant);
- fișa tehnică a produsului;
- manual de utilizare în limba română sau limba engleză.

7. **Atribuțiile și responsabilitățile părților**

Ofertantul are obligația de a furniza un sistem de protecție de tip Web Application Firewall și mentenanță anuala licențe semnături de Securitate pentru sistemul de protecție de tip Web Application Firewall, în conformitate cu specificațiile caietului de sarcini.

Autoritatea contractantă are obligația de a plăti prețul sistemului de protecție de tip Web Application Firewall și mentenanță anuala licențe semnături de securitate pentru sistemul de protecție de tip Web Application Firewall, în termen de maximum 30 de zile de la data primirii facturii.

8. **Modalități și condiții de plată**

Plata se va efectua prin ordin de plată, în contul de trezorerie al furnizorului, în baza facturii transmise de acesta, primită și acceptată de Autoritatea contractantă, în termen de maxim 30 de zile de la data primirii facturii.

Factura se va emite după semnarea procesului - verbal de recepție calitativă și cantitativă.

INSPECTORATUL DE STAT ÎN CONSTRUCȚII
Devotament și profesionalism. Pentru siguranța ta!

Str. C.F. Robescu nr. 23, Sector 3
Cod poștal 030217
București

Tel: +40 21 318 17 00
Fax: +40 21 318 17 19
+40 21 318 17 03
+40 21 318 17 04
E-mail: isc@isc.gov.ro
www.isc.gov.ro

CRITERIUL DE ATRIBUIRE
și factorii de evaluare utilizați

A. **Criteriul de atribuire propus:** Cel mai bun raport calitate/preț - în conformitate cu prevederile legale în vigoare și directivele UE privind achizițiile publice în spațiul comunitar.

B. **Factori de evaluare propuși:**

1. Prețul ofertei:
Punctajul pentru factorul de evaluare „prețul ofertei" se acordă astfel:

a) Pentru oferta care are cel mai scăzut preț (**$preț_{minim}$**)se acordă punctajul maxim alocat factorului de evaluare respectiv 80 puncte.
b) Pentru un alt preț decât cel prevăzut la lit. a) punctajul se acordă astfel:
Punctaj acordat ofertei X= ($preț_{minim}$/preț oferta X) x punctaj maxim

2. Termen de livrare pentru Sistemul de protecție de tip Web Application Firewall

Notă:
Punctajul pentru acest factor de evaluare se acordă astfel:
a) 20 puncte se acordă pentru oferta care prezintă cel mai mic termen de livrare.
b) Pentru celelalte oferte punctajul se va calcula astfel:

T furnizare = T minim / T ofertat x 20;
T minim - cel mai mic termen de livrare, pentru care se va acorda maximul de puncte, respectiv 20 puncte;
T ofertat - termenul de livrare pentru Sistemul de protecție de tip Web Application Firewall;

Termene aplicabile:
Termenul minim punctat pentru livrarea sistemului este **1 zi**, considerat timpul minim necesar pentru realizarea acestei operațiuni;
Termenul maxim punctat pentru livrarea sistemului este este **45 de zile**.